

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1 **BRYAN CAVE LEIGHTON PAISNER LLP**
2 DANIEL T. ROCKEY (SBN 178604)
3 Three Embarcadero Center, 7th Floor
4 San Francisco, CA 94111
5 Email: daniel.rockey@BCLPLaw.com
6 Telephone: (415) 675-3400
7 Facsimile: (415) 675-3434
8
9 Attorneys for Defendant
10 NEIGHBORHOOD HEALTHCARE
11

12 **UNITED STATES DISTRICT COURT**
13 **SOUTHERN DISTRICT OF CALIFORNIA**

14 JANE DOE, individually and on behalf of all
15 others similarly situated,

16 Plaintiff,

17 vs.

18 NEIGHBORHOOD HEALTHCARE; HEALTH
19 CENTER PARTNERS OF SOUTHERN
20 CALIFORNIA; NETGAIN TECHNOLOGY,
21 LLC; and DOE DEFENDANTS 1-100,

22 Defendants.

Case No. **'21CV1587 BEN RBB**

**NOTICE OF REMOVAL OF ACTION
UNDER 28 U.S.C. §§ 1331, 1442, 2679(d)
AND 42 U.S.C. § 233(l)(2)**

**[FEDERAL QUESTION
JURISDICTION/FEDERAL DEFENDANT]**

Superior Court Case No.: 37-2021-00023936-
CU-BT-CTL
Complaint Filed: June 8, 2021
Trial Date: None Set

23 **TO THE CLERK OF THE ABOVE-ENTITLED COURT:**

24 **PLEASE TAKE NOTICE** that pursuant to 28 U.S.C. §§ 1331, 1442, 2679(d), and 42
25 U.S.C. § 233(l)(2), and on the grounds set forth below, Defendant Neighborhood Healthcare
26 (“Neighborhood”) hereby removes the above-captioned action, styled *Jane Doe, individually and*
27 *on behalf of all others similarly situated v. Neighborhood Healthcare; Health Center Partners of*
28 *Southern California; Netgain Technology, LLC; and Doe Defendants 1-100*, Case No. 37-2021-

00023936-CU-BT-CTL, from the Superior Court of the State of California for the County of San Diego to this Court. Neighborhood states the following in support of this Notice of Removal.

I. BACKGROUND

1. On June 8, 2021, Plaintiff Jane Doe (“Plaintiff”) commenced the above-referenced action in the Superior Court of the State of California for the County of San Diego (the “Superior Court”) by filing a Complaint (“Complaint”) against Removing Defendant Neighborhood and co-defendants Health Center Partners of Southern California (HCP), Netgain Technology, LLC (Netgain), and Doe Defendants 1-100 (the “State Court Action”). On September 8, 2021, Plaintiff filed a First Amended Class Action Complaint For Damages, Restitution, And Injunctive Relief For Violations Of: (1) The Confidentiality Of Medical Information Act, Civil Code §§ 56, Et Seq.; (2) Breach Of California Security Notification Laws, California Civil Code § 1798.82; And (3) Business And Professions Code §§ 17200, *et seq.* against the same three defendants (“FAC”). A copy of all process, pleadings, orders, and other documents currently on file in the state court, including the FAC (collectively, the “State Court File”) is attached hereto as Exhibit 1.

2. Neighborhood is a non-profit benefit corporation and community health center that provides medical, dental, and behavioral health services to underserved communities in and around Escondido, California, where it is located. Pursuant to § 330 of the Public Health Service Act (codified at 42 U.S.C. § 254b *et seq.*), Neighborhood is a “health center” that serves medically underserved communities, a federal grant recipient (Grant No. H80CS00285), and a “deemed entity” pursuant to 42 U.S.C. § 233(g). A copy of the “Deeming Notice” issued by the Health Resources and Services Administration (“HRSA”) is attached as Exhibit 2 (“Deeming Notice”).

3. At all times relevant to the allegations of the Complaint, including the period January 1, 2020 through December 31, 2020, the Secretary of the U.S. Department of Health and Human Services (“HHS”) deemed Neighborhood and its officers, governing board members, employees,

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

and contractors as U.S. Public Health Service (“PHS”) “employees” under 42 U.S.C. § 233(a). Ex. 2. “Deeming” status under 42 U.S.C. § 233(a) and § 233(g) provides the deemed entity with absolute immunity from any civil action or proceeding concerning the provision of medical, surgical, dental, or “related functions.”

4. As explained more fully below, the immunity from suit provided by § 233(a) and § 233(g) “deeming” applies to the State Court Action. Plaintiff Doe, a patient of Neighborhood Healthcare, alleges that Neighborhood failed to ensure the confidentiality of her electronic patient medical records, as required by Civil Code § 56.10 and § 56.101 of the Confidentiality of Medical Information Act (“CMIA”). See Ex. 1. As reflected in Plaintiff’s FAC, Plaintiff seeks damages and injunctive relief arising from a December 2020 ransomware attack against Netgain, Neighborhood’s former data hosting provider, which allegedly resulted in the unauthorized disclosure of Plaintiff Doe’s electronic patient medical records maintained by Neighborhood. See Ex. 1, FAC, at ¶¶10 - 13, Ex. B (Neighborhood notice letter).

II. VENUE

5. Venue is proper in this Court pursuant to 28 U.S.C. § 1446 as the United States District Court for the Southern District of California embraces the state court in the County of San Diego, California, in which Plaintiff filed her state court action.

III. FEDERAL QUESTION JURISDICTION

6. Federal district courts have subject-matter jurisdiction only as authorized by the Constitution and Congress. U.S. Const. art. III, § 2, cl. 1. A suit filed in state court may be removed to federal court. 28 U.S.C. § 1441(a) where the District Court would have original jurisdiction over the matter. Federal courts have original jurisdiction where an action arises under federal law. 28 U.S.C. § 1331.

IV. STATUTORY FRAMEWORK

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

A. FSHCAA Deemed Entity: 42 U.S.C. § 233

1. Federal Tort Claims Act

7. A federal district court has original jurisdiction over claims arising under the Federal Torts Claims Act (“FTCA”). *McDaniel v. Mylan Inc.*, Case No. 7:19-cv-00209-LSC, 2019 WL 1989234, at *3 (N.D. Ala. May 6, 2019). The Federally Supported Health Centers Assistance Act of 1992 (FSHCCA), 42 U.S.C. § 233(g)-(n), amended the Public Health Services Act (“PHSA”), 42 U.S.C. § 201 *et seq.*, to provide that the FTCA is the exclusive remedy for all personal injury claims brought against Deemed Entities and their employees, officers, board members, etc. *Rosenblatt v. St. John’s Episcopal Hosp.*, Case No. 11-CV-1106 (ERK) (CLP), 2012 WL 294518, at *4 (E.D.N.Y. Jan. 31, 2012).

8. “Specifically, the FSHCAA ‘created a process by which ‘public and nonprofit private entities’ receiving federal funds pursuant to 42 U.S.C. § 254b(c)(1)(A) ‘shall be deemed to be [employees] of the Public Health Service.’ 42 U.S.C. § 233(g)(1)(A).” *Friedenberg v. Lane Cnty.*, Case No. 6:18-cv-00177-JR, 2018 WL 11352363, at *2 (D. Ore. May 23, 2018) (*quoting Lomando v. United States*, 667 F.3d 363, 371 (3d Cir. 2011)). Under § 233(a), the FTCA remedy applies to “damage for personal injury, including death, resulting from the performance of medical, surgical, dental, or related functions” 42 U.S.C. § 233(a). An “‘entity receiving Federal funds under [42 U.S.C. § 254(b)]’” is deemed to be a PHS employee for purposes of such claims. *Rosenblatt*, 2012 WL 294518, at 4 (*quoting* 42 U.S.C. § 233(g)(4)). “[A]ny officer, governing board member, or employee of such an entity” is also included. 42 U.S.C. § 233(g)(1)(A). Claims concerning conduct or activities committed by deemed PHS employees while acting within the scope of their employment are covered by the FSHCAA. *Rosenblatt*, 2012 WL 294518, at *4 (*citing* 42 U.S.C. § 233(a)).

1 9. Accordingly, “both federally supported community health centers and their
2 employees . . . are immunized from tort claims arising from medical care (within the course and
3 scope of their employment), in that such claims can only be brought against the United States under
4 the FTCA.” *Huynh v. Sutter Health*, Case No. 2:20-cv-1757-MCE-CKD, 2021 WL 2268889, at *2
5 (E.D. Cal. June 3, 2021) (*citing* 42 U.S.C. § 233(a)). This immunity is absolute. *See Hui v.*
6 *Castaneda*, 559 U.S. 799, 806 (2010) (“Section 233(a) grants absolute immunity to PHS officers
7 and employees for actions arising out of the performance of medical or related functions within the
8 scope of their employment by barring all actions against them for such conduct.”)).

10 **2. FSHCAA “Deeming” Protection via HHS**

11 10. “Pursuant to 42 U.S.C. § 233(g), HHS is authorized to “deem” federally funded
12 health centers to be employees of the Public Health Service’ and ‘[a]ny suit filed against an entity
13 so deemed must be asserted pursuant to the FTCA.” *Rosenblatt*, 2012 WL 294518, at *4 (*quoting*
14 *A.Q.C. ex rel. Castillo v. Bronx–Lebanon Hosp. Ctr.*, No. 11 Civ. 2656, 2012 WL 170902, at *3
15 (S.D.N.Y. Jan. 20, 2012) (*citing* 42 U.S.C. § 233(a))). FSHCAA “deeming” protection is extended
16 to “public or nonprofit private entities that receive certain federal health funds, submit an annual
17 application to HHS, meet certain criteria, and obtain annual approval by the Secretary of HHS.”
18 *Friedenberg*, 2018 WL 11352363, at *2 (*citing* 42 U.S.C. § 233(g), (h)).

19 11. “The FSHCAA sets out detailed rules and procedures for ‘deeming’ an entity (i.e.,
20 health center) or individual to be a PHS employee. . . . [H]ealth centers apply to HHS annually for
21 themselves and their employees, and HHS determines whether they are deemed to be an employee
22 of the PHS.” *Huynh*, 2021 WL 2268889, at *2 (*citing* 42 U.S.C. §§ 233(g)(1)(D)-(E)). “HHS advises
23 the applicant of its determination in a ‘deeming notice.’” *Huynh*, 2021 WL 2268889, at *2. HHS-
24 approved “deeming” status applies to the upcoming calendar year. *See Friedenberg*, 2018 WL
25 11352363, at *2 (*citing* 42 U.S.C. § 233(g)(1)(A), (E)) (“Upon approval of the required application,
26
27
28

1 the Secretary of HHS ‘deems’ these entities and their employees to be employees of the PHS for the
2 upcoming calendar year.”).

3 12. After “HHS deems an entity or individual a Public Health Service employee, this
4 determination ‘shall be final and binding upon the Secretary and the Attorney General and other
5 parties to any civil action or proceeding.” *Rosenblatt*, 2012 WL 294518, at *4 (citing 42 U.S.C. §
6 233(g)(1)(F)). “Once deemed a PHS employee, the entity and covered individuals enjoy certain
7 procedural protections in litigation.” *Huynh*, 2021 WL 2268889, at *3.

8
9 13. On or about August 29, 2019, the HRSA issued a Deeming Notice confirming that
10 Neighborhood is deemed to be a PHS employee for purposes of the FTCA and FSHCAA for the
11 period January 1, 2020 through December 31, 2020. *See* Ex. B.

12 **3. “Deemed” Entities’ Right to Removal**

13 14. A federally funded community health center facing a state court suit asserting claims
14 that “fall under the FTCA through the FSHCAA” must notify the appropriate agency – in this case,
15 HHS – of the filing of the action and provide a copy of the relevant pleadings. *See McDaniel*, 2019
16 WL 1989234, at *3; *Estate of Booker v. Greater Philadelphia Health Action, Inc.*, 10 F. Supp. 3d
17 656, 665 (E.D. Penn. 2014); 28 C.F.R. § 15.2. The agency is then directed to notify the United
18 States Attorney for the district embracing the court in which the lawsuit was filed. 28 C.F.R. § 15.2.

19 20. Within 15 days after being notified that a complaint has been filed in state court
20 against a Deemed Entity, the Attorney General “shall make an appearance in such court and advise
21 such court as to whether the Secretary has determined under subsections (g) and (h), that such entity,
22 officer, governing board member, employee, or contractor of the entity is deemed to be an employee
23 of the Public Health Service for purposes of this section with respect to the actions or omissions that
24 are the subject of such civil action or proceeding.” 42 USC § 233(l)(1). In the event the Attorney
25 General fails to appear in court within 15 days, “upon petition of any entity ... named, the civil
26
27
28

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1 action or proceeding shall be removed to the appropriate United States district court.” 42 USC §
 2 233(l)(2); *Friedenberg*, 2018 WL 11352363, at *2 (“[I]f the Attorney General or her designee ‘fails
 3 to appear in State court within [the 15-day] time period,’ the defendant[] may remove the case to
 4 the appropriate United States district court.”).

5 16. Once the potential federal employee removes the action, the action ‘is stayed until
 6 the district court conducts a hearing and makes a determination as to the appropriate forum for
 7 assertion of the claim.’” *McDaniel*, 2019 WL 1989234, at *3 (*quoting Allen v. Christenberry*, 327
 8 F.3d 1290,1294 (11th Cir. 2003)).
 9

10 **B. Federal Officer Removal: 28 U.S.C. § 1442**

11 17. “[T]he Federal Officer Removal statute as set forth in 28 U.S.C. § 1442(a)(1), []
 12 ‘authorizes removal of a civil action brought against any person acting under an officer of the United
 13 States for or relating to any act under color of such office.’” *Kruse v. Actuant Corp.*, Case No. 2:19-
 14 cv-09540-ODW (RAOx), 2020 WL 3287883, at *3 (C.D. Cal. June 18, 2020) (*quoting Leite v.*
 15 *Crane Co.*, 749 F.3d 1117, 1120 (9th Cir. 2014)). “Unlike removal pursuant to 28 U.S.C. § 1441,
 16 the Supreme Court has ‘mandated a generous interpretation of the federal officer removal statute.’”
 17 *Cratin v. Sandiford*, Case No. 14-CV-03374-LHK, 2014 WL 5454691, at *2 (N.D. Cal. Oct. 27,
 18 2014) (*quoting Durham v. Lockheed Martin Corp.*, 445 F.3d 1247, 1252 (9th Cir. 2006)). “The
 19 right of removal under § 1442 is ‘absolute.’” *Cratin*, 2014 WL 5454691, at *2 (*quoting Durham*,
 20 445 F.3d at 1252. Therefore, as the U.S. Court of Appeals for the Ninth Circuit has stated, “[s]ection
 21 1442 is to be ‘interpreted broadly in favor of removal.’” *Perez v. Consol. Tribal Health Project*,
 22 Case No. 12-5403-SC, 2013 WL 1191242, at *2-3 (N.D. Cal. Mar. 21, 2013) (*quoting Durham*, 445
 23 F.3d 1247 at 1252). Thus, Section 1442(a)(1) removal “is not subject to the well-pleaded complaint
 24 rule.” *Kruse*, 2020 WL 3287883, at *3 (*citing Durham*, 445 F.3d at 1252).
 25
 26
 27
 28

1 18. Importantly, a defendant removing under Section 1442(a)(1) “may remove an
 2 entire action unilaterally, without the consent of other defendants.” *Kruse*, 2020 WL 3287883, at *3
 3 (*citing Durham*, 445 F.3d at 1252). Thus, unlike removal on the basis of diversity, a Deemed Entity
 4 need not include a statement in the Notice of Removal confirming the consent of other defendants
 5 or explaining their lack of consent. *Id.*

6 19. Furthermore, removal under § 233(l)(2) is not constrained by the usual 30-day time
 7 limit on removal, and may occur at any time prior to the trial of the action. *See Estate of Booker*,
 8 10 F. Supp. 3d at 665 (“The fact that § 233(l)(2) was added to a statutory scheme in which suits
 9 against health centers were removable at any time before trial provides a basis to infer that Congress
 10 intended the same time frame to govern removals by the health centers themselves.”); 28 U.S.C.A.
 11 § 2679(d)(1) (“shall be removed without bond at any time before trial....”).

12 20. “A party seeking removal under section 1442 must demonstrate that (a) it is a
 13 ‘person’ within the meaning of the statute; (b) there is a causal nexus between its actions, taken
 14 pursuant to a federal officer’s directions, and plaintiff’s claims; and (c) it can assert a ‘colorable
 15 federal defense.’” *Perez*, 2013 WL 1191242, at *2. With respect to a “colorable” federal defense,
 16 “the removing defendant need not show that the defense is meritorious, but that there is a legitimate
 17 question of federal law to be decided regarding the validity of the defense.” *Kruse*, 2020 WL
 18 3287883, at *3 (*citing Mesa v. California*, 489 U.S. 121, 129 (1989)).

21 V. FACTUAL AND LEGAL GROUNDS FOR REMOVAL

22 A. Section 233(g) Immunity Extends to the Alleged Breach of Patient Confidentiality

23 21. Under § 233(a), immunity applies to “damage for personal injury, including death,
 24 resulting from the performance of medical, surgical, dental, or *related functions*” 42 U.S.C. §
 25 233(a) (emphasis added). Consistent with the foregoing, federal courts have long recognized that §
 26 233(a) immunity “is not limited to claims for medical malpractice” and instead extends to claims
 27

1 which arise from functions *related* to the provision of medical care. *Teresa T. v. Ragaglia*, 154 F.
 2 Supp. 2d 290, 299-300 (D. Conn. 2001). *See also Cuoco v. Moritsugu*, 222 F.3d 99, 108 (2d Cir.
 3 2000) (“Cuoco asserts that § 233(a) provides immunity only from medical malpractice claims. But
 4 there is nothing in the language of § 233(a) to support that conclusion.”); *Z.B. ex rel. Next Friend v.*
 5 *Ammonoosuc Cmty. Health Servs., Inc.*, Case No. CIV. 03-540 (NH), Civ. 04-34-P-S (ME), 2004
 6 WL 1571988, at *3 (D. Me., June 13, 2004) (report and recommendation adopted *sub nom. Z.B. ex*
 7 *rel. Kilmer v. Ammonoosuc Cmty. Health Servs., Inc.*, Case No. CIV. 04-34-P-S, 2004 WL 1925538
 8 (D. Me. Aug. 31, 2004) (holding that alleged failure to report domestic abuse in connection with
 9 home health visits subject to § 233(a) immunity as such “negligence is ‘related to’ the provision of
 10 medical services because the duty to report arises out of the employees’ status as medical
 11 professionals.”); *Pinzon v. Mendocino Coast Clinics Inc.*, Case No. 14-CV-05504-JST, 2015 WL
 12 4967257, at *3 (N.D. Cal., Aug. 20, 2015) (holding that plaintiff’s claims for violation of the
 13 Americans with Disabilities Act, the Civil Rights Act of 1964, and the Health Insurance Portability
 14 and Accountability Act of 1996 were covered by § 233(a) immunity because the remedy against the
 15 United States provided thereby is “‘exclusive of any other civil action or proceeding by reason of
 16 the same subject-matter’ against the employee”).

19 22. As this Court has held, the term “related functions” as used in § 233(a) includes
 20 administrative or operational activities that relate to the provision of medical, dental, or surgical
 21 healthcare. *See, e.g., C. K. v. United States*, Case No. 19-CV-2492 TWR (RBB), 2020 WL 6684921,
 22 at *6 (S.D. Cal., Nov. 12, 2020) (“administrative or operational duties could qualify as related
 23 functions where they were connected to the provision of medical care”).

25 23. Maintaining medical records for patients receiving health care and ensuring the
 26 confidentiality of such records is a core administrative and operational function of providing
 27 healthcare and is thus a “medical ... or related function” within the meaning of 42 U.S.C. § 233(a).

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1 Maintaining the confidentiality of health records is a legally mandated function of providing health
2 care under both state and federal law. With respect to federal law, the Health Insurance Portability
3 and Accountability Act of 1996 (“HIPAA”) requires that healthcare providers maintain patient
4 health records and disclose such records only with patient authorization (45 C.F.R. § 164.502) or
5 “for treatment, payment, or health care operations” (45 C.F.R. § 164.506), and requires maintenance
6 of administrative, physical, and technical safeguards for electronic patient health records to guard
7 against unauthorized access or disclosure (45 C.F.R. § 164.302 et seq.). Likewise, the CMIA, the
8 statute under which Plaintiff Doe sues here, requires that health care providers who maintain patient
9 medical records take steps to ensure the confidentiality of such records and disclose them only for
10 authorized purposes. Civ. Code §56.10, § 56.101. Furthermore, the statute which governs the
11 federal health center program, and which renders health centers eligible for § 233(a) immunity,
12 requires the center to have, among other things, “an ongoing quality improvement system that
13 includes clinical services and management, and that maintains the confidentiality of patient
14 records.” 42 U.S.C. § 254b(b)(1)–(2), (k)(3)(C).
15
16

17 24. Consistent with the foregoing, federal courts have determined that § 233(a) immunity
18 applies to alleged breaches of patient confidentiality, such as those alleged here. For example, in
19 *Mele v. Hill Health Ctr.*, the district court held that allegations the defendant improperly disclosed
20 the plaintiff’s medical records in violation of medical confidentiality laws fell within the “related
21 functions” covered by §233(a). Case No. 3:06CV455 (SRU), 2008 WL 160226, *2-4 (D. Conn.,
22 Jan. 8, 2008). As the court explained, the “claims concern the medical functions of providing
23 treatment and the related function of ensuring the privacy of patient medical information. Thus, the
24 claims are covered by section 233(a).” *Id.* at *3.
25

26 25. The court in *Kezer v. Penobscot Cmty. Health Ctr.*, Case No. 15-cv-225-JAW, 2019
27 BL 141566 (D. Me. Mar. 21, 2019), similarly held that an alleged breach of patient confidentiality
28

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1 fell within the scope of § 233(a) immunity, as “the [p]laintiffs’ claim arose when the [d]efendants,
 2 who are all medical providers, fa[iled] to comply with their ongoing professional duty to keep Ms.
 3 Kezer’s medical records confidential while performing health care services.” *Id.*, at *6. In *Kezer*,
 4 the court determined that courts must look to state law to determine whether an alleged breach of
 5 confidentiality by a medical professional is covered by § 233(a). Finding that a breach of patient
 6 confidentiality is among the class of cases considered medical negligence under state law, the court
 7 had no trouble concluding that plaintiff’s claims were related functions covered by § 233(a). *Id.*
 8 Notably, this Court cited *Kezer* approvingly in rejecting the Department of Justice’s argument that
 9 § 233(a) did not embrace a health center employee’s alleged failure to report suspected sexual abuse.
 10 *See C.K.*, 2020 WL 6684921, at *6 (“As in *Kezer*, applicable state law supports a medical
 11 malpractice claim,....”) (J. Robinson).

12
 13 26. Other courts have likewise found that § 233 immunity applies to the alleged breaches
 14 of medical confidentiality. *See Logan v. St. Charles Health Council, Inc.*, Case No. 1:06CV00039,
 15 2006 WL 1149214, at *1–3 (W.D. Va., May 1, 2006) (holding that FTCA embraces claims for
 16 breach of privacy statute, though § 233(a) did not apply in that case because plaintiff’s claims
 17 implicated employer/employee relationship, rather than patient/medical professional relationship);
 18 *Roberson v. Greater Hudson Valley Family Health Ctr., Inc.*, Case No. 17-CV-7325 (NSR), 2018
 19 WL 2976024, at *1 (S.D.N.Y. June 12, 2018) (claim alleging that employee of defendant
 20 inappropriately accessed plaintiff’s medical records and disclosed information to people who knew
 21 plaintiff must be dismissed for failure to file administrative claim as required by FTCA).

22
 23
 24 **B. The FAC Alleges that Neighborhood Negligently Allowed Access to Plaintiff’s Medical
 Records in Violation of the CMIA**

25 27. The FAC alleges that “Plaintiff JANE DOE was a patient of, received medical
 26 treatment and diagnosis from, and provided her personal information, including her name, address,
 27 date of birth, social security number, phone number and email address to Defendant Neighborhood
 28

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1 Healthcare.” FAC, ¶10. The FAC further alleges that “At all times relevant to this action, NH
2 [Neighborhood] was and is a provider of health care, a contractor, and/or other authorized recipient
3 of personal and confidential medical information, as that term is defined and set forth in the
4 [Confidentiality of Medical Information] Act, including the names, addresses, dates of birth,
5 diagnosis/treatment information and treatment cost information of Plaintiff and the SubClass
6 (defined infra), and is subject to the requirements and mandates of the Act, including but not limited
7 to Civil Code §§ 56.10, 56.101 and 56.36.” FAC, ¶11.¹

8
9 28. The FAC additionally alleges that a data breach of Netgain’s servers occurred,
10 allowing an unauthorized third party to gain access to medical files maintained by Neighborhood
11 between October 22, 2020 and December 3, 2020. FAC, ¶¶10-13. The FAC goes on to allege that
12 “[a]t all times relevant to this action, including the period from October 22, 2020 to December 3,
13 2020, Defendants negligently created, maintained, preserved, and/or stored Plaintiff’s, the
14 SubClass’ and the Class’ medical information, including Plaintiff’s, the SubClass’ and the Class’
15 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
16 electronic form, onto Defendants’ computer networks in a manner that did not preserve the
17 confidentiality of the information, and negligently failed to protect and preserve confidentiality of
18 electronic medical information of Plaintiff, the SubClass and the Class in their possession, as
19 required by HIPPA and the Act, and specifically, under Civil Code §§ 56.10(a), 56.26(a),
20
21

22
23 ¹ The FAC further alleges: “At all times relevant to this action, including the period from October
24 22, 2020 to December 3, 2020, NH maintained and continues to maintain “medical information,”
25 “patients” within the meaning of Civil Code § 56.05(k). At all times relevant to this action,
26 including the period from October 22, 2020 to December 3, 2020, NH was and is a “provider of
27 health care” within the meaning of Civil Code § 56.05(m). At all times relevant to this action,
28 including the period from October 22, 2020 to December 3, 2020, Plaintiff and SubClass members
were patients, within the meaning of Civil Code § 56.05(k).” FAC, ¶18.

1 56.36(e)(2)(E), 56.101(a), and 56.101(b)(1)(A), and according to their written representations to
2 Plaintiff and the Class.” FAC, ¶60.

3 29. The FAC asserts two causes of action against Neighborhood. The FAC alleges that
4 Neighborhood violated Civ. Code § 56.10 and § 56.101 of the CMIA by disclosing Plaintiff’s
5 medical information without Plaintiff’s authorization or an exemption, and negligently storing
6 Plaintiff’s medical information in such a way that it was accessed by an unauthorized third party.
7 ¶¶93-104. The FAC also asserts a claim under the Unfair Competition Law, Bus. & Prof. Code §
8 17200 *et seq.*, based upon the alleged violations of the CMIA. FAC, ¶¶130-139.

9
10 30. California courts have made clear that the alleged failure of a healthcare provider to
11 maintain the confidentiality of medical records in violation of §56.10 of the CMIA – the precise
12 claim asserted here – constitutes a claim for professional negligence under California law. *See, e.g.,*
13 *Francies v. Kapla*, 127 Cal. App. 4th 1381, 1386, fn. 11, (2005) as modified (Apr. 8, 2005) (holding
14 that claim for unauthorized disclosure of medical records in violation of CMIA is subject to cap on
15 noneconomic damages under Medical Injury Compensation Reform Act); Civ. Code, § 3333.2
16 (MICRA applies to “any action for injury against a health care provider based on professional
17 negligence.”). Because the FAC alleges that Neighborhood negligently stored and/or shared
18 Plaintiff’s medical information, acquired in the course of the provider/patient relationship and in
19 connection with the provision of healthcare services, in violation of § 56.10 and § 56.101 of the
20 CMIA, the he claims asserted against Neighborhood in fall squarely within the claims covered by §
21 233(g).
22

23
24 **B. Federal Officer Removal: 28 U.S.C. § 1442**

25 31. In the instant matter, the three requirements for Federal Officer Removal under 42
26 U.S.C. § 1442 are met. *See Perez*, 2013 WL 1191242, at *2. First, as a non-profit public benefit
27 corporation and community health center, Neighborhood is a “person” within the meaning of 28

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1 U.S.C. § 1442(a)(1). *See Fung v. Abex Corp.*, 816 F. Supp. 569, 572 (N.D. Cal. 1992) (determining
2 that a corporation can qualify as a “person” under § 1442(a)(1)).

3 32. Second, there is a causal nexus between Neighborhood’s actions taken pursuant to a
4 federal officer’s directions and plaintiff’s claims. Plaintiff alleges that, in violation of California
5 state law, Neighborhood failed to ensure the confidentiality of her patient records—records that
6 relate to and document the medical services she received from Neighborhood. “The FSHCAA was
7 enacted in 1992 to reduce costs for health centers serving medically underserved populations.”
8 *Huynh*, 2021 WL 2268889, at *2 n.4. The HHS grant was issued to Neighborhood to support the
9 provision of general health services, such as medical, dental, and behavioral health services to
10 underserved communities, such as those provided to Plaintiff here. *See Ex. 2, HRSA Deeming*
11 *Notice; Perez*, 2013 WL 1191242, at *3.

12 33. Third, Neighborhood asserts a “colorable federal defense” through, as set forth
13 above, its assertion of § 233(a) immunity. *See e.g., Fung* (determining defendant “satisfied the final
14 requirement of removal under § 1442(a)(1) by asserting the government contractor immunity as a
15 colorable federal defense”).

16 **VI. NOTIFICATION TO HHS AND US ATTORNEY**

17 34. On August 18, 2021, Neighborhood notified HHS, as well as the Acting U.S.
18 Attorney for the Southern District of California, of the State Court Action as required under HHS
19 regulations and consistent with the HHS guidance. *See Ex. 3.* The U.S. Attorney has not appeared
20 in the State Court Action within the 15-day limit of § 233(l)(1), which expired on September 3,
21 2021.

22 35. As a result, pursuant to § 233(l)(2), Neighborhood now removes this action to this
23 Court. *Friedenberg*, 2018 WL 11352363, at *2 (*citing* 42 U.S.C. § 233(l)(2)) (“[I]f the Attorney
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

General or her designee ‘fails to appear in State court within [the 15-day] time period,’ the defendant[] may remove the case to the appropriate United States district court.”).

36. Removal pursuant to 42 U.S.C. § 233(l)(2) may occur at any time prior to trial.² See *Estate of Booker*, 10 F. Supp. 3d at 665. This Notice of Removal is therefore timely.

37. Pursuant to 28 U.S.C. § 1446(d), a copy of this Notice of Removal will be filed in the Superior Court of the State of California, County of San Diego, and served upon Plaintiff.

Dated: September 8, 2021

Daniel T. Rockey
BRYAN CAVE LEIGHTON PAISNER LLP

By: /s/ Daniel T. Rockey
Daniel T. Rockey

Attorneys for Defendant
Neighborhood Healthcare

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

² Given its August 18, 2021 FTCA Notice Letter, Neighborhood calculated the Attorney General’s 15-day deadline as September 3, 2021. Given the court-observed Labor Day holiday on September 6, 2021, Neighborhood files its Notice of Removal on the business day immediately following.

CERTIFICATE OF SERVICE

I am employed in the aforesaid County, State of California; I am over the age of eighteen years and not a party to the within entitled action; my business address is: Three Embarcadero Center, 7th Floor, San Francisco, CA 94111.

On September 9, 2021, I caused to be served on the interested parties in said action the within:


- **NOTICE OF REMOVAL OF ACTION UNDER 28 U.S.C. §§ 1331, 1442, 2679(d) AND 42 U.S.C. § 233(l)(2)**
- **CIVIL CASE COVER SHEET**
- **CORPORATE DISCLOSURE STATEMENT**

Patrick N. Keegan, Esq. KEEGAN & BAKER, LLP 2292 Faraday Avenue Suite 100 Carlsbad, CA 92008 pkeegan@keeganbaker.com <i>Attorneys for Plaintiff</i>	MICHAEL J. DAILEY GORDON REES SCULLY MANSUKHANI 633 West Fifth Street, 52nd Floor Los Angeles, CA 90071 D: 213-929-2418 <i>Counsel for HEALTH CENTER</i> PARTNERS OF SOUTHERN CALIFORNIA
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[X] BY E-MAIL – I caused a true copy of the foregoing document(s) to be served by electronic email transmission at the time shown on each transmission, to each interested party at the email address shown above. Each transmission was reported as complete and without error.

[X] BY MAIL I am “readily familiar” with the firm’s practice of collection and processing correspondence for mailing. Under that practice it would be deposited with U.S. Postal Service on that same day with postage thereon fully prepaid at **San Francisco**, California in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed on September 9, 2021, at San Francisco, California.



 Bridgette Warren

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT 1

SUPERIOR COURT OF CALIFORNIA
County of SAN DIEGO

Register of Actions Notice

Case Number:	37-2021-00023936-CU-BT-CTL	Filing Date:	06/01/2021
Case Title:	Doe vs Neighborhood Healthcare [EFILE]	Case Age:	99 days
Case Status:	Pending	Location:	Central
Case Category:	Civil - Unlimited	Judicial Officer:	Joel R. Wohlfeil
Case Type:	Business Tort	Department:	C-73

Future Events

Date	Time	Department	Event
11/05/2021	01:30 PM	C-73	Civil Case Management Conference - Complaint

Participants

Name	Role	Representation
Doe, Jane	Plaintiff	KEEGAN, PATRICK N
Health Center Partners of Southern California	Defendant	
Neighborhood Healthcare	Defendant	Rockey, Daniel T
Netgain Technology LLC	Defendant	

Representation

Name	Address	Phone Number
KEEGAN, PATRICK N	2292 Faraday Avenue Suite 100 Carlsbad CA 92008	
ROCKEY, DANIEL T	3 Embarcadero Center San Francisco CA 94111	(415) 675-3400

ROA#	Entry Date	Short/Long Entry	Filed By
1	06/01/2021	Complaint filed by Doe, Jane. Refers to: Neighborhood Healthcare; Health Center Partners of Southern California; Netgain Technology LLC	Doe, Jane (Plaintiff)
2	06/01/2021	Civil Case Cover Sheet filed by Doe, Jane. Refers to: Neighborhood Healthcare; Health Center Partners of Southern California; Netgain Technology LLC	Doe, Jane (Plaintiff)
3	06/01/2021	Original Summons filed by Doe, Jane. Refers to: Neighborhood Healthcare; Health Center Partners of Southern California; Netgain Technology LLC	Doe, Jane (Plaintiff)
4	06/02/2021	Summons issued.	
5	06/01/2021	Case assigned to Judicial Officer Wohlfeil, Joel.	
6	06/02/2021	Civil Case Management Conference scheduled for 11/05/2021 at 01:30:00 PM at Central in C-73 Joel R. Wohlfeil.	
7	06/02/2021	Civil Case Management Conference scheduled for 11/05/2021 at 01:30:00 PM at Central in C-73 Joel R. Wohlfeil.	
8	06/02/2021	Case initiation form printed.	
9	06/02/2021	Ex Parte scheduled for 06/08/2021 at 08:30:00 AM at Central in C-73 Joel R. Wohlfeil.	
10	06/02/2021	Civil Case Management Conference scheduled for 11/05/2021 at 01:30:00 PM at Central in C-73 Joel R. Wohlfeil was vacated.	
11	06/02/2021	Ex Parte Application - Other and Supporting Documents filed by Doe, Jane.	Doe, Jane (Plaintiff)
12	06/02/2021	Proposed Order submitted by Doe, Jane received but not filed on 06/02/2021.	Doe, Jane (Plaintiff)
13	06/08/2021	Minutes finalized for Ex Parte heard 06/08/2021 08:30:00 AM.	

14	06/08/2021	Order After Hearing (Order granting Pltf's ex parte application to appear by Pseudonym. Order is without prejudice.) filed by Doe, Jane.	Doe, Jane (Plaintiff)
15	06/16/2021	Proof of Service of Summons & Complaint - Unnamed Occupants filed by Doe, Jane.	Doe, Jane (Plaintiff)
16	08/09/2021	Notice and Acknowledgment of Receipt filed by Doe, Jane. Refers to: Health Center Partners of Southern California	Doe, Jane (Plaintiff)
17	08/16/2021	Stipulation - Other - Fee Due (Extending Time to Respond to Initial Complaint and Order) filed by Neighborhood Healthcare; Doe, Jane.	Neighborhood Healthcare (Defendant); Doe, Jane (Plaintiff)

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Telephone: (760) 929-9303
4 Facsimile: (760) 929-9260

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego
06/01/2021 at 04:40:18 PM
Clerk of the Superior Court
By Richard Day, Deputy Clerk

5 Attorneys for Plaintiff JANE DOE

6
7 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
8 **FOR THE COUNTY OF COUNTY OF SAN DIEGO**

9 JANE DOE, individually and on behalf of all
others similarly situated,

10 Plaintiff,

11 vs.

12 NEIGHBORHOOD HEALTHCARE; HEALTH
13 CENTER PARTNERS OF SOUTHERN
CALIFORNIA; NETGAIN TECHNOLOGY,
14 LLC; and DOE DEFENDANTS 1-100;

15 Defendants.
16

) Case No.: 37-2021-00023936-CU-BT-CTL
)

) **CLASS ACTION COMPLAINT FOR**
) **DAMAGES, RESTITUTION, AND**
) **INJUNCTIVE RELIEF FOR VIOLATIONS**
) **OF:**

-) (1) **THE CONFIDENTIALITY OF**
) **MEDICAL INFORMATION ACT,**
) **CIVIL CODE §§ 56, ET SEQ.;**
) (2) **BREACH OF CALIFORNIA**
) **SECURITY NOTIFICATION**
) **LAWS, CALIFORNIA CIVIL CODE**
) **§ 1798.82; AND**
) (3) **BUSINESS AND PROFESSIONS**
) **CODE §§ 17200, ET SEQ.**

) **JURY TRIAL DEMANDED**
)

17
18
19 Plaintiff Jane Doe (or “Plaintiff”), by and through her attorneys, bring this class action on
20 behalf of herself individually and all others similarly situated, against Defendants Neighborhood
21 Healthcare, Health Center Partners of Southern California, and Netgain Technology, LLC
22 (collectively referred to as “Defendants”), and alleges upon information and belief as follows:

23 **INTRODUCTION**

24 1. This class action arises from the negligent and failure of Defendants to properly
25 create, maintain, preserve, and/or store confidential, medical and personal identifying information
26 of Plaintiff¹ and all other persons similarly situated which allowed an unauthorized person to gain
27

28 ¹ California statutory law specifically allows a party to bring a lawsuit using a pseudonym in cases involving health care patients. Cal. Civ. Code § 3427.3 (West 2011). Specifically, section 3427.3

1 access to a computer database server of Defendants from October 22, 2020 to December 3, 2020,
2 causing unauthorized access, viewing, exfiltration, theft, and/or disclosure of unencrypted medical
3 and personal identifying information of Plaintiff and other persons similarly situated, to at least one
4 unauthorized person resulting in violations of the Confidentiality of Medical Information Act, Civil
5 Code §§ 56, *et seq.* (hereinafter referred to as the “Act”), the Security Notification Laws, Civil Code
6 § 1798.82, and the Business and Professions Code §§ 17200 *et seq.* Under the Act, Plaintiff, and
7 all other persons similarly situated, have the right to expect that the confidentiality of their medical
8 information in possession of Defendants and/or derived from Defendants to be reasonably
9 preserved and protected from unauthorized access, viewing, exfiltration, theft, and/or disclosure.

10 2. As alleged more fully below, failing to take adequate and reasonable measures to
11 ensure its data systems were protected against unauthorized intrusions, by failing to invest in cyber
12 security and data protection safeguards, failing to implement adequate and reasonable security
13 controls and user authorization and authentication processes, failing to limit the types of data
14 permitted to be transferred, failing to properly and adequately educate and train its employees, and
15 to put into place reasonable or adequate computer systems and security practices to safeguard
16 customers’ and patients’ medical and personal identifying information, Defendants negligently
17 created, maintained, preserved, and stored Plaintiff’s and the Class (defined *infra*) members’
18 medical and personal identifying information in possession of or derived from Defendants allowed
19 such information to be accessed and actually viewed by at least one unauthorized third party,
20 without Plaintiff’s and the Class members’ prior written authorization, which constitutes
21 unauthorized disclosure and/or release of their information in violation of Civil Code §§ 56.10(a)
22 and 56.101(a) of the Act. In fact, Defendant Health Center Partners of Southern California’s form

23
24
25 provides, “The court having jurisdiction over a civil proceeding under this title shall take all steps
26 ***reasonably necessary to safeguard the individual privacy and prevent harassment of a health care***
27 ***patient***, licensed health practitioner, or employee, client, or customer of a health care facility who is
28 a party or witness in the proceeding, including granting protective orders. ***Health care patients***,
licensed health practitioners, and employees, clients, and customers of the health care facility ***may***
use pseudonyms to protect their privacy.” Cal. Civ. Code § 3427.3 (emphasis added). Here, a
pseudonym has been used in place of the real name of Plaintiff because at all times relevant to this
action, Plaintiff is a health care patient under Civil Code § 56.05(k) and has individual privacy
concerns and a reasonable fear of harassment in light of the nature of the case.

1 letter, entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle, President &
2 Chief Executive Officer, Health Center Partners of Southern California, sent to Plaintiff and all
3 other persons similarly situated, informing them, in part, of “a recent data security incident
4 experienced by Netgain Technology, LLC (‘Netgain’), the IT service provider for Health Center
5 Partners of Southern California (‘HCP’)” and stating, in part, “HCP supports community health
6 centers in a variety of ways, including collaborative grant-funded programs and services for
7 Neighborhood Healthcare.... **What Happened:** Netgain recently informed HCP that it had
8 experienced a data security incident that involved systems containing HCP data.... According to
9 Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital
10 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
11 obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the
12 attacker in exchange for assurances that the attacker will delete all copies of this data and that it will
13 not publish, sell, or otherwise disclose the data.... The information involved varies depending on the
14 individual but may include the following: name, address, date of birth, diagnosis/treatment
15 information and treatment cost information. Once we learned that HCP data may have been
16 involved in the incident, we worked with our cybersecurity experts to review the impacted files and
17 identify the individuals whose information was contained in such files so that we may notify such
18 individuals. Our investigation revealed that the impacted files contained your personal information.”
19 An exemplar of Defendant Health Center Partners of Southern California’s “**Notice of Data**
20 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
21 as **Exhibit A.**

22 3. Additionally, Defendant Neighborhood Healthcare caused a form letter sent on its
23 behalf, entitled “**Notice of Data Breach,**” dated April 8, 2021, signed by Rakesh Patel, CEO,
24 Neighborhood Healthcare, stating, in part, “We are writing to make you aware of an issue brought
25 to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud
26 hosting and managed services provider. Neighborhood Healthcare used Netgain to host some
27 Neighborhood Healthcare files. **What Happened** On November 24, 2020, Netgain became aware
28 of a security incident that involved unauthorized access to portions of the Netgain environment and

1 Netgain client environments and began taking steps to investigate this incident. But, on December
2 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files
3 owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain
4 took additional measures to contain the threat and address the issue. Netgain’s technical teams
5 worked closely with third-party experts to remove the threat in the impacted environments and
6 confirm that client and internal systems are protected. Neighborhood Healthcare learned of the
7 ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to
8 believe that the protected health information (“PHI”) of our patients had been impacted in the
9 incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some
10 information including, potentially, some files containing patient PHI may have been impacted in the
11 incident. Netgain could not confirm, at that time, what records may have been impacted in the
12 incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood
13 Healthcare that Netgain believed were impacted by the attackers. Those files came from a
14 Neighborhood Healthcare server accessible by the Netgain environment. Since that time,
15 Neighborhood Healthcare has worked to review those records, to identify individuals impacted,
16 conduct an investigation into the incident with the assistance outside experts, and to transmit this
17 letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood
18 Healthcare determined that the impacted files included some of your information. **What**
19 **Information Was Involved** The information involved may have included some of the following:
20 your name, date of birth, address, Social Security Number and information about the care that you
21 received from Neighborhood Healthcare such as insurance coverage information, physician you
22 saw, and treatment codes.” An exemplar of Defendant Neighborhood Healthcare’s “**Notice of Data**
23 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
24 as **Exhibit B**.

25 4. Additionally, Defendant Netgain Technology, LLC stated in a blog post, entitled
26 “What we learned as a ransomware victim – so you don’t become one,” that “late last year, Netgain
27 was the victim of a criminal ransomware attack.... to become a victim of such an attack is both
28 humbling and galvanizing.... we identified additional opportunities to strengthn our security posture

1 in a continuous journey with an ongoing commitment to ensure this remains top-of-mind. As part
2 of our incident response, we have implemented a number of these identified enhancements to our
3 security posture and have continued to progress a multipronged approach. We've deployed new
4 tools, revised policies and enforcement procedures, and implemented an advanced around-the-clock
5 managed detections and response service for proactive threat monitoring.”

6 5. Because the individually identifiable medical information and other personal
7 identifying information of Plaintiff and the Class was subject to unauthorized access and viewing by
8 at least one unauthorized third party and in violation of the Act, Plaintiff, individually and on behalf
9 of all others similarly situated, seeks from Defendants nominal damages in the amount of one
10 thousand dollars (\$1,000) for each violation under Civil Code §56.36(b)(1) and actual damages,
11 according to proof, for each violation pursuant to Civil Code § 56.36(b)(2). Further, because
12 Plaintiff also alleges Defendants' conduct violates Business & Professions Code §§ 17200, *et seq.*,
13 Plaintiff, individually and on behalf of others similarly situated, seeks injunctive relief and
14 restitution from Defendants under Business and Professions Code § 17203.

15 6. This action, if successful, will enforce an important right affecting the public interest
16 and would confer a significant benefit, whether pecuniary or non-pecuniary, on a large class of
17 persons. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff
18 in relation to Plaintiff's stake in the matter, and therefore class certification is appropriate in this
19 matter.

20 **JURISDICTION AND VENUE**

21 7. This Court has jurisdiction over this action under California Code of Civil Procedure
22 § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class in the aggregate
23 exceeds the \$25,000 jurisdictional minimum of this Court. Further, the amount in controversy as to
24 Plaintiff individually does not exceed \$75,000.

25 8. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of
26 Civil Procedure §§ 395(a) and 395.5 because Defendant Neighborhood Healthcare is incorporated
27 in and does business in the State of California, and employs persons located in the County of San
28 Diego and in this judicial district. Defendants have obtained medical information of Plaintiff and

1 the Class in the transaction of business in the State of California and in this judicial district, which
2 has caused both obligations and liability of Defendants to arise in the State of California and in this
3 judicial district.

4 9. Further, this action does not qualify for federal jurisdiction under the Class Action
5 Fairness Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies
6 to this action because (1) more than two-thirds of the members of the proposed Class and SubClass
7 are citizens of the State of California, and (2) Defendants are citizens of the State of California.

8 **PARTIES**

9 **A. PLAINTIFF**

10 10. Plaintiff Jane Doe is and was at all times relevant to this action a resident of the State
11 of California and citizen of the State of California. At all times relevant to this action, Plaintiff
12 JANE DOE was a patient of, received medical treatment and diagnosis from, and provided her
13 personal information, including her name, address, date of birth, social security number, phone
14 number and email address to Defendant Neighborhood Healthcare. Additionally, Plaintiff received
15 a letter addressed to her, sent on Defendant Health Center Partners of Southern California's behalf,
16 entitled "**Notice of Data Breach,**" dated April 12, 2021, signed by Henry Tuttle, President & Chief
17 Executive Officer, Health Center Partners of Southern California, informing her, in part, of "a
18 recent data security incident experienced by Netgain Technology, LLC ('Netgain'), the IT service
19 provider for Health Center Partners of Southern California ('HCP')" and stating, in part, "HCP
20 supports community health centers in a variety of ways, including collaborative grant-funded
21 programs and services for Neighborhood Healthcare.... **What Happened:** Netgain recently
22 informed HCP that it had experienced a data security incident that involved systems containing
23 HCP data.... According to Netgain, in late September 2020, an unauthorized third party gained
24 access to Netgain's digital environment, and between October 22, 2020 to December 3, 2020, the
25 unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an
26 undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies
27 of this data and that it will not publish, sell, or otherwise disclose the data.... The information
28 involved varies depending on the individual but may include the following: name, address, date of

1 birth, diagnosis/treatment information and treatment cost information. Once we learned that HCP
2 data may have been involved in the incident, we worked with our cybersecurity experts to review
3 the impacted files and identify the individuals whose information was contained in such files so that
4 we may notify such individuals. Our investigation revealed that the impacted files contained your
5 personal information.” As a result, Plaintiff reasonably fears that disclosure and/or release of her
6 medical information created, maintained, preserved and/or stored on Defendants’ computer
7 networks could subject her to harassment or abuse.

8 **B. DEFENDANTS**

9 11. Defendant Neighborhood Healthcare (“NH”) is a California corporation, is registered
10 to do business and does business in the State of California (CA Corp. No. C0667935), with its
11 principal business office located at 1540 E. Valley Parkway, Escondido CA 92026, and with its
12 registered agent of service of process located at 150 La Terraza Blvd, Suite 201, Escondido CA
13 92025. On or about April 8, 2021, NH caused a form letter sent on its behalf, entitled “**Notice of**
14 **Data Breach,**” dated April 8, 2021, signed by Rakesh Patel, CEO, Neighborhood Healthcare, an
15 exemplar of which is attached hereto as **Exhibit B**, to be submitted to the Attorney General of the
16 State of California. At all times relevant to this action, NH was and is a provider of health care, a
17 contractor, and/or other authorized recipient of personal and confidential medical information, as
18 that term is defined and set forth in the Act, including the names, addresses, dates of birth,
19 diagnosis/treatment information and treatment cost information of Plaintiff and the SubClass
20 (defined *infra*), and is subject to the requirements and mandates of the Act, including but not limited
21 to Civil Code §§ 56.10, 56.101 and 56.36. At all times relevant to this action, NH was and is a
22 provider of health care and employed and employs persons located in the County of San Diego
23 and in this judicial district.

24 12. Defendant Health Center Partners of Southern California (“HCP”) is a business
25 entity doing business in the State of California, with its principal business office located at 3710
26 Ruffin Road, San Diego, CA 92123. On or about April 12, 2021, HCP caused a form letter sent on
27 its behalf, entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle,
28 President & Chief Executive Officer, Health Center Partners of Southern California, an exemplar of

1 which is attached hereto as **Exhibit A**, to be submitted to the Attorney General of the State of
2 California and to be mailed to Plaintiff and the Class. At all times relevant to this action, HCP was
3 and is a “business” within the meaning of Civil Code § 1798.140(c)(1), owns or licenses
4 computerized data which includes Plaintiff’s and the Class’ personal information, within the
5 meaning of Civil Code § 1798.82(h), collected Plaintiff’s and the Class’ personal information
6 within the meaning of Civil Code § 1798.81.5(d)(1)(A).

7 13. Defendant Netgain Technology, LLC (“NETGAIN”) is a business entity doing
8 business in the State of California, with its principal business office located at 5353 Mission Center
9 Road, Suite 202, San Diego, CA 92108. At all times relevant to this action, NETGAIN was and is
10 NH’s and HCP’s third-party vendor. On March 24, 2021, NETGAIN posted on its website a blog,
11 entitled “What we learned as a ransomware victim – so you don’t become one,” which stated, in
12 part, “In our case, late last year, Netgain was the victim of a criminal ransomware attack.... to
13 become a victim of such an attack is both humbling and galvanizing.... we identified additional
14 opportunities to strengthn our security posture in a continuous journey with an ongoing commitment
15 to ensure this remains top-of-mind. As part of our incident response, we have implemented a
16 number of these identified enhancements to our security posture and have continued to progress a
17 multipronged approach. We’ve deployed new tools, revised policies and enforcement procedures,
18 and implemented an advanced around-the-clock managed detections and response service for
19 proactive threat monitoring.”

20 **C. DOE DEFENDANTS**

21 14. The true names and capacities, whether individual, corporate, associate, or otherwise,
22 of Defendants sued herein as Doe Defendants 1 through 100, inclusive, are currently unknown to
23 Plaintiff, who therefore sue the Defendants by such fictitious names under the Code of Civil
24 Procedure § 474. Each of the Defendants designated herein as a Doe Defendant is legally
25 responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of
26 court and/or amend this complaint to reflect the true names and capacities of the Defendants
27 designated hereinafter as Doe Defendants 1 through 100 when such identities become known. Any
28

1 reference made to a named Defendant by specific name or otherwise, individually or plural, is also a
2 reference to the actions or inactions of Doe Defendants 1 through 100, inclusive.

3 **D. AGENCY/AIDING AND ABETTING**

4 15. At all times herein mentioned, Defendants, and each of them, were an agent or joint
5 venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the
6 course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the
7 acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized
8 the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

9 16. Defendants, and each of them, aided and abetted, encouraged and rendered
10 substantial assistance to the other Defendants in breaching their obligations to Plaintiff and the
11 Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially
12 assist the commissions of these wrongful acts and other wrongdoings complained of, each of the
13 Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its
14 conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals,
15 and wrongdoing.

16 **FACTUAL ALLEGATIONS**

17 17. As a result, at all times relevant to this action, including the period from October 22,
18 2020 to December 3, 2020, HCP possessed Plaintiff's and the Class' medical information, in
19 electronic and physical form, in possession of or derived from Defendant regarding their medical
20 history, mental or physical condition, or treatment. Such medical information included or contained
21 an element of personal identifying information sufficient to allow identification of Plaintiff and the
22 Class, such as their names, date of birth, addresses, medical record numbers, insurance provider,
23 electronic mail addresses, telephone numbers, or social security numbers, or other information that,
24 alone or in combination with other publicly available information, reveals their identity. At all
25 times relevant to this action, including the period from October 22, 2020 to December 3, 2020, HCP
26 maintained and continues to maintain "medical information," within the meaning of Civil Code §
27 56.05(j), of Plaintiff and the Class, each of which are "patients" within the meaning of Civil Code §
28 56.05(k).

1 18. As a result, at all times relevant to this action, including the period from October 22,
2 2020 to December 3, 2020, NH possessed Plaintiff’s and the SubClass’ medical information, in
3 electronic and physical form, in possession of or derived from Defendant regarding their medical
4 history, mental or physical condition, or treatment. Such medical information included or contained
5 an element of personal identifying information sufficient to allow identification of Plaintiff and the
6 SubClass, such as their names, date of birth, addresses, medical record numbers, insurance provider,
7 electronic mail addresses, telephone numbers, or social security numbers, or other information that,
8 alone or in combination with other publicly available information, reveals their identity. At all
9 times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH
10 maintained and continues to maintain “medical information,” within the meaning of Civil Code §
11 56.05(j), of Plaintiff and the SubClass, each of which are “patients” within the meaning of Civil
12 Code § 56.05(k). At all times relevant to this action, including the period from October 22, 2020 to
13 December 3, 2020, NH was and is a “provider of health care” within the meaning of Civil Code §
14 56.05(m). At all times relevant to this action, including the period from October 22, 2020 to
15 December 3, 2020, Plaintiff and SubClass members were patients, within the meaning of Civil Code
16 § 56.05(k).

17 19. As a result, at all times relevant to this action, including the period from October 22,
18 2020 to December 3, 2020, NETGAIN possessed Plaintiff’s, the SubClass’ and the Class’ medical
19 information, in electronic and physical form, in possession of or derived from Defendant regarding
20 their medical history, mental or physical condition, or treatment. Such medical information
21 included or contained an element of personal identifying information sufficient to allow
22 identification of Plaintiff, the SubClass and the Class, such as their names, date of birth, addresses,
23 medical record numbers, insurance provider, electronic mail addresses, telephone numbers, or social
24 security numbers, or other information that, alone or in combination with other publicly available
25 information, reveals their identity. At all times relevant to this action, including the period from
26 October 22, 2020 to December 3, 2020, NETGAIN maintained and continues to maintain “medical
27 information,” within the meaning of Civil Code § 56.05(j), of Plaintiff and the Class, each of which
28 are “patients” within the meaning of Civil Code § 56.05(k).

1 20. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, pursuant to Civil Code § 56.06(a), HCP, as a business that created, maintained,
3 preserved, and stored records of the care, products and services that Plaintiff and the Class members
4 received in the State of California from HCP’s over 16 member community health centers, 140
5 member practice sites, 857,757 patients served, and/or other providers of health care, health care
6 service plans, pharmaceutical companies, and contractors, as defined by the Act, is and was
7 organized for the purpose of maintaining medical information, within the meaning of Civil Code §
8 56.05(j), in order to make the information available to Plaintiff and the Class members or to a
9 provider of health care at the request of Plaintiff and the Class members or a provider of health care,
10 for purposes of allowing Plaintiff and the Class members to manage their information, or for the
11 diagnosis and treatment of Plaintiff and the Class members, is and was deemed to be a “provider of
12 health care,” within the meaning of Civil Code § 56.05(m).

13 21. Alternatively, at all times relevant to this action, including the period from October
14 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), HCP, as an entity that is a
15 medical group, independent practice association, pharmaceutical benefits manager, or a medical
16 service organization, and is not a health care service plan or provider of health care to Plaintiff and
17 the Class members, is and was a “contractor” under Civil Code § 56.05(d).

18 22. Alternatively, at all times relevant to this action, including the period from October
19 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, HCP is and was a recipient of
20 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
21 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
22 further disclosing that medical information except in accordance with a new authorization that
23 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
24 of this chapter or by law.

25 23. Alternatively, at all times relevant to this action, including the period from October
26 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, HCP is and was a recipient of
27 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
28 the Act, and was prohibited from further disclosing such medical information unless in accordance

1 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
2 permitted by other provisions of this chapter or by law.

3 24. Additionally, at all times relevant to this action, including prior to the period from
4 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), HCP is and was an entity
5 engaged in the business of furnishing administrative services to programs that provide payment for
6 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
7 or permitting its employees or agents to use or disclose Plaintiff's and the Class members' medical
8 information possessed in connection with performing administrative functions for a program, except
9 as reasonably necessary in connection with the administration or maintenance of the program, or as
10 required by law, or with an authorization.

11 25. As a provider of health care, a contractor, and/or other authorized recipient of
12 personal and confidential medical information, HCP is required by the Act to ensure that medical
13 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
14 patients' authorization, and to protect and preserve the confidentiality of the medical information
15 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

16 26. At all times relevant to this action, including the period from October 22, 2020 to
17 December 3, 2020, pursuant to Civil Code § 56.06(a), NH, as a business that created, maintained,
18 preserved, and stored records of the care, products and services that Plaintiff and the Class members
19 received in the State of California from NH and/or other providers of health care, health care service
20 plans, pharmaceutical companies, and contractors, as defined by the Act, is and was organized for
21 the purpose of maintaining medical information, within the meaning of Civil Code § 56.05(j), in
22 order to make the information available to Plaintiff and the Class members or to a provider of health
23 care at the request of Plaintiff and the Class members or a provider of health care, for purposes of
24 allowing Plaintiff and the Class members to manage their information, or for the diagnosis and
25 treatment of Plaintiff and the Class members, is and was deemed to be a "provider of health care,"
26 within the meaning of Civil Code § 56.05(m).

27 27. Alternatively, at all times relevant to this action, including the period from October
28 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), NH, as an entity that is a medical

1 group, independent practice association, pharmaceutical benefits manager, or a medical service
2 organization, and is not a health care service plan or provider of health care to Plaintiff and the
3 Class members, is and was a “contractor” under Civil Code § 56.05(d).

4 28. Alternatively, at all times relevant to this action, including the period from October
5 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NH is and was a recipient of
6 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
7 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
8 further disclosing that medical information except in accordance with a new authorization that
9 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
10 of this chapter or by law.

11 29. Alternatively, at all times relevant to this action, including the period from October
12 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NH is and was a recipient of
13 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
14 the Act, and was prohibited from further disclosing such medical information unless in accordance
15 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
16 permitted by other provisions of this chapter or by law.

17 30. Additionally, at all times relevant to this action, including prior to the period from
18 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), NH is and was an entity
19 engaged in the business of furnishing administrative services to programs that provide payment for
20 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
21 or permitting its employees or agents to use or disclose Plaintiff’s and the Class members’ medical
22 information possessed in connection with performing administrative functions for a program, except
23 as reasonably necessary in connection with the administration or maintenance of the program, or as
24 required by law, or with an authorization.

25 31. As a provider of health care, a contractor, and/or other authorized recipient of
26 personal and confidential medical information, NH is required by the Act to ensure that medical
27 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
28

1 patients' authorization, and to protect and preserve the confidentiality of the medical information
2 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

3 32. At all times relevant to this action, including the period from October 22, 2020 to
4 December 3, 2020, pursuant to Civil Code § 56.06(a), NETGAIN, as a business that created,
5 maintained, preserved, and stored records of the care, products and services that Plaintiff and the
6 Class members received in the State of California from NH and/or other providers of health care,
7 health care service plans, pharmaceutical companies, and contractors, as defined by the Act, is and
8 was organized for the purpose of maintaining medical information, within the meaning of Civil
9 Code § 56.05(j), in order to make the information available to Plaintiff and the Class members or to
10 a provider of health care at the request of Plaintiff and the Class members or a provider of health
11 care, for purposes of allowing Plaintiff and the Class members to manage their information, or for
12 the diagnosis and treatment of Plaintiff and the Class members, is and was deemed to be a "provider
13 of health care," within the meaning of Civil Code § 56.05(m).

14 33. Alternatively, at all times relevant to this action, including the period from October
15 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NETGAIN is and was a recipient of
16 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
17 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
18 further disclosing that medical information except in accordance with a new authorization that
19 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
20 of this chapter or by law.

21 34. Alternatively, at all times relevant to this action, including the period from October
22 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NETGAIN is and was a recipient
23 of medical information of Plaintiff and the Class members pursuant to an authorization as provided
24 by the Act, and was prohibited from further disclosing such medical information unless in
25 accordance with a new authorization that meets the requirements of Section 56.21, or as specifically
26 required or permitted by other provisions of this chapter or by law.

27 35. As a provider of health care and/or other authorized recipient of personal and
28 confidential medical information, NETGAIN is required by the Act to ensure that medical

1 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
2 patients' authorization, and to protect and preserve the confidentiality of the medical information
3 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

4 36. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, HCP created, maintained, preserved, and stored records of the care, services and
6 products, including the names, addresses, dates of birth, diagnosis/treatment information and
7 treatment cost information of Plaintiff and the Class (all of which constitutes medical information,
8 as that term is defined and set forth in the Act), that Plaintiff and other Class members received in
9 the State of California from NH and other HCP providers of health care on its computer server.

10 37. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, NH created, maintained, preserved, and stored records of the care, services and
12 products, including the names, addresses, dates of birth, diagnosis/treatment information and
13 treatment cost information of Plaintiff and the SubClass (all of which constitutes medical
14 information, as that term is defined and set forth in the Act), that Plaintiff and other SubClass
15 members received in the State of California from NH on its computer network.

16 38. As a result, on or before October 30, 2020, Defendants possessed Plaintiff's,
17 SubClass' and the Class' medical information, in electronic and physical form, in possession of or
18 derived from Defendants regarding their medical history, mental or physical condition, or treatment.
19 Such medical information included or contained an element of personal identifying information
20 sufficient to allow identification of Plaintiff, the SubClass and the Class, such as their names,
21 addresses, dates of birth, social security numbers, phone numbers and/or email addresses, or other
22 information that, alone or in combination with other publicly available information, reveals their
23 identity.

24 39. As providers of health care, contractors, and/or other recipients of medical
25 information, Defendants are required by the Act to ensure that medical information regarding a
26 patient is not disclosed or disseminated or released without their patients' authorization, and to
27 protect and preserve the confidentiality of the medical information regarding a patient, under Civil
28 Code §§ 56.10, 56.26, 56.36, and 56.101.

1 40. As providers of health care, contractors, and/or other recipients of medical
2 information, Defendants are required by the Act not to disclose medical information regarding a
3 patient without first obtaining an authorization under Civil Code §§ 56.10 and 56.26.

4 41. As providers of health care, contractors, and/or other recipients of medical
5 information, Defendants are required by the Act to create, maintain, preserve, and store medical
6 information in a manner that preserves the confidentiality of the information contained therein
7 under Civil Code § 56.101(a).

8 42. As providers of health care, contractors, and/or other recipients of medical
9 information, Defendants are required by the Act to protect and preserve confidentiality of electronic
10 medical information of Plaintiff and the Class in its possession under Civil Code § 56.101(b)(1)(A).

11 43. As providers of health care, contractors, and/or other recipients of medical
12 information, Defendants are required by the Act to take appropriate preventive actions to protect the
13 confidential information or records against release consistent with Defendants' obligations under
14 the Act, under Civil Code § 56.36(e)(2)(E), or other applicable state law, and the Health Insurance
15 Portability and Accountability Act of 1996 (Public Law 104-191) (HIPAA) and all HIPAA
16 Administrative Simplification Regulations in effect on January 1, 2012, contained in Parts 160, 162,
17 and 164 of Title 45 of the Code of Federal Regulations, and Part 2 of Title 42 of the Code of
18 Federal Regulations, including, but not limited to, all of the following:

- 19 i. Developing and implementing security policies and procedures.
- 20 ii. Designating a security official who is responsible for developing and implementing
21 its security policies and procedures, including educating and training the workforce.
- 22 iii. Encrypting the information or records, and protecting against the release or use of
23 the encryption key and passwords, or transmitting the information or records in a
24 manner designed to provide equal or greater protections against improper
25 disclosures.

26 44. At all times relevant to this action, including the period from October 22, 2020 to
27 December 3, 2020, HCP created, maintained, preserved, and stored Plaintiff's and the Class
28 members' medical information in an un-encrypted format.

1 45. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, NH created, maintained, preserved, and stored Plaintiff’s and the SubClass
3 members’ medical information in an un-encrypted format.

4 46. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, NH disclosed and/or delivered Plaintiff’s and the SubClass members’ medical
6 information to HCP and NETGAIN. At all times relevant to this action, NH did not obtain written
7 authorization from the Plaintiff and the SubClass prior to disclosing and/or delivering Plaintiff’s and
8 the SubClass members’ medical information to HCP and NETGAIN. Furthermore, NH’s disclosure
9 of and/or delivery of Plaintiff’s and the SubClass members’ medical information to HCP and
10 NETGAIN was not permissible without written authorization from the Plaintiff and the SubClass or
11 under any exemption under Civil Code § 56.10(c).

12 47. At all times relevant to this action, including the period from October 22, 2020 to
13 December 3, 2020, HCP created, maintained, preserved, stored, disclosed and/or delivered
14 Plaintiff’s and the Class members’ medical information to NETGAIN on its computer servers. At
15 all times relevant to this action, HCP did not obtain written authorization from the Plaintiff and the
16 Class prior to creating, maintaining, preserving, storing, disclosing and/or delivering Plaintiff’s and
17 the Class members’ medical information to NETGAIN on its computer servers. Furthermore,
18 NETGAIN’s disclosure of and/or delivery of Plaintiff’s and the Class members’ medical
19 information to NETGAIN on its computer servers was not permissible without written authorization
20 from the Plaintiff and the Class or under any exemption under Civil Code § 56.10(c).

21 48. By law, the HIPAA Privacy Rule applies only to covered entities, e.g. health care
22 providers. However, most health care providers do not carry out all of their health care activities
23 and functions by themselves. Instead, they often use the services of a variety of other persons or
24 businesses. The Privacy Rule allows covered providers to disclose protected health information
25 (PHI) to these “business associates” if the providers obtain assurances that the business associate
26 will use the information only for the purposes for which it was engaged by the covered entity, will
27 safeguard the information from misuse, and will help the covered entity comply with some of the
28 covered entity’s duties under the Privacy Rule. Covered entities may disclose PHI to an entity in its

1 role as a business associate only to help the covered entity carry out its health care functions – not
2 for the business associate’s independent use or purposes, except as needed for the proper
3 management and administration of the business associate. The Privacy Rule requires that a covered
4 entity obtain assurances from its business associate that the business associate will appropriately
5 safeguard the PHI it receives or creates on behalf of the covered entity. The satisfactory assurances
6 must be in writing, whether in the form of a contract or other agreement between the covered entity
7 and the business associate.

8 49. When hiring and monitoring a service provider or business associate such as
9 NETGAIN, HCP and NH knew or should have known that they had a duty to inquire about
10 potential service providers’ and business associates’ cybersecurity programs and how such
11 programs are maintained. HCP and NH knew or should have known that they had a duty to
12 compare potential service providers’ and business associates’ cybersecurity programs to the
13 industry standards adopted by other healthcare providers, and should evaluate potential service
14 providers’ track records in the industry by reviewing public information about data security
15 incidents and litigation. HCP and NH knew or should have known that they had a duty to also ask
16 potential service providers and business associates about whether they have experienced any
17 cybersecurity incidents and how such incidents were handled, as well as whether the potential
18 service provider has an insurance policy in place that would cover losses caused by cybersecurity
19 breaches (including losses caused by internal and external threats). HCP and NH knew or should
20 have known that they had a duty to review service provider and business associates contracts to
21 ensure that the contracts require the service providers to comply, on an ongoing basis, with
22 cybersecurity and information security standards (and avoid contract provisions that limit service
23 providers’ responsibility for cybersecurity and information technology breaches). Finally, HCP and
24 NH knew or should have known that they had a duty to pay particular attention to contract terms
25 relating to confidentiality, the use and sharing of information, notice by the vendor of cybersecurity
26 risk assessments and audit reports, cybersecurity breaches and records retention and destruction.

27 50. Alternatively, Plaintiff alleges on information and belief that HCP’s and NH’s
28 disclosure of and/or delivery of Plaintiff’s, the Class’ and the SubClass’ medical information to

1 NETGAIN was either without a business associate agreement or pursuant to a business associate
2 agreement that was not permissible under the Privacy Rule or any exemption under Civil Code §
3 56.10(c), and/or because HCP and NH negligently failed to obtain reasonable assurances and
4 negligently failed to monitor and conduct assessments of NETGAIN to verify that NETGAIN
5 would comply with HIPAA privacy regulations and to follow guidelines and policies to maintain
6 the privacy, confidentiality, including by encryption, and otherwise reasonably protect Plaintiff’s
7 and the Class’ medical information from disclosure and/or release to at least one unauthorized third
8 party “user” prior to and after HCP’s and NH’s disclosure of and/or delivery of Plaintiff’s and the
9 Class members’ medical information to NETGAIN.

10 51. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, at least one “unauthorized third party gained access to Netgain’s digital
12 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
13 obtained certain files” containing including Plaintiff’s, the SubClass’ and the Class’ medical
14 information (i.e., their names, addresses, dates of birth, diagnosis/treatment information and
15 treatment cost information) that was located on a NETGAIN server in an un-encrypted format, as
16 represented in HCP’s “**Notice of Data Breach**” form letter submitted to the Attorney General of the
17 State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**.

18 52. Defendants had the resources necessary to protect and preserve confidentiality of
19 electronic medical information of Plaintiff, the SubClass and the Class in their possession, but
20 neglected to adequately implement data security measures as required by HIPPA and the Act,
21 despite their obligation to do so.

22 53. Additionally, the risk of vulnerabilities in its computer and data systems of being
23 exploited by an unauthorized third party trying to steal Plaintiff’s, the SubClass’ and the Class’
24 electronic personally identifying and medical information was foreseeable and/or known to
25 Defendants. The California Data Breach Report 2012-2015, issued in February 2016 by Attorney
26 General, Kamala D. Harris, reported, “Malware and hacking presents the greatest threat, both in the
27 number of breaches and the number of records breached” and “Social Security numbers and
28 medical information – was breached than other data types.” Moreover, as Attorney General further

1 reported, just because “[e]xternal adversaries cause most data breaches, [] this does not mean that
2 organizations are solely victims; they are also stewards of the data they collect and maintain. People
3 entrust businesses and other organizations with their data on the understanding that the
4 organizations have a both an ethical and a legal obligation to protect it from unauthorized access.
5 Neglecting to secure systems and data opens a gateway for attackers, who take advantage of
6 uncontrolled vulnerabilities.” Regarding encryption, Attorney General instructed in California Data
7 Breach Report 2012-2015, “As we have said in the past, breaches of this type are preventable.
8 Affordable solutions are widely available: strong full-disk encryption on portable devices and
9 desktop computers when not in use.[] Even small businesses that lack full time information security
10 and IT staff can do this. They owe it to their patients, customers, and employees to do it now.”

11 54. More recently the HIPAA Journal posted on November 1, 2018 warned, “Healthcare
12 organization[s] need to ensure that their systems are well protected against cyberattacks, which
13 means investing in technologies to secure the network perimeter, detect intrusions, and block
14 malware and phishing threats.”

15 55. Further, it also was foreseeable and/or known to Defendants that negligently
16 creating, maintaining, preserving, and/or storing Plaintiff’s, the SubClass’ and the Class’ medical
17 and personal identifying information, in electronic form, onto Defendants’ computer networks in a
18 manner that did not preserve the confidentiality of the information could have a devastating effect
19 on them. As reported in the California Data Breach Report 2012-2015, “There are real costs to
20 individuals. Victims of a data breach are more likely to experience fraud than the general public,
21 according to Javelin Strategy & Research. In 2014, 67 percent of breach victims in the U.S. were
22 also victims of fraud, compared to just 25 percent of all consumers.”

23 56. To be successful, phishing relies on a series of affirmative acts by a company and its
24 employees such as clicking a link, downloading a file, or providing sensitive information. Once
25 criminals gained access to the email accounts of a company and its employees, the email servers
26 communicated—that is, disclosed—the contents of those accounts to the criminals. “Phishing
27 scams are one of the most common ways hackers gain access to sensitive or confidential
28 information. Phishing involves sending fraudulent emails that appear to be from a reputable

1 company, with the goal of deceiving recipients into either clicking on a malicious link or
2 downloading an infected attachment, usually to steal financial or confidential information.”
3 (<https://www.varonis.com/blog/data-breach-statistics/>). As posted on April 21, 2020, the FBI had
4 issued a fresh warning [Alert Number MI-000122-MW] following an increase in COVID-19
5 phishing scams targeting healthcare providers.

6 57. At all times relevant to this action, including the period from October 22, 2020 to
7 December 3, 2020, Defendants negligently created, maintained, preserved, and/or stored Plaintiff’s,
8 the SubClass’ and the Class’ medical information, including Plaintiff’s, the SubClass’ and the
9 Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
10 information, in electronic form, onto Defendants’ computer networks in a manner that did not
11 preserve the confidentiality of the information, and negligently failed to protect and preserve
12 confidentiality of electronic medical information of Plaintiff, the SubClass and the Class in their
13 possession, as required by HIPPA and the Act, and specifically, under Civil Code §§ 56.10(a),
14 56.26(a), 56.36(e)(2)(E), 56.101(a), and 56.101(b)(1)(A), and according to their written
15 representations to Plaintiff and the Class.

16 58. Had Defendants taken such appropriate preventive actions, fix the deficiencies in
17 their data security systems and adopted security measures as required by HIPPA and the Act from
18 October 22, 2020 to December 3, 2020, Defendants could have prevented Plaintiff’s and the Class’
19 electronic medical information within Defendants’ computer networks from being accessed and
20 actually viewed by unauthorized third parties.

21 59. At all times relevant to this action, including the period of from October 22, 2020 to
22 December 3, 2020, NH, by disclosing and/or delivering Plaintiff’s and the SubClass’ personal
23 identifying and medical information to HCP, allowed Plaintiff’s and the SubClass’ personal
24 identifying and medical information to be accessed and actually viewed by at least one unauthorized
25 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
26 Code § 56.10(a).

27 60. At all times relevant to this action, including the period of from October 22, 2020 to
28 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic

1 medical information of Plaintiff and the SubClass on NETGAIN's computer server, allowed
2 Plaintiff's and the SubClass' medical and personal identifying information to be accessed and
3 actually viewed by at least one unauthorized third party, without first obtaining an authorization,
4 constituting a disclosure in violation of Civil Code § 56.10(a).

5 61. At all times relevant to this action, including the period from October 22, 2020 to
6 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
7 medical information of Plaintiff and the Class on NETGAIN's computer server, allowed Plaintiff's
8 and the Class' medical and personal identifying information to be accessed and actually viewed by
9 at least one unauthorized third party, without first obtaining an authorization, constituting a
10 disclosure in violation of Civil Code § 56.10(a).

11 62. At all times relevant to this action, including the period from October 22, 2020 to
12 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
13 medical information of Plaintiff and the Class on NETGAIN's computer server, allowed Plaintiff's
14 and the Class' medical and personal identifying information to be accessed and actually viewed by
15 at least one unauthorized third party, without first obtaining an authorization, constituting a
16 disclosure in violation of Civil Code § 56.26(a).

17 63. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, NH, by disclosing and/or delivering Plaintiff's and the SubClass members'
19 medical and personal identifying information to HCP, allowed Plaintiff's and the SubClass' medical
20 and personal identifying information to be accessed and actually viewed by at least one
21 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

22 64. At all times relevant to this action, including the period from October 22, 2020 to
23 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic
24 medical information of Plaintiff and the SubClass on NETGAIN's computer server, allowed
25 Plaintiff's and the SubClass' medical and personal identifying information to be accessed and
26 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
27 Code § 56.101(a).

28

1 65. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
3 medical information of Plaintiff and the Class on NETGAIN’s computer server, allowed Plaintiff’s
4 and the Class’ medical and personal identifying information to be accessed and actually viewed by
5 at least one unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

6 66. At all times relevant to this action, including the period from October 22, 2020 to
7 December 3, 2020, NH, by disclosing and/or delivering Plaintiff’s and the SubClass members’
8 medical and personal identifying information to HCP, allowed Plaintiff’s and the SubClass’ medical
9 and personal identifying information to be accessed and actually viewed by at least one
10 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

11 67. At all times relevant to this action, including the period from October 22, 2020 to
12 December 3, 2020, NH’s negligent failure to protect and preserve confidentiality of electronic
13 medical information of Plaintiff and the SubClass, on NETGAIN’s computer server, allowed
14 Plaintiff’s and the SubClass’ medical and personal identifying information to be accessed and
15 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
16 Code § 56.101(b)(1)(A).

17 68. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, HCP’s negligent failure to protect and preserve confidentiality of electronic
19 medical information of Plaintiff and the Class, on NETGAIN’s computer server, allowed Plaintiff’s
20 and the Class’ medical and personal identifying information to be accessed and actually viewed by
21 at least one unauthorized third party, constituting a release in violation of Civil Code §
22 56.101(b)(1)(A).

23 69. On or about April 12, 2021, HCP caused a form letter, entitled “**Notice of Data**
24 **Breach,**” dated April 12, 2021, signed by Henry Tuttle, President & Chief Executive Officer,
25 Health Center Partners of Southern California, to be mailed to Plaintiff and the Class, informing
26 them, in part, of “a recent data security incident experienced by Netgain Technology, LLC
27 (‘Netgain’), the IT service provider for Health Center Partners of Southern California (‘HCP’)” and
28 stating, in part, “HCP supports community health centers in a variety of ways, including

1 collaborative grant-funded programs and services for Neighborhood Healthcare.... **What**
2 **Happened:** Netgain recently informed HCP that it had experienced a data security incident that
3 involved systems containing HCP data.... According to Netgain, in late September 2020, an
4 unauthorized third party gained access to Netgain’s digital environment, and between October 22,
5 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data.
6 Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the
7 attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the
8 data.... The information involved varies depending on the individual but may include the following:
9 name, address, date of birth, diagnosis/treatment information and treatment cost information. Once
10 we learned that HCP data may have been involved in the incident, we worked with our
11 cybersecurity experts to review the impacted files and identify the individuals whose information
12 was contained in such files so that we may notify such individuals. Our investigation revealed that
13 the impacted files contained your personal information.” An exemplar of HCP’s “**Notice of Data**
14 **Breach**” form letter submitted to the Attorney General of the State of California and mailed to
15 Plaintiff and the Class is attached hereto as **Exhibit A**. Plaintiff received in the mail a HCP “**Notice**
16 **of Data Breach**” form letter, addressed to her, which alerted Plaintiff that her medical and personal
17 identifying information, along with other Class members, was improperly accessed by at least one
18 unauthorized third party. As a result, Plaintiff fears that disclosure and/or release of her medical
19 and personal identifying information created, maintained, preserved, and/or stored on Defendants’
20 computer networks could subject her to harassment or abuse. Moreover, although thereafter, on
21 May 4, 2021, Plaintiff wrote both HCP and NH separately requesting further information about this
22 security incident, neither HCP nor NH provided a substantive response to her requests.

23 70. HCP’s “**Notice of Data Breach**” form letter submitted to the Attorney General of
24 the State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**, further
25 states, “**What We Are Doing:** [] We are providing you with steps that you can take to help protect
26 your personal information, and as an added precaution, we are offering you complimentary identity
27 protection services through IDX, a leader in risk mitigation and response.”

28

1 71. HCP’s “**Notice of Data Breach**” form letter concludes by making the following
2 hollow gesture, “The security of your information is a top priority for HCP, and we are committed
3 to safeguarding your data and privacy.” Other than offering “steps that you can take to help protect
4 your personal information” and “complimentary identity protection services through IDX” “as an
5 added precaution,” HCP’s “**Notice of Data Breach**” form letter does nothing to further protect
6 Plaintiff and the Class from future incidents of identity theft despite the severity of the unauthorized
7 access, viewing, exfiltration, theft, disclosure and/or release of their electronic medical and personal
8 information caused by Defendants’ violations of their duty to implement and maintain reasonable
9 security procedures and practices.

10 72. To date, other than offering “steps that you can take to help protect your personal
11 information” and “complimentary identity protection services through IDX” “as an added
12 precaution,” HCP has not offered any monetary compensation for the unauthorized disclosure
13 and/or release of Plaintiff’s and the Class’ electronic medical information under the Act. In effect,
14 HCP is shirking its responsibility for the harm it has caused, while shifting the burdens and costs of
15 its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

16 73. To date, NH has not offered any compensation for the unauthorized disclosure and/or
17 release of Plaintiff’s and SubClass’ electronic medical information under the Act. In effect, NH is
18 shirking its responsibility for the harm it has caused, while shifting the burdens and costs of its
19 wrongful conduct onto its patients, i.e. Plaintiff and the SubClass.

20 74. To date, NETGAIN has not offered any monetary compensation for the unauthorized
21 disclosure and/or release of Plaintiff’s and the Class’ electronic medical information under the Act.
22 In effect, NETGAIN is shirking its responsibility for the harm it has caused, while shifting the
23 burdens and costs of its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

24 75. Based upon the information posted on the U.S. Department of Health and Human
25 Services’ official website, HCP reported on “04/09/2021” a “Hacking/IT Incident” involving
26 “Network Server” affecting “293,516” persons, which involved a “Business Associate,” to the U.S.
27 Department of Health & Human Services’ Office for Civil Rights.

28

1 76. Based upon the information posted on the U.S. Department of Health and Human
2 Services' official website, NH reported on "04/14/2021" a "Hacking/IT Incident" involving
3 "Network Server" affecting "45,200" persons, which involved a "Business Associate," to the U.S.
4 Department of Health & Human Services' Office for Civil Rights.

5 77. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA
6 covered entities to provide notification following a breach of unsecured protected health
7 information. Following a breach of unsecured protected health information, covered entities must
8 provide notification of the breach to affected individuals. Covered entities must *only* provide the
9 required notifications if the breach involved unsecured protected health information. Unsecured
10 protected health information is protected health information (PHI) that has not been rendered
11 unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or
12 methodology specified by the Secretary of the U.S. Department of Health and Human Services in
13 guidance. Under approved guidance of the U.S. Department of Health and Human Services, PHI is
14 rendered unusable, unreadable, or indecipherable to unauthorized individuals if (1) electronic PHI
15 has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process
16 to transform data into a form in which there is a low probability of assigning meaning without use
17 of a confidential process or key" (45 CFR 164.304 definition of encryption) and (2) such
18 confidential process or key that might enable decryption has not been breached. By reporting this
19 incident to the U.S. Department of Health and Human Services, HCP and NH each has separately
20 determined and is affirming that Plaintiff's, the Class' and the SubClass' electronic PHI was either
21 not encrypted at all, or if it was encrypted, the encryption has been breached by the unauthorized
22 third party. Further, because Plaintiff's, the Class' and the SubClass' identifiable medical
23 information contained in NETGAIN's computer server was not rendered unusable, unreadable, or
24 indecipherable, the unauthorized third party or parties who "obtained" and downloaded Plaintiff's
25 and the Class' identifiable medical information was able to and did actually view Plaintiff's, the
26 Class' and the SubClass' electronic medical information contained in and "obtained" and
27 downloaded from NETGAIN's computer server. As a result, HCP and NH each has separately
28 determined and have affirmed that Plaintiff's, the Class' and the SubClass' identifiable medical

1 information contained in NETGAIN’s computer server was unencrypted and thus, the unauthorized
2 third party or parties who “obtained” and downloaded Plaintiff’s, the Class’ and the SubClass’
3 identifiable medical information was able to and did actually view Plaintiff’s, the Class’ and the
4 SubClass’ electronic medical information contained in and “obtained” and downloaded from
5 NETGAIN’s computer server. Therefore, HCP, NH and NETGAIN was negligent for failing to
6 encrypt or adequately encrypt Plaintiff’s, the Class’ and the SubClass’ electronic medical
7 information contained in NETGAIN’s computer server.

8 78. As a result, Defendants were negligent for failing to encrypt or adequately encrypt
9 Plaintiff’s, the Class’ and the SubClass’ electronic medical information on their computer networks.
10 Further, because Plaintiff’s, the Class’ and the SubClass’ identifiable medical information on
11 Defendants’ computer networks was not rendered unusable, unreadable, or indecipherable, the
12 unauthorized third party or parties who accessed Plaintiff’s, the Class’ and the SubClass’
13 identifiable medical information was able to and did view Plaintiff’s, the Class’ and the SubClass’
14 electronic medical information contained within NETGAIN’s computer server.

15 CLASS ACTION ALLEGATIONS

16 79. Plaintiff brings this action on behalf of herself individually and on behalf of all
17 others similarly situated. The putative class and subclass that Plaintiff seeks to represent is defined
18 as follows:

19 Class: All persons to whom Health Center Partners of Southern California sent a
20 notification letter of a data security incident that has occurred between October
21 22, 2020 to December 3, 2020, an exemplar of which is attached hereto as
Exhibit A.

22 SubClass: All persons to whom Neighborhood Healthcare sent a notification
23 letter of a data security incident that has occurred between November 24, 2020 to
December 3, 2020, an exemplar of which is attached hereto as **Exhibit B**.

24 The officers, directors, employees, and agents of Defendants and any “affiliate,” “principal” or
25 “subsidiary” of Defendants, as defined in the Corporations Code §§ 150, 175, and 189, respectively,
26 are excluded from the Class and the SubClass. Plaintiff reserves the right under California Rule of
27 Court 3.765 to amend or modify the Class definition with greater particularity or further division
28

1 into subclasses or limitation to particular issues as warranted, and as additional facts are discovery
2 by Plaintiff during her future investigations.

3 80. This action is properly maintainable as a class action. The members of the Class and
4 the SubClass are so numerous that joinder of all members is impracticable, if not completely
5 impossible. While the exact number of the Class is unknown to Plaintiff at this time, HCP filed a
6 report with the U.S. Department of Health & Human Services' Office for Civil Rights, on or about
7 December 28, 2020, that this incident affected 293,516 persons. The disposition of the claims of
8 the members of Class through this class action will benefit both the parties and this Court. In
9 addition, the Class and the SubClass is readily identifiable from information and records in the
10 possession of Defendants and their agents, and the Class and the SubClass is defined in objective
11 terms that make the eventual identification of the Class and the SubClass members possible and/or
12 sufficient to allow members of the Class and the SubClass identify themselves as having a right to
13 recover.

14 81. There is a well-defined community of interest among the members of the Class and
15 the SubClass because common questions of law and fact predominate, Plaintiff's claims are typical
16 of the members of the class, and Plaintiff can fairly and adequately represent the interests of the
17 Class.

18 82. Common questions of law and fact exist as to all members of the Class and the
19 SubClass and predominate over any questions affecting solely individual members of the Class and
20 the SubClass. Among the questions of law and fact common to the Class that predominate over
21 questions which may affect individual Class members, including the following:

- 22 a) Whether Defendants possessed Plaintiff's, the SubClass' and the Class' medical and
23 personal identifying information from October 22, 2020 to December 3, 2020;
24 b) Whether Defendants created, maintained, preserved and/or stored Plaintiff's, the
25 SubClass' and the Class' medical and personal identifying information, in electronic
26 form, onto Defendants' computer networks from October 22, 2020 to December 3,
27 2020;

- 1 c) Whether Defendants implemented and maintained reasonable security procedures
2 and practices to protect Plaintiff's, the SubClass' and the Class' medical and
3 personal identifying information, in electronic form, within Defendants' computer
4 networks from October 22, 2020 to December 3, 2020;
- 5 d) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
6 information, in electronic form, within Defendants' computer networks from October
7 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
8 exposed by an unauthorized third party;
- 9 e) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
10 information, in electronic form, within Defendants' computer networks from October
11 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
12 exposed by an unauthorized third party without the prior written authorization of
13 Plaintiff, the SubClass and the Class, as required by Civil Code §§ 56.10 and 56.26;
- 14 f) Whether Defendants' creation, maintenance, preservation and/or storage of
15 Plaintiff's, the SubClass' and the Class' medical and personal identifying
16 information, in electronic form, within Defendants' computer networks, accessed,
17 viewed, exfiltrated and/or publicly exposed by an unauthorized third party was
18 permissible without written authorization from Plaintiff, the SubClass and the Class
19 or under any exemption under Civil Code § 56.10(c);
- 20 g) Whether Defendants' creation, maintenance, preservation and/or storage of
21 Plaintiff's, the SubClass' and the Class' medical and personal identifying
22 information, in electronic form, within Defendants' computer networks, accessed,
23 viewed, exfiltrated and/or publicly exposed by an unauthorized third party
24 constitutes a release in violation of Civil Code §56.101;
- 25 h) Whether the timing of HCP's notice that Plaintiff's and the Class' medical and
26 personal identifying information, in electronic form, was accessed, viewed,
27 exfiltrated and/or publicly exposed by an unauthorized third party, was given in the
28 most expedient time possible and without reasonable delay;

1 i) Whether Defendants' conduct constitute unlawful, fraudulent or unfair practices in
2 violation of Business and Professions Code §§ 17200, *et seq.*; and

3 j) Whether Plaintiff, the SubClass and the Class are entitled to actual, nominal or
4 statutory damages, injunctive relief and/or restitution.

5 83. Plaintiff's claims are typical of those of the other SubClass and Class members
6 because Plaintiff, like every other SubClass and Class member, were exposed to virtually identical
7 conduct and now suffer from the same violations of the law as other SubClass and Class members.

8 84. Plaintiff will fairly and adequately protect the interests of the SubClass and the
9 Class. Moreover, Plaintiff has no interest that is contrary to or in conflict with those of the
10 SubClass and the Class, she seeks to represent. In addition, Plaintiff has retained competent counsel
11 experienced in class action litigation to further ensure such protection and intend to prosecute this
12 action vigorously.

13 85. The nature of this action and the nature of laws available to Plaintiff and the other
14 SubClass and Class members make the use of the class action format a particularly efficient and
15 appropriate procedure to afford relief to Plaintiff and the other SubClass and Class members for the
16 claims alleged and the disposition of whose claims in a class action will provide substantial benefits
17 to both the parties and the Court because:

18 a) If each of the SubClass and the Class members were required to file an individual
19 lawsuit, the Defendants would necessarily gain an unconscionable advantage since
20 they would be able to exploit and overwhelm the limited resources of each individual
21 member of the SubClass and Class with its vastly superior financial and legal
22 resources;

23 b) The costs of individual suits could unreasonably consume the amounts that would be
24 recovered;

25 c) Proof of a common business practice or factual pattern which Plaintiff experienced is
26 representative of that experienced by the SubClass and the Class and will establish
27 the right of each of the members to recover on the causes of action alleged;

28

1 d) Individual actions would create a risk of inconsistent results and would be
2 unnecessary and duplicative of this litigation; and

3 e) The disposition of the claims of the members of the SubClass and the Class through
4 this class action will produce salutary by-products, including a therapeutic effect
5 upon those who indulge in fraudulent practices, and aid to legitimate business
6 enterprises by curtailing illegitimate competition.

7 86. The prosecution of separate actions by individual members of the SubClass and the
8 Class would create a risk of inconsistent or varying adjudications with respect to individual
9 members of the SubClass and the Class, which would establish incompatible standards of conduct
10 for the Defendants in the State of California and would lead to repetitious trials of the numerous
11 common questions of fact and law in the State of California. Plaintiff knows of no difficulty that
12 will be encountered in the management of this litigation that would preclude its maintenance as a
13 class action. As a result, a class action is superior to other available methods for the fair and
14 efficient adjudication of this controversy.

15 87. Notice to the members of the SubClass and the Class may be made by e-mail or first-
16 class mail addressed to all persons who have been individually identified by Defendants and who
17 have been given notice of the data breach.

18 88. Plaintiff, the SubClass and the Class have suffered irreparable harm and damages
19 because of Defendants' wrongful conduct as alleged herein. Absent certification, Plaintiff, the
20 SubClass and the Class will continue to be damaged and to suffer by the unauthorized disclosure
21 and/or release of their medical and personal identifying information, thereby allowing these
22 violations of law to proceed without remedy.

23 89. Moreover, Plaintiff's, the SubClass' and the Class' individual damages are
24 insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendants'
25 violations of law inflicting substantial damages in the aggregate would go unremedied. In addition,
26 Defendants have acted or refused to act on grounds generally applicable to Plaintiff, the SubClass
27 and the Class, thereby making appropriate final injunctive relief with respect to, the Class as a
28 whole.

FIRST CAUSE OF ACTION
Violations of the Confidentiality of Medical Information Act
California Civil Code §§ 56, et seq.
(On Behalf of Plaintiff and the SubClass Against NH)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

90. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if fully stated herein.

91. At all times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH is considered a “provider of health care,” within the meaning of Civil Code § 56.05(m), and maintained and continues to maintain “medical information” within the meaning of Civil Code § 56.05(j), of Plaintiff and the SubClass.

92. Plaintiff and the SubClass are “patients” of NH within the meaning of Civil Code § 56.05(k) and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure and/or release of their medical information could subject them to harassment or abuse.

93. At all times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH negligently created, maintained, preserved, and/or stored Plaintiff’s and the SubClass’ medical information, including Plaintiff’s and the SubClass’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in electronic form, onto Defendants’ computer networks in a manner that did not preserve the confidentiality of the information, and negligently failed to protect and preserve confidentiality of electronic medical information of Plaintiff and the SubClass in its possession, as required by the Act, and specifically, under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and 56.36(e)(2)(E), and according to their written representations to Plaintiff and the SubClass.

94. Due to NH’s disclosure and/or delivery Plaintiff’s and the SubClass members’ medical and personal identifying information to HCP without written authorization from Plaintiff and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff’s and the SubClass’ medical information, including Plaintiff’s and the SubClass’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be accessed and actually viewed by at least one unauthorized third party, without first obtaining an

1 authorization, constituting a disclosure in violation of Civil Code §§ 56.10, 56.13, 56.245, and
2 56.26(a).

3 95. Due to NH's negligent creation, maintenance, preservation and/or storage of
4 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server, NH
5 allowed Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass'
6 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
7 electronic form, to be accessed and actually viewed by at least one unauthorized third party, without
8 first obtaining an authorization, constituting a disclosure in violation of Civil Code §§ 56.10, 56.13,
9 56.245, and 56.26(a).

10 96. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass members'
11 medical and personal identifying information to HCP without written authorization from Plaintiff
12 and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff's and
13 the SubClass' medical information, including Plaintiff's and the SubClass' names, addresses, dates
14 of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be
15 accessed and actually viewed by at least one unauthorized third party, constituting a release in
16 violation of Civil Code § 56.101(a).

17 97. Due to NH's negligent creation, maintenance, preservation and/or storage of
18 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server,
19 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
20 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
21 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
22 constituting a release in violation of Civil Code § 56.101(a).

23 98. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass' medical
24 information and personal identifying information to HCP without written authorization from
25 Plaintiff and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed
26 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
27 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
28

1 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
2 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

3 99. Due to NH's negligent creation, maintenance, preservation and/or storage of
4 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server, NH
5 allowed Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass'
6 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
7 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
8 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

9 100. As a result of NH's above-described conduct in violation of the Act, Plaintiff and the
10 SubClass have suffered damages from the unauthorized disclosure and/or release of their medical
11 and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

12 101. As a result of NHs' above-described conduct in violation of the Act, Plaintiff and the
13 SubClass seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
14 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
15 Code § 56.36(b)(2).

16 **SECOND CAUSE OF ACTION**
17 **Violations of the Confidentiality of Medical Information Act**
18 **California Civil Code §§ 56, et seq.**
19 **(On Behalf of Plaintiff and the Class Against HCP)**

20 102. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
21 fully stated herein.

22 103. At all times relevant to this action, including the period from October 22, 2020 to
23 December 3, 2020, HCP is considered a "provider of health care" within the meaning of Civil Code
24 § 56.05(m), a "contractor" under Civil Code § 56.05(d), and/or "engaged in the business of
25 furnishing administrative services to programs that provide payment for health care services" under
26 Civil Code § 56.26(a), and maintained and continues to maintain "medical information" within the
27 meaning of Civil Code § 56.05(j), of Plaintiff and the Class.
28

1 104. Plaintiff and the Class are “patients” within the meaning of Civil Code § 56.05(k)
2 and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure
3 and/or release of their medical information could subject them to harassment or abuse.

4 105. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, HCP negligently created, maintained, preserved, and/or stored Plaintiff’s and the
6 Class’ medical information, including Plaintiff’s and the Class’ names, addresses, dates of birth,
7 diagnosis/treatment information and treatment cost information, in electronic form, onto
8 NETGAIN’s computer server in a manner that did not preserve the confidentiality of the
9 information, and negligently failed to protect and preserve confidentiality of electronic medical
10 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
11 under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
12 56.36(e)(2)(E).

13 106. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
14 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
15 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
16 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
17 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
18 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
19 Code §§ 56.10, 56.13, 56.245, and 56.26(a).

20 107. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
21 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
22 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
23 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
24 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
25 third party, constituting a release in violation of Civil Code § 56.101(a).

26 108. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
27 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
28 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s

1 and the Class' names, addresses, dates of birth, diagnosis/treatment information and treatment cost
2 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
3 third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

4 109. As a result of HCP's above-described conduct in violation of the Act, Plaintiff and
5 the Class have suffered damages from the unauthorized disclosure and/or release of their medical
6 and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

7 110. As a result of HCP's above-described conduct in violation of the Act, Plaintiff and
8 the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
9 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
10 Code § 56.36(b)(2).

11 **THIRD CAUSE OF ACTION**
12 **Violations of the Confidentiality of Medical Information Act**
13 **California Civil Code §§ 56, et seq.**
14 **(On Behalf of Plaintiff and the Class Against NETGAIN)**

15 111. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
16 fully stated herein.

17 112. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, NETGAIN is considered a "provider of health care" within the meaning of Civil
19 Code § 56.05(m), and maintained and continues to maintain "medical information" within the
20 meaning of Civil Code § 56.05(j), of Plaintiff and the Class.

21 113. Plaintiff and the Class are "patients" within the meaning of Civil Code § 56.05(k)
22 and are "Endanger" within the meaning of Civil Code § 56.05(e) because they fear that disclosure
23 and/or release of their medical information could subject them to harassment or abuse.

24 114. At all times relevant to this action, including the period from October 22, 2020 to
25 December 3, 2020, NETGAIN negligently created, maintained, preserved, and/or stored Plaintiff's
26 and the Class' medical information, including Plaintiff's and the Class' names, addresses, dates of
27 birth, diagnosis/treatment information and treatment cost information, in electronic form, onto
28 NETGAIN's computer server in a manner that did not preserve the confidentiality of the
information, and negligently failed to protect and preserve confidentiality of electronic medical

1 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
2 under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
3 56.36(e)(2)(E).

4 115. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
5 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
6 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
7 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
8 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
9 unauthorized third party, without first obtaining an authorization, constituting a disclosure in
10 violation of Civil Code §§ 56.10, 56.13, 56.245, and 56.26(a).

11 116. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
12 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
13 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
14 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
15 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
16 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

17 117. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
18 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
19 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
20 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
21 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
22 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

23 118. As a result of NETGAIN's above-described conduct in violation of the Act, Plaintiff
24 and the Class have suffered damages from the unauthorized disclosure and/or release of their
25 medical and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

26 119. As a result of NETGAIN's above-described conduct in violation of the Act, Plaintiff
27 and the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
28

1 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
2 Code § 56.36(b)(2).

3 **FOURTH CAUSE OF ACTION**
4 **Breach of California Security Notification Laws**
5 **California Civil Code § 1798.82**
6 **(On Behalf of Plaintiff and the Class Against HCP)**

7 120. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
8 fully stated herein.

9 121. Pursuant to Civil Code § 1798.82(a), “A person or business that conducts business in
10 California, and that owns or licenses computerized data that includes personal information, shall
11 disclose a breach of the security of the system following discovery or notification of the breach in
12 the security of the data to a resident of California (1) whose unencrypted personal information was,
13 or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted
14 personal information was, or is reasonably believed to have been, acquired by an unauthorized
15 person and the encryption key or security credential was, or is reasonably believed to have been,
16 acquired by an unauthorized person and the person or business that owns or licenses the encrypted
17 information has a reasonable belief that the encryption key or security credential could render that
18 personal information readable or usable. The disclosure shall be made in the most expedient time
19 possible and without unreasonable delay, consistent with the legitimate needs of law enforcement,
20 as provided in subdivision (c), or any measures necessary to determine the scope of the breach and
21 restore the reasonable integrity of the data system.” Prior to passages of such statute, the California
22 State Assembly cited an incident where authorities knew of the breach in security for 21 days
23 “before state workers were told” as an example of “late notice.”

24 122. Civil Code § 1798.82 further provides, “(h) For purposes of this section, ‘personal
25 information’ means an individual’s first name or first initial and last name in combination with any
26 one or more of the following data elements, when either the name or the data elements are not
27 encrypted: (1) Social security number. (2) Driver’s license number or California Identification Card
28 number. (3) Account number, credit or debit card number, in combination with any required
security code, access code, or password that would permit access to an individual's financial

1 account. (4) Medical information. (5) Health insurance information. (i) (2) For purposes of this
2 section, ‘medical information’ means any information regarding an individual’s medical history,
3 mental or physical condition, or medical treatment or diagnosis by a health care professional. (3)
4 For purposes of this section, ‘health insurance information’ means an individual’s health insurance
5 policy number or subscriber identification number, any unique identifier used by a health insurer to
6 identify the individual, or any information in an individual’s application and claims history,
7 including any appeals records.”

8 123. HCP conducts business in California and owns or licenses computerized data which
9 includes the personal information, within the meaning of Civil Code § 1798.82(h), of Plaintiff and
10 the Class.

11 124. Based upon NH’s “**Notice of Data Breach**” form letter, HCP was aware that
12 Plaintiff’s and the Class’ unencrypted personal information on NETGAIN’s computer server was,
13 or is reasonably believed to have been, acquired by an unauthorized person no later than December
14 3, 2020, but did not begin to mail notification letters to Plaintiff and the Class until April 12, 2021.
15 Thus, HCP waited at least 131 days before *beginning* to inform Plaintiff and the Class of this
16 incident and the subsequent threat to Plaintiff’s and the Class’ personal information. As a result,
17 HCP did not disclose to Plaintiff and the Class that their personal information was, or was
18 reasonably believed to have been, acquired by an unauthorized person, in the most expedient time
19 possible and without reasonable delay in violation of Civil Code § 1798.82(a). Given the example
20 of the Legislature finding that a delay of 21 days to be “late notice” under the statute, HCP’s delay
21 of 131 days before *beginning* to inform Plaintiff and the Class that their personal information was,
22 or was reasonably believed to have been, acquired by an unauthorized person by mailing HCP’s
23 form letter to Plaintiff and the Class is presumptively unreasonable notice in violation of Civil Code
24 § 1798.82(a).

25 125. Plaintiff and the Class have been injured by fact that HCP did not disclose their
26 personal information was, or was reasonably believed to have been, acquired by an unauthorized
27 person in the most expedient time possible and without reasonable delay in violation of Civil Code
28 § 1798.82(a). HCP’s delays in informing required by Civil Code § 1798.82(a) and providing all of

1 the information required by Civil Code § 1798.82(d) to Plaintiff and the Class that their personal
2 information was, or was reasonably believed to have been, acquired by an unauthorized person,
3 have prevented Plaintiff and the Class from taking steps to protect their personal information from
4 unauthorized use and/or identify theft.

5 126. Plaintiff and the Class seek recovery of their damages pursuant to Civil Code §
6 1798.84(b) and injunctive relief pursuant to Civil Code § 1798.84(e).

7 **FIFTH CAUSE OF ACTION**
8 **Unlawful and Unfair Business Acts and Practices in Violation of**
9 **California Business & Professions Code §17200, *et seq.***
10 **(On Behalf of Plaintiff, the SubClass and the Class Against All Defendants)**

11 127. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
12 fully stated herein.

13 128. The acts, misrepresentations, omissions, practices, and non-disclosures of
14 Defendants as alleged herein constituted unlawful and unfair business acts and practices within the
15 meaning of California Business & Professions Code §§ 17200, *et seq.*

16 129. By the aforementioned business acts or practices, Defendants have engaged in
17 “unlawful” business acts and practices in violation of the aforementioned statutes, including Civil
18 Code §§ 56.10(a), 56.26(a), 56.36(e)(2)(E), 56.101(a), 56.101(b)(1)(A), 1798.82(a) and 1798.82(d).
19 Plaintiff reserves the right to allege other violations of law committed by Defendants which
20 constitute unlawful acts or practices within the meaning of California Business & Professions Code
21 §§ 17200, *et seq.*

22 130. By the aforementioned business acts or practices, Defendants have also engaged in
23 “unfair” business acts or practices in that the harm caused by Defendants’ failure to maintain
24 adequate information security procedures and practices, including but not limited to, failing to take
25 adequate and reasonable measures to ensure its data systems were protected against unauthorized
26 intrusions, failing to properly and adequately educate and train its employees, failing to put into
27 place reasonable or adequately computer systems and security practices to safeguard patients’
28 identifiable medical information including access restrictions and encryption, failing to have
adequate privacy policies and procedures in place that did not preserve the confidentiality of the

1 medical and personal identifying information of Plaintiff, the SubClass and the Class in their
2 possession, and failing to protect and preserve confidentiality of electronic medical information of
3 Plaintiff, the SubClass and the Class in their possession against disclosure and/or release, outweighs
4 the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous,
5 unethical, deceitful and offensive, and causes substantial injury to Plaintiff, the SubClass and the
6 Class.

7 131. Defendants have obtain money and property from Plaintiff, the SubClass and the
8 Class because of the payment of the services and products they received from Defendants. Plaintiff,
9 the SubClass and the Class have suffered an injury in fact by acquiring less in their transactions
10 with Defendants for the services and products they received from Defendants than they otherwise
11 would have if Defendants would had adequately protected the confidentiality of their medical and
12 personal identifying information.

13 132. Pursuant to the Business & Professions Code § 17203, Plaintiff, the SubClass and the
14 Class seek an order of this Court requiring Defendants awarding Plaintiff and the Class restitution
15 of monies wrongfully acquired by Defendants in the form of payments for services by means of
16 such unlawful, fraudulent and unfair business acts and practices, so as to restore any and all monies
17 to Plaintiff, the SubClass and the Class which were acquired and obtained by means of such
18 unlawful, fraudulent and unfair business acts and practices, which ill-gotten gains are still retained
19 by Defendants.

20 133. The aforementioned unlawful, fraudulent and unfair business acts or practices
21 conducted by Defendants have been committed in the past and continues to this day. Defendants
22 have failed to acknowledge the wrongful nature of their actions. Defendants have not corrected or
23 publicly issued comprehensive corrective notices to Plaintiff, the SubClass and the Class, and have
24 not corrected or enacted adequate privacy policies and procedures to protect and preserve
25 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
26 Class in their possession.

27
28

1 134. Because of Defendants' aforementioned conduct, Plaintiff, the SubClass and the
2 Class have no other adequate remedy of law in that absent injunctive relief from the Court and
3 Defendants are likely to continue to injure Plaintiff, the SubClass and the Class.

4 135. Pursuant to Business & Professions Code § 17203, Plaintiff, the SubClass and the
5 Class also seek an order of this Court for equitable and/or injunctive relief in the form of requiring
6 Defendants to correct its illegal conduct that is necessary and proper to prevent Defendants from
7 repeating their illegal and wrongful practices as alleged above and protect and preserve
8 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
9 Class in Defendants' possession that has already been accessed, viewed, exfiltrated and/or publicly
10 exposed by at least one unauthorized third party because by way of Defendants' illegal and
11 wrongful practices set forth above. Pursuant to Business & Professions Code § 17203, Plaintiff, the
12 SubClass and the Class further seek an order of this Court for equitable and/or injunctive relief in
13 the form of requiring Defendants to publicly issue comprehensive corrective notices.

14 136. Because this case is brought for the purposes of enforcing important rights affecting
15 the public interest, Plaintiff, the SubClass and the Class also seek the recovery of attorneys' fees
16 and costs in prosecuting this action against Defendants under Code of Civil Procedure § 1021.5 and
17 other applicable law.

18 **PRAYER FOR RELIEF**

19 WHEREFORE, Plaintiff respectfully request that the Court grant Plaintiff and the proposed
20 SubClass and Class the following relief against Defendants, and each of them:

21 **As for the First, Second and Third Causes of Action**

- 22 1. For nominal damages in the amount of one thousand dollar (\$1,000) per violation to Plaintiff
23 individually and to each member of the SubClass and the Class pursuant to Civil Code §
24 56.36(b)(1);
- 25 2. For actual damages according to proof per violation pursuant to Civil Code § 56.36(b)(2);

26 **As for the Fourth Cause of Action**

- 27 3. For damages according to proof to Plaintiff individually and to each member of the Class
28 pursuant to California Civil Code § Civil Code § 1798.84(b);

1 4. For injunctive relief pursuant to California Civil Code § Civil Code § 1798.84(e);

2 **As for the Fifth Cause of Action**

3 5. For an order awarding Plaintiff, the SubClass and the Class restitution of all monies
4 wrongfully acquired by Defendants by means of such unlawful, fraudulent and unfair
5 business acts and practices;

6 6. For injunctive relief in the form of an order instructing Defendants to prohibit the
7 unauthorized release of medical and personal identifying information of Plaintiff, the
8 SubClass and the Class, and to adequately maintain the confidentiality of the medical and
9 personal identifying information of Plaintiff and the Class;

10 7. For injunctive relief in the form of an order enjoining Defendants from disclosing the
11 medical and personal identifying information of Plaintiff, the SubClass and the Class
12 without the prior written authorization of each Plaintiff, the SubClass and the Class member;

13 **As to All Causes of Action**

14 8. That the Court issue an Order certifying this action be certified as a class action on behalf of
15 the proposed SubClass and Class, appointing Plaintiff as representative of the proposed
16 SubClass and Class, and appointing Plaintiff's attorneys, as counsel for members of the
17 proposed SubClass and Class;

18 9. For an award of attorneys' fees as authorized by statute, including, but not limited to, the
19 provisions of California Code of Civil Procedure § 1021.5, and as authorized under the
20 "common fund" doctrine, and as authorized by the "substantial benefit" doctrine;

21 10. For costs of the suit;

22 11. For prejudgment interest at the legal rate; and

23 12. Any such further relief as this Court deems necessary, just, and proper.

24 Dated: June 1, 2021

KEEGAN & BAKER LLP

25
26 By:



Patrick N. Keegan, Esq.
Attorney for Plaintiff

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

Plaintiff, the SubClass and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

Dated: June 1, 2021

KEEGAN & BAKER LLP

By: 
Patrick N. Keegan, Esq.
Attorney for Plaintiff

Exhibit A



C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE



NAME

ADDRESS1

ADDRESS2

CSZ

COUNTRY



SEQ
CODE 2D
Ver 1

BREAK

To Enroll, Please Call:
1-833-416-0926
Or Visit:
<https://response.idx.us/hcp-netgain-incident>
Enrollment Code: <<XXXXXXXXXX>>

April 12, 2021

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by Netgain Technology, LLC (“Netgain”), the IT service provider for Health Center Partners of Southern California (“HCP”). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTHCENTER>>. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, we engaged our own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, our health center members and partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain’s cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

Once we learned that HCP data may have been involved in the incident, we worked with our cybersecurity experts to review the impacted files and identify the individuals whose information was contained in such files so that we may notify such individuals. Our investigation revealed that the impacted files contained your personal information. **Again, we are not aware of any misuse of your personal information as a result of this incident.** Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your information.

What Information Was Involved: The information involved varies depending on the individual but may include the following: <<VARPARAGRAPH>>.

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, we have reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and we are committed to assisting their investigation into the matter.

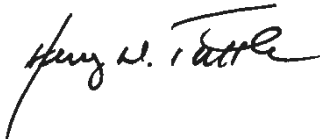
We are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include **xx** months of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What You Can Do: As we have stated, we are not aware of any misuse of your information as a result of this incident. However, we encourage you to follow the recommendations on the next page to help protect your information. We also encourage you to enroll in the complimentary services offered by going to <https://response.idx.us/hcp-netgain-incident> or calling 1-833-416-0926 and using the enrollment code provided above. Please note that the deadline to enroll is July 12, 2021.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-833-416-0926 between 6:00 a.m. and 6:00 p.m. Pacific Time.

The security of your information is a top priority for HCP, and we are committed to safeguarding your data and privacy.

Sincerely,

A handwritten signature in black ink, appearing to read "Henry W. Tuttle". The signature is written in a cursive, flowing style.

Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
www.consumer.ftc.gov ,	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
and	1-888-743-0023	1-877-566-7226	1-401-274-4400
www.ftc.gov/idtheft			
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Exhibit B



C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 903-3642
Or Visit:
<https://response.idx.us/nhc-netgain-incident>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

April 8, 2021

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

The privacy and security of your personal information is very important to Neighborhood Healthcare. We are writing to make you aware of an issue brought to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud hosting and managed services provider. Neighborhood Healthcare used Netgain to host some Neighborhood Healthcare files.

What Happened

On November 24, 2020, Netgain became aware of a security incident that involved unauthorized access to portions of the Netgain environment and Netgain client environments and began taking steps to investigate this incident. But, on December 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files owned by Netgain and Netgain's clients and disrupting Netgain's operations. In response, Netgain took additional measures to contain the threat and address the issue. Netgain's technical teams worked closely with third-party experts to remove the threat in the impacted environments and confirm that client and internal systems are protected.

Neighborhood Healthcare learned of the ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to believe that the protected health information ("PHI") of our patients had been impacted in the incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some information including, potentially, some files containing patient PHI may have been impacted in the incident. Netgain could not confirm, at that time, what records may have been impacted in the incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood Healthcare that Netgain believed were impacted by the attackers. Those files came from a Neighborhood Healthcare server accessible by the Netgain environment. Since that time, Neighborhood Healthcare has worked to review those records, to identify individuals impacted, conduct an investigation into the incident with the assistance outside experts, and to transmit this letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood Healthcare determined that the impacted files included some of your information.

What Information Was Involved

The information involved may have included some of the following: your name, date of birth, address, Social Security Number and information about the care that you received from Neighborhood Healthcare such as insurance coverage information, physician you saw, and treatment codes. Neighborhood Healthcare is offering credit monitoring services to you at no charge. Please see the **What You Can Do** section below for information about these services including how to enroll. Please also see the **Additional Important Information** section below for further precautionary measures you may wish to take. Netgain has received assurances that the data has not gone beyond the attacker, that the data was not and will not be misused, and that the data will not be disseminated or otherwise be made publicly available.

What We Are Doing

Please know that we take this incident and the security of your personal information very seriously. Ensuring the safety of our patients' data is of the utmost importance to us. Since we learned of this incident, we have been working with Netgain to seek assurances that they are taking appropriate steps to respond to this incident. We have also conducted an investigation of the incident with the help of outside experts, and we have transitioned to a new hosting provider (a transition that was already in process when this incident occurred).

In addition, we are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include <<12/24 months>> of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What Netgain Is Doing

Netgain took several steps to strengthen its environment following the incident, including international Geo-fencing for Azure-hosted environments, deploying additional log monitoring across all servers, and additional hardening of network security rules and protocols to restrict lateral movement across environments. Netgain stated that it paid a significant amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

What You Can Do

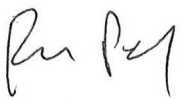
We recommend that you review the additional information enclosed. Additionally, we encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 903-3642 or going to <https://response.idx.us/nhc-netgain-incident> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 8, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

We very much regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, please call (833) 903-3642, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely



Rakesh Patel
CEO
Neighborhood Healthcare

Additional Important Information

1. Website and Enrollment. Go to <https://response.idx.us/nhc-netgain-incident> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 903-3642 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Generally. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing financial account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state's Attorney General.

5. The FTC. You can obtain information from Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

6. Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

7. Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788 equifax.com/personal/credit-report-services/ 800-525-6285	Experian Security Freeze P.O. Box 9554 Allen, TX 75013-9544 experian.com/freeze/center.html 888-397-3742	TransUnion (FVAD) P.O. Box 160 Woodlyn, PA 19094 transunion.com/credit-freeze 888-909-8872
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

More information can also be obtained by contacting the Federal Trade Commission listed above.

8. Protecting Medical Information: To date, we have no reason to believe that your PHI potentially involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following steps can help protect you from medical identity theft issues.

- Do not share health insurance cards with anyone apart from your care providers and other family members who are covered under the insurance plan or who help you with your medical care.
- Review the “explanation of benefits statements” that you receive from your health insurance company. If you see something amiss, follow up with your insurance company or the health care provider identified on the explanation of benefits to request further information.
- Ask your health insurance company for a report on all services they have paid for you for the current year. If you do not recognize an item in that list, speak with your insurance company to verify it.

9. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Tel: (760) 929-9303
4 Fax: (760) 929-9260

ELECTRONICALLY RECEIVED
Superior Court of California,
County of San Diego
06/02/2021 at 02:51:43 PM
Clerk of the Superior Court
By Kristin Sorianosos, Deputy Clerk

5 Attorney for Plaintiff
6 JANE DOE
7

8 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
9 **FOR THE COUNTY OF SAN DIEGO**

10 JANE DOE, individually and on behalf of all others
11 similarly situated,

12 Plaintiff,

13 vs.

14 NEIGHBORHOOD HEALTHCARE; HEALTH
CENTERS PARTNERS OF SOUTHERN
15 CALIFORNIA; NETGAIN TECHNOLOGY, LLC;
and DOE DEFENDANTS 1-100;

16 Defendants.
17

Case No. 37-2021-00023936-CU-BT-CTL

CLASS ACTION

Assigned to: Hon. Joel R. Wohlfeil, Dept. C-73

**[PROPOSED] ORDER GRANTING
PLAINTIFF'S EX PARTE APPLICATION TO
APPEAR BY PSEUDONYM**

Date: June 8, 2021

Time: 8:30 a.m.

Place: Department C-73

IMAGED FILE

18 Plaintiff Jane Doe's application for an order allowing Plaintiff to appear by pseudonym in this matter,
19 came *ex parte* for hearing on June 8, 2021, at 8:30 a.m. in Department C-73 before the Honorable Joel R.
20 Wohlfeil, and the Court, having reviewed Plaintiff Jane Doe's application and for good cause appearing
21 therefore, hereby orders as follows:

22 **IT IS HEREBY ORDERED THAT:**

23 Plaintiff Jane Doe alleges she was a patient within the meaning of Civil Code § 56.05(k). As such,
24 she is authorized by Civil Code § 3427.3 to use a pseudonym in this action to protect her privacy.
25

26 Dated: _____

27 _____
Hon. Joel R. Wohlfeil
Judge of the Superior Court
28

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar number, and address): Patrick Keegan, 167698 Keegan & Baker, LLP 2292 Faraday Avenue, Suite 100 Carlsbad, CA 92008 TELEPHONE NO.: (760)929-9303 Ext 100 ATTORNEY FOR (Name): Plaintiff	FOR COURT USE ONLY ELECTRONICALLY FILED Superior Court of California, County of San Diego 06/16/2021 at 11:34:00 AM Clerk of the Superior Court By E- Filing, Deputy Clerk
SUPERIOR COURT OF CALIFORNIA, COUNTY OF Superior Court of California, San Diego County 330 W. Broadway San Diego, CA 92101-3409	
PLAINTIFF/PETITIONER: JANE DOE, et al DEFENDANT/RESPONDENT: Neighborhood Healthcare. et al	CASE NUMBER: 37-2021-00023936-CU-BT-CTL
<p style="text-align: center;">PROOF OF SERVICE OF SUMMONS</p>	Ref. No. or File No.: 5187-Netgain

BY FAX

1. At the time of service I was a citizen of the United States, at least 18 years of age and not a party to this action.
2. I served copies of: Summons, Civil Case Cover Sheet, Class Action Complaint, Notice of Case Assignment and Case Management Conference, Alternative Dispute Resolution (ADR) Information, Stipulation to Use Alternative Dispute Resolution (ADR), Plaintiff's Ex Parte Application for an Order for Plaintiff to Appear by Pseudonym, Minute Order, Order Granting Plaintiff's Ex Parte Application to Appear by Pseudonym,
3. a. Party served: Neighborhood Healthcare

 b. Person Served: Sallie Barnett - Person Authorized to Accept Service of Process
4. Address where the party was served: 150 La Terraza Blvd, Ste. 201
 Escondido, CA 92025
5. I served the party
 b. **by substituted service.** On (date): 06/11/2021 at (time): 2:07PM I left the documents listed in item 2 with or in the presence of: Michelle Olmeda - Person In Charge Of Office
 (1) (business) a person at least 18 years of age apparently in charge at the office or usual place of business of the person to be served. I informed him or her of the general nature of the papers.
 (4) A declaration of mailing is attached.
6. The "Notice to the Person Served" (on the summons) was completed as follows:
 d. on behalf of:
 Neighborhood Healthcare

 under: CCP 416.10 (corporation)
7. **Person who served papers**
 a. Name: Tom Reinhardt
 b. Address: One Legal - P-000618-Sonoma
 1400 North McDowell Blvd, Ste 300
 Petaluma, CA 94954
 c. Telephone number: 415-491-0606
 d. The fee for service was: \$ 197.50
 e. I am:
 (3) registered California process server.
 (i) Employee or independent contractor.
 (ii) Registration No. P121764
 (iii) County San Diego
8. I declare under penalty of perjury under the laws of the United States of America and the State of California that the foregoing is true and correct.

Date: 06/15/2021

Tom Reinhardt

(NAME OF PERSON WHO SERVED PAPERS)



(SIGNATURE)

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name and Address): Patrick Keegan, 167698 Keegan & Baker, LLP 2292 Faraday Avenue, Suite 100 Carlsbad, CA 92008 ATTORNEY FOR (Name): Plaintiff	TELEPHONE NO.: (760)929-9303 Ext 100 Ref. No. or File No. 5187-Netgain	FOR COURT USE ONLY	
Insert name of court, judicial district or branch court, if any: Central - Civil 330 W. Broadway San Diego, CA 92101-3409			
PLAINTIFF: JANE DOE, et al			
DEFENDANT: Neighborhood Healthcare, et al			
PROOF OF SERVICE BY MAIL			CASE NUMBER: 37-2021-00023936-CU-BT-CTL

BY FAX

I am a citizen of the United States, over the age of 18 and not a party to the within action. My business address is 1400 N. McDowell Blvd, Petaluma, CA 94954.

On 06/16/2021, after substituted service under section CCP 415.20(a) or 415.20(b) or FRCP 4(e)(2)(B) or FRCP 4(h)(1)(B) was made (if applicable), I mailed copies of the:

Summons, Civil Case Cover Sheet, Class Action Complaint, Notice of Case Assignment and Case Management Conference, Alternative Dispute Resolution (ADR) Information, Stipulation to Use Alternative Dispute Resolution (ADR), Plaintiff's Ex Parte Application for an Order for Plaintiff to Appear by Pseudonym, Minute Order, Order Granting Plaintiff's Ex Parte Application to Appear by Pseudonym,

to the person to be served at the place where the copies were left by placing a true copy thereof enclosed in a sealed envelope, with First Class postage thereon fully prepaid, in the United States Mail at Petaluma, California, addressed as follows:

Neighborhood Healthcare

Sallie Barnett

150 La Terraza Blvd, Ste. 201

Escondido, CA 92025

I am readily familiar with the firm's practice for collection and processing of documents for mailing. Under that practice, it would be deposited within the United States Postal Service, on that same day, with postage thereon fully prepaid, in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one (1) day after date of deposit for mailing in affidavit.

Fee for Service: \$ 197.50

I declare under penalty of perjury under the laws of the United States of America and the State of California that the foregoing is true and correct and that this declaration was executed on 06/16/2021 at Petaluma, California.

One Legal - P-000618-Sonoma
 1400 North McDowell Blvd, Ste 300
 Petaluma, CA 94954



Travis Carpenter

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego

08/16/2021 at 04:57:00 PM

Clerk of the Superior Court
By Richard Day, Deputy Clerk

1 **BRYAN CAVE LLP**
2 DANIEL T. ROCKEY (SBN 178604)
3 Three Embarcadero Center, 7th Floor
4 San Francisco, CA 94111
5 Email: daniel.rockey@BCLPLaw.com
6 Telephone: (415) 675-3400
7 Facsimile: (415) 675-3434

8 Attorneys for Defendant
9 NEIGHBORHOOD HEALTHCARE

10 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
11 **COUNTY OF SAN DIEGO**

12 JANE DOE, individually and on behalf of all
13 others similarly situated,

14 Plaintiff,

15 vs.

16 NEIGHBORHOOD HEALTHCARE; HEALTH
17 CENTER PARTNERS OF SOUTHERN
18 CALIFORNIA; NETGAIN TECHNOLOGY,
19 LLC; and DOE DEFENDANTS 1-100,

20 Defendants.

Case No. 37-2021-00023936-CU-BT-CTL

**STIPULATION EXTENDING TIME
TO RESPOND TO INITIAL
COMPLAINT; [~~PROPOSED~~]
ORDER**

Complaint Filed: June 8, 2021
Trial Date: None Set

21 Plaintiff Jane Doe (“Plaintiff”) and Defendant Neighborhood Healthcare (“Defendant”)
22 (collectively “the Parties”), by and through their counsel of record, hereby stipulate and agree as
23 follows:

24 WHEREAS, Plaintiff filed her Complaint in this action on June 8, 2021 naming three
25 defendants: Neighborhood Healthcare (“Neighborhood”), Health Center Partners of Southern
26 California (“HCP”), and Netgain Technology, LLC (“Netgain”) in connection with a ransomware
27 attack occurring in December 2020.

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

WHEREAS, on July 20, 2021, counsel for Plaintiff and counsel for defendant Neighborhood Healthcare (“Neighborhood”) met and conferred regarding Neighborhood’s intent to demur to the Complaint and certain other related issues. At that meet and confer, Neighborhood indicated that it would consider voluntarily producing to Plaintiff certain documents relevant to Plaintiff’s allegations in the interest of facilitating an amendment to the Complaint. At that time, Plaintiff agreed to a 15 day extension of the time for Neighborhood to respond to the complaint and proposed that once Plaintiff had effected service on the remaining defendants, the parties should agree upon a further extension of time to align the dates for all defendants to respond to the complaint. Neighborhood agreed to this proposal.

WHEREAS, on August 11, 2021, Neighborhood voluntarily produced to Plaintiff’s counsel certain agreements relevant to the allegations of the Complaint and inquired whether Plaintiff had effected service on the remaining defendants.

WHEREAS, Plaintiff’s counsel responded the next day, confirming receipt of the documents and indicating that based upon thereon, he intended to file an amended complaint, and additionally indicated that he had received an Acknowledgment of Receipt of Service of Summons and Complaint from HCP, dated August 9, 2021, and proposed that the parties enter into a stipulation seeking court approval to extend the deadline for Neighborhood to respond to the Complaint up to and including September 8, 2021, corresponding to the date for HCP’s response to the Complaint.

WHEREAS, Neighborhood accepted Plaintiff’s counsel’s proposal.

WHEREAS, a further extension of time for Defendant to respond to the Complaint will allow for coordination of responses to the Complaint, will allow time for Plaintiff to file an amended complaint, and will allow additional time for the Parties to discuss potential resolution.

1 WHEREAS, the proposed stipulation will not alter the date of any event or any deadline
2 already fixed by Court order.

3 WHEREAS, the parties have not previously sought any extensions of time from the Court,
4 NOW, THEREFORE, the Parties hereby agree and stipulation that Defendants' response
5 deadline to the Complaint should be continued to September 8, 2021.

6 IT IS THEREFORE STIPULATED AND AGREED THAT:


7
8 1. Neighborhood's deadline to respond to the Complaint shall be extended to
9 September 8, 2021.

10 2. The Parties further agree that if Plaintiff files an amended complaint, Defendant's
11 deadline to respond shall be extended accordingly.

12
13 IT IS SO STIPULATED.

14 Dated: August 16, 2021

Patrick N. Keegan
KEEGAN & BAKER, LLP

15 By: 
16 Patrick N. Keegan

17 Attorneys for Plaintiff
18 Jane Doe

19 Dated: August 16, 2021

Daniel T. Rockey
BRYAN CAVE LEIGHTON PAISNER LLP

20 By: _____
21 Daniel T. Rockey

22 Attorneys for Defendant
23 Neighborhood Healthcare
24
25
26
27
28

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

~~PROPOSED~~ ORDER

Pursuant to the foregoing Stipulation of the parties, and good cause appearing therefor, IT IS SO ORDERED that Defendant Neighborhood Healthcare shall have until September 8, 2021 to respond to Plaintiff's initial complaint.



Dated: 8/17/21

Judge Joel R. Wohlfeil

Judge of the Superior Court of California
County of San Diego

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

PROOF OF SERVICE

I am employed in the aforesaid County, State of California; I am over the age of eighteen years and not a party to the within entitled action; my business address is: Three Embarcadero Center, 7th Floor, San Francisco, CA 94111.

On August 16, 2021, I caused to be served on the interested parties in said action the within:

**STIPULATION EXTENDING TIME TO RESPOND TO INITIAL COMPLAINT;
[PROPOSED] ORDER**

Patrick Keegan
Keegan & Baker
2292 Faraday Avenue, Suite 100
Carlsbad, CA 92008
Tel: (760)929-9303 ext 100

BY U.S. MAIL -- I am “readily familiar” with the firm’s practice of collection and processing correspondence for mailing. Under that practice it would be deposited with U.S. Postal Service on that same day with postage thereon fully prepaid at San Francisco, California in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit.

BY E-MAIL – I caused a true copy of the foregoing document(s) to be served by electronic email transmission at the time shown on each transmission, to each interested party at the email address shown above. Each transmission was reported as complete and without error.

BY OVERNIGHT DELIVERY -- Depositing the above document(s) in a box or other facility regularly maintained by FedEx in an envelope or package designated by FedEx with delivery fees paid or provided for.

(BY File & Serve XPress) -- I caused a true copy of the foregoing documents to be served by File & Serve XPress to each interested party at the email address shown above. Each transmission was reported as complete and without error.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed on August 16, 2021, at San Francisco, California.



Bridgette Warren

BRYAN CAVE LEIGHTON PAISNER LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**SUPERIOR COURT OF CALIFORNIA,
COUNTY OF SAN DIEGO
CENTRAL**

MINUTE ORDER

DATE: 06/08/2021

TIME: 08:30:00 AM

DEPT: C-73

JUDICIAL OFFICER PRESIDING: Joel R. Wohlfeil

CLERK: Jessica Pascual, Andrea Taylor

REPORTER/ERM: Not Requested

BAILIFF/COURT ATTENDANT:

CASE NO: **37-2021-00023936-CU-BT-CTL** CASE INIT.DATE: 06/01/2021

CASE TITLE: **Doe vs Neighborhood Healthcare [EFILE]**

CASE CATEGORY: Civil - Unlimited CASE TYPE: Business Tort

EVENT TYPE: Ex Parte

APPEARANCES

PATRICK N KEEGAN, counsel, present for Plaintiff(s) telephonically.

Counsel is before the court on Plaintiff's ex parte application for an order for Plaintiff to Appear by Pseudonym.

The Court, having read the moving papers, and having heard comments from counsel, grants the Ex Parte.

The Court signs the proposed order as modified.

Joel R. Wohlfeil

Judge Joel R. Wohlfeil

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Tel: (760) 929-9303
4 Fax: (760) 929-9260

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego
06/02/2021 at 02:51:00 PM
Clerk of the Superior Court
By Kristin Sorianosos, Deputy Clerk

5 Attorney for Plaintiff
6 JANE DOE

7 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
8 **FOR THE COUNTY OF SAN DIEGO**

9 JANE DOE, individually and on behalf of all others
similarly situated,

10 Plaintiff,

11 vs.

12 NEIGHBORHOOD HEALTHCARE; HEALTH
13 CENTERS PARTNERS OF SOUTHERN
CALIFORNIA; NETGAIN TECHNOLOGY, LLC;
14 and DOE DEFENDANTS 1-100;

15 Defendants.

Case No. 37-2021-00023936-CU-BT-CTL

CLASS ACTION

Assigned to: Hon. Joel R. Wohlfeil, Dept. C-73

**PLAINTIFF’S EX PARTE APPLICATION
FOR AN ORDER FOR PLAINTIFF TO
APPEAR BY PSEUDONYM; MEMORANDUM
OF POINTS AND AUTHORITIES;
DECLARATION OF PATRICK N. KEEGAN**

Date: June 8, 2021

Time: 8:30 a.m.

Place: Department C-73

16 IMAGED FILE

17 PLEASE TAKE NOTICE that pursuant to California Rules of Court, Rules 3.1200, *et seq.* and the
18 Court’s June 2, 2021 telephonic request, that on June 8, 2021, at 8:30 a.m. in the courtroom of Honorable
19 Joel R. Wohlfeil, in Department C-73 of the San Diego Superior Court, 330 West Broadway, San Diego,
20 California 92101, counsel for Plaintiff Jane Doe will appear *ex parte* (via CourtCall or Microsoft Teams)
21 for an Order allowing Plaintiff to appear by pseudonym in this matter, pursuant to Cal. Civ. Code § 3427.3
22 (West 2011).

23 This *ex parte* application is based upon section 3427.3 and good cause shown, and is supported by
24 the memorandum of points and authorities, the declaration of Patrick N. Keegan, the files and records in this
25 action, and such oral argument as the Court may consider in deciding this application.

26 Dated: June 2, 2021

KEEGAN & BAKER, LLP

s/ Patrick N. Keegan

Patrick N. Keegan, Esq.

Attorney for Plaintiff JANE DOE

1 **MEMORANDUM OF POINTS AND AUTHORITIES**

2 Plaintiff Jane Doe (or “Plaintiff”), individually and on behalf of others similarly situated, respectfully
3 submits this memorandum of points and authorities in support of her *ex parte* application for an order
4 allowing her to proceed by pseudonym in place of the real name of Plaintiff, pursuant to Cal. Civ. Code §
5 3427.3 (West 2011) (specifically allowing health care patients to bring a lawsuit using a pseudonym)
6 because at all times relevant to this action, Plaintiff is a health care patient under Civil Code § 56.05(k) and
7 has individual privacy concerns and a reasonable fear of harassment in light of the nature of the case.

8 **I. INTRODUCTION**

9 As alleged in Plaintiff’s Class Action Complaint for Damages, Restitution, and Injunctive Relief for
10 Violations of: (1) the Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*; (2) Breach of
11 California Security Notification Laws, California Civil Code § 1798.82; and (3) Business and Professions
12 Code §§ 17200, *et seq.*, filed on June 1, 2021 (“Complaint”), this class action arises from Defendants’
13 negligent failure to properly create, maintain, preserve, and/or store confidential, medical and person
14 identifying information that allowed an unauthorized person to gain access to a computer database server
15 of Defendants from October 22, 2020 to December 3, 2020, causing the disclosure and/or release of
16 unencrypted medical and personal information of Plaintiff and other persons similarly situated, to an
17 unauthorized person resulting in violations of the Confidentiality of Medical Information Act, Civil Code
18 §§ 56, *et seq.* (See, e.g., Complaint, at ¶1).

19 California statutory law specifically allows a party to bring a lawsuit using a pseudonym in cases
20 involving health care patients. Cal. Civ. Code § 3427.3 (West 2011). The Complaint at page 1, in footnote
21 1, cites and sets forth section 3427.3 in its entirety, and then further alleges, “Here, a pseudonym has been
22 used in place of the real name of Plaintiff because at all times relevant to this action, Plaintiff is a health care
23 patient under Civil Code § 56.05(k) and has individual privacy concerns and a reasonable fear of harassment
24 in light of the nature of the case.” (Complaint, at ¶1 n.1). The Complaint further alleges that the Notice of
25 Data Breach letter that Plaintiff received states that “in late September 2020, an unauthorized third party
26 gained access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the
27 unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an
28 undisclosed amount to the attacker.... The [Plaintiff’s] information involved ... may include the following:

1 name, address, date of birth, diagnosis/treatment information and treatment cost information.” (Complaint,
 2 at ¶2). Additionally, the Complaint also alleges that Plaintiff “fears that disclosure and/or release of her
 3 medical information created, maintained, preserved, and/or stored on Defendants’ computer networks could
 4 subject her to harassment or abuse.” (Complaint, at ¶¶10 and 69).

5 Further, Plaintiff is *not* proceeding *anonymous* in this action. Prior to filing the Complaint, Plaintiff
 6 sent separate letters to Defendant Neighborhood Healthcare (“NH”) and Defendant Health Center Partners
 7 of Southern California (“HCP”) disclosing the true name of Plaintiff Jane Doe and requesting further
 8 information about this security incident. (Complaint, at ¶69; and Keegan Decl., ¶3). Therefore, the
 9 Defendants are not prejudice by Plaintiff proceeding pseudonymously in this action.

10 As demonstrated below, section 3427.3 specifically allows a party to bring a lawsuit using a
 11 pseudonym in cases involving health care patients. Even before the enactment of section 3427.3, California
 12 courts have allowed plaintiffs to proceed pseudonymously in countless published state court decisions. Even
 13 before the enactment of section 3427.3, California courts have also held that the California Code of Civil
 14 Procedure does not prohibit pseudonymous litigation. Accordingly, good cause exists for the granting of
 15 Plaintiff’s *ex parte* application.

16 **II. ARGUMENT**

17 California statutory law specifically allows a party to bring a lawsuit using a pseudonym in cases
 18 involving health care patients. Cal. Civ. Code § 3427.3 (West 2011). Specifically, section 3427.3 provides,

19 The court having jurisdiction over a civil proceeding under this title ***shall take all steps***
 20 ***reasonably necessary to safeguard the individual privacy*** and prevent harassment ***of a***
 21 ***health care patient***, licensed health practitioner, or employee, client, or customer of a health
 22 ***care facility who is a party or witness in the proceeding, including granting protective orders.***
Health care patients, licensed health practitioners, and employees, clients, and customers
 of the health care facility ***may use pseudonyms to protect their privacy.***

23 Cal. Civ. Code § 3427.3 (emphasis added). Here, the Complaint alleges that at all times relevant to this
 24 action, Plaintiff is and was a health care patient.¹ (Complaint, at ¶1 n.1). The Complaint further alleges that
 25 the Notice of Data Breach letter that Plaintiff received states that “in late September 2020, an unauthorized
 26 third party gained access to Netgain’s digital environment, and between October 22, 2020 to December 3,

27
 28 ¹ As alleged in the Complaint, Plaintiff is a “natural person ... who received health care services from
 a provider of health care” within the meaning of Civil Code § 56.05(k). Complaint, at ¶10.

1 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid
 2 an undisclosed amount to the attacker.... The [Plaintiff's] information involved ... may include the following:
 3 name, address, date of birth, diagnosis/treatment information and treatment cost information.” (Complaint,
 4 at ¶2). Additionally, Plaintiff also alleges in the Complaint that she “fears that disclosure and/or release of
 5 her medical information created, maintained, preserved, and/or stored on Defendants’ computer networks
 6 could subject her to harassment or abuse.” (Complaint, at ¶¶10 and 69). Thus, under section 3427.3,
 7 Plaintiff may proceed in this case using the pseudonym “Jane Doe” in conformity with the laws of the State
 8 of California.

9 Further, Plaintiff, as a health care patient, may use a pseudonym in the Complaint and in this
 10 litigation to protect her privacy under section 3427.3, and there is no additional requirement under section
 11 3427.3 that Plaintiff must also *show* a risk of “harassment, injury, ridicule, or embarrassment” in order to
 12 proceed pseudonymously.

13 Moreover, Plaintiff is *not* proceeding *anonymous* in this action. (Keegan Decl., ¶3). Defendants
 14 Neighborhood Healthcare (“NH”) and Defendant Health Center Partners of Southern California (“HCP”)
 15 have known all along the true identity of Plaintiff, as pre-filing communications between the parties identify
 16 Plaintiff’s true identity. (Complaint, at ¶69; and Keegan Decl., ¶3). Therefore, the Defendants are not
 17 prejudice by Plaintiff proceeding pseudonymously in this action. Moreover, what Plaintiff seeks to avoid
 18 by proceeding pseudonymously in this action is additional harassment or abuse, i.e. in addition to the
 19 harassment or abuse suffered and caused by the disclosure and/or release of her medical information created,
 20 maintained, preserved, and/or stored on Defendants’ computer networks, that she fears she could be
 21 subjected to if her name is disclosed in public facing documents filed with this Court in this action. Clearly,
 22 the Legislature recognized this “need to safeguard the individual privacy and prevent harassment of a health
 23 care patient” when enacting Civil Code § 3427.3.

24 **1. Prior to the Enactment of Civil Code § 3427.3, California Courts Have Allowed**
 25 **Plaintiffs to Proceed Pseudonymously in Countless Published State Court Decisions**

26 Even before the enactment of section 3427.3, California courts have allowed plaintiffs to proceed
 27 pseudonymously in countless published state court decisions. For example, *prior to the enactment of section*
 28 *3427.3*, California courts have allowed plaintiffs to proceed with pseudonyms in a variety of cases *not*

1 *involving health care patients*. For example, *prior to the enactment of section 3427.3*, in *Doe v. Saenz*
2 (2006) 140 Cal.App.4th 960, 977–979, three convicted felons were permitted to pursue legal actions under
3 fictitious names challenging a decision by the Department of Social Services to classify their offenses as
4 nonexemptible, thereby precluding them from working in licensed community care facilities. In *Hooper v.*
5 *Deukmejian* (1981) 122 Cal.App.3d 987, 993, an individual convicted on a plea of maintaining a place for
6 selling or using marijuana was permitted to sue under a fictitious name *on behalf of himself and all others*
7 *similarly situated* (in a class action) to determine whether they were entitled to the benefits and protections
8 of marijuana reform legislation. In *Doe v. Superior Court (Luster)* (2011) 194 Cal.App.4th 750, the Court
9 of Appeal held that in an action brought under a fictitious name, it was appropriate for plaintiff to verify her
10 discovery responses using the fictitious name: “Any other rule would render the ability to use a fictitious
11 name in the litigation meaningless.” *Id.*, at 754. In *Starbucks Corp. v. Superior Court* (2008) 168
12 Cal.App.4th 1436, the Court of Appeal noted that the use of “Doe plaintiffs” to protect legitimate privacy
13 rights “The judicial use of ‘Doe plaintiffs’ to protect legitimate privacy rights has gained wide currency,
14 particularly given the rapidity and ubiquity of disclosures over the World Wide Web.” *Id.*, at 1452.

15 Additionally, *prior to the enactment of section 3427.3*, California courts have allowed plaintiffs to
16 proceed with a pseudonym in a variety of cases *involving health care patients*. *Jane Doe 8015 v. Superior*
17 *Court* (2007) 148 Cal.App.4th 489, 491-492, a patient was allowed to bring an action against a laboratory
18 using a pseudonym after it was determined that one of the laboratory’s phlebotomists had reused needles,
19 resulting in the plaintiff’s contraction of HIV.

20 California courts have also recognized that the U.S. Supreme Court has also implicitly endorsed the
21 use of pseudonyms to protect a health care patient’s privacy. *See, e.g., Doe v. Lincoln Unified School Dist.*,
22 188 Cal.App.4th at 766-767 (citing *Roe v. Wade* (1973) 410 U.S. 113, 93 S.Ct. 705, 35 L.Ed.2d 147
23 [abortion]; *Doe v. Bolton* (1973) 410 U.S. 179, 93 S.Ct. 739, 35 L.Ed.2d 201 [abortion]; and *Poe v. Ullman*
24 (1961) 367 U.S. 497, 81 S.Ct. 1752, 6 L.Ed.2d 989 [birth control].)

25 **2. Prior to the Enactment of Civil Code § 3427.3, California Courts Have Long Held That**
26 **the California Code of Civil Procedure Does Not Prohibit Pseudonymous Litigation**

27 California courts have also held that the California Code of Civil Procedure does not prohibit
28 pseudonymous litigation. *See, Doe v. Lincoln Unified School Dist.* (2010) 188 Cal.App.4th 758, 765-767;

1 and *Doe v. Superior Court (Luster)* (2011) 194 Cal.App.4th 750, 754 (holding that in an action brought
2 under a fictitious name, it was appropriate for plaintiff to verify her discovery responses using the fictitious
3 name). In *Doe v. Lincoln Unified School Dist.*, a teacher who had been placed on sick leave, sued under a
4 fictitious name to protect her privacy. She used “Jane Doe” as the plaintiff’s name on her complaint to
5 protect her privacy. *Id.*, at 762. The school district defendant argued on appeal that the teacher had no
6 standing to sue because Jane Doe was not the real party in interest and that a party must sue in his or her own
7 real name because of Code of Civil Procedure § 367. *Id.*, at 765. The *Doe v. Lincoln Unified School Dist.*
8 court rejected defendant’s argument, and held that Code of Civil Procedure § 367 does not require that a
9 party sue in his or her own name, citing “countless published state court decisions where one or more of the
10 parties have used fictitious names.” *Id.*, at 766. Code of Civil Procedure § 367 states that, “Every action
11 must be prosecuted in the name of the real party in interest, except as otherwise provided by statute.” Cal.
12 Code Civ. Pro. § 367. Specifically, the *Doe v. Lincoln Unified School Dist.* court held Code of Civil
13 Procedure § 367 to mean that a lawsuit must be brought on behalf of a person having legal standing to
14 commence the action, and “[t]he question for purposes of standing is not the name used by the party suing
15 but whether the party suing is the party possessing the right sued upon.” *Id.*, at 765-767 (holding using a
16 fictitious name does not deprive a plaintiff of standing or preclude it from being the real party in interest).

17 Furthermore, *Doe v. Superior Court (Luster)* (2011) 194 Cal.App.4th 750 is instructive. The *Doe*
18 *v. Superior Court (Luster)* court rejected the defendant’s argument that the Doe plaintiff’s true name must
19 be supplied on the verifications under Code of Civil Procedure § 2015.5, which allows declarations under
20 penalty of perjury when “subscribed” by the party or witness, *id.* at 754, and held that, “for purposes of this
21 litigation, plaintiff’s verification of the petition using the name Jane Doe is appropriate. Any other rule
22 would render the ability to use a fictitious name in the litigation meaningless.” *Id.*, at 754.

23 **III. CONCLUSION**

24 For the foregoing reasons, Plaintiff respectfully requests that the Court allow Plaintiff to proceed in
25 this matter by pseudonym.

26 Dated: June 2, 2021

KEEGAN & BAKER, LLP
s/ Patrick N. Keegan
Patrick N. Keegan, Esq.
Attorney for Plaintiff JANE DOE

DECLARATION OF PATRICK N. KEEGAN

I, Patrick N. Keegan, declare as follows:

1. I am an attorney licensed to practice before all of the courts of the State of California. I am a partner of the law firm of Keegan & Baker, LLP, counsel of record for Plaintiff Jane Doe (or “Plaintiff”).

2. I submit this declaration pursuant to California Rules of Court, Rules 3.1200, *et seq.* in support of Plaintiff’s Ex Parte Application for an Order allowing Plaintiff to appear by pseudonym in this matter, pursuant to Cal. Civ. Code § 3427.3 (West 2011). On June 2, 2021, I received a call from the Court’s clerk for the Department requesting this *Ex Parte* Application be made.

3. Prior to filing Plaintiff’s Class Action Complaint for Damages, Restitution, and Injunctive Relief for Violations of: (1) the Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*; (2) Breach of California Security Notification Laws, California Civil Code § 1798.82; and (3) Business and Professions Code §§ 17200, *et seq.*, on June 1, 2021 (“Complaint”), I, on behalf of Plaintiff, sent separate letters to Defendant Neighborhood Healthcare (“NH”) and Defendant Health Center Partners of Southern California (“HCP”) disclosing the true name of Plaintiff Jane Doe and requesting further information about this security incident. Therefore, Plaintiff is *not* proceeding *anonymous* in this action, and the Defendants are not prejudice by Plaintiff proceeding pseudonymously in this action.

4. The Complaint was filed on Tuesday, June 1, 2021, thereafter I received a call from the Court’s clerk for the Department requesting this *Ex Parte* Application on Wednesday, June 2, 2021, and no defendant has been served or has yet appeared in this litigation and, for reasons specified herein, no opposition is anticipated and Plaintiff should not be required to inform defendants prior to the hearing on this matter.

I declare under penalty of perjury pursuant to the laws of the State of California that the foregoing is true and correct. Executed this 2nd day of June, 2021, in Carlsbad, California.

s/ Patrick N. Keegan
Patrick N. Keegan

FILED
Clerk of the Superior Court

JUN 08 2021

By: A. TAYLOR

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Tel: (760) 929-9303
4 Fax: (760) 929-9260

5 Attorney for Plaintiff
JANE DOE
6
7

8 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
9 **FOR THE COUNTY OF SAN DIEGO**

10 JANE DOE, individually and on behalf of all others
similarly situated,

11 Plaintiff,

12 vs.

13 NEIGHBORHOOD HEALTHCARE; HEALTH
14 CENTERS PARTNERS OF SOUTHERN
15 CALIFORNIA; NETGAIN TECHNOLOGY, LLC;
and DOE DEFENDANTS 1-100;

16 Defendants.
17

Case No. 37-2021-00023936-CU-BT-CTL

CLASS ACTION

Assigned to: Hon. Joel R. Wohlfeil, Dept. C-73

**[PROPOSED] ORDER GRANTING
PLAINTIFF'S EX PARTE APPLICATION TO
APPEAR BY PSEUDONYM**

Date: June 8, 2021

Time: 8:30 a.m.

Place: Department C-73

IMAGED FILE

18 Plaintiff Jane Doe's application for an order allowing Plaintiff to appear by pseudonym in this matter,
19 came *ex parte* for hearing on June 8, 2021, at 8:30 a.m. in Department C-73 before the Honorable Joel R.
20 Wohlfeil, and the Court, having reviewed Plaintiff Jane Doe's application and for good cause appearing
21 therefore, hereby orders as follows:

22 IT IS HEREBY ORDERED THAT:

23 Plaintiff Jane Doe alleges she was a patient within the meaning of Civil Code § 56.05(k). As such,
24 she is authorized by Civil Code § 3427.3 to use a pseudonym in this action to protect her privacy.

25 *order is w/o prejudice to an application to vacate this*
26 *order. 6-8-21*
Dated: _____

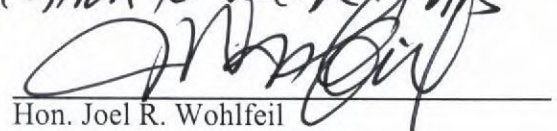
27 
Hon. Joel R. Wohlfeil
28 Judge of the Superior Court

EXHIBIT 2

1. ISSUE DATE: (MM/DD/YYYY) 8/29/2019
2a. FTCA DEEMING NOTICE NO.: 1-F00000167-19-01
2b. Supersedes: []
3. COVERAGE PERIOD: From: 1/1/2020 Through: 12/31/2020
4. NOTICE TYPE: Renewal
5. ENTITY NAME AND ADDRESS: NEIGHBORHOOD HEALTHCARE 425 N DATE ST ESCONDIDO, CA 92025
6. ENTITY TYPE: Grantee
7. EXECUTIVE DIRECTOR: Rakesh Patel
8a. GRANTEE ORGANIZATION: NEIGHBORHOOD HEALTHCARE
8b. GRANT NUMBER: H80CS00285

DEPARTMENT OF HEALTH AND HUMAN SERVICES
HEALTH RESOURCES AND SERVICES ADMINISTRATION



NOTICE OF DEEMING ACTION
FEDERAL TORT CLAIMS ACT AUTHORIZATION:
Federally Supported Health Centers Assistance Act(FSHCAA), as amended,
Sections 224(g)-(n) of the Public Health Service (PHS) Act, 42 U.S.C. § 233(g)-(n)

9. THIS ACTION IS BASED ON THE INFORMATION SUBMITTED TO, AND AS APPROVED BY HRSA, AS REQUIRED UNDER 42 U.S.C. § 233(h) FOR THE ABOVE TITLED ENTITY AND IS SUBJECT TO THE TERMS AND CONDITIONS INCORPORATED EITHER DIRECTLY OR BY REFERENCE IN THE FOLLOWING:

- a. The authorizing program legislation cited above.
- b. The program regulation cited above, and,
- c. HRSA's FTCA-related policies and procedures.

In the event there are conflicting or otherwise inconsistent policies applicable to the program, the above order of precedence shall prevail.

10. Remarks:

The check box [x] in the supersedes field indicates that this notice supersedes any and all active NDAs and rescinds any and all future NDAs issued prior to this notice.

Electronically signed by Tonya Bowers, Deputy Associate Administrator for Primary Health Care on: 8/29/2019 6:44:48 PM

A printer version document only. The document may contain some accessibility challenges for the screen reader users. To access same information, a fully 508 compliant accessible HTML version is available on the HRSA Electronic Handbooks in the FTCA Folder. If you need more information, please contact the BPHC Helpline at 877-974-BPHC (2742); Weekdays from 8:30 AM to 5:30 PM ET.

FTCA DEEMING NOTICE NO.:
1-F00000167-19-01

GRANT NUMBER:
H80CS00285



NEIGHBORHOOD HEALTHCARE
425 N DATE ST
ESCONDIDO, CA92025

Dear Rakesh Patel:

The Health Resources and Services Administration (HRSA), in accordance with the Federally Supported Health Centers Assistance Act (FSHCAA), as amended, sections 224(g)-(n) of the Public Health Service (PHS) Act, 42 U.S.C. §§ 233(g)-(n), deems NEIGHBORHOOD HEALTHCARE to be an employee of the PHS, for the purposes of section 224, effective 1/1/2020 through 12/31/2020.

Section 224(a) of the PHS Act provides liability protection under the Federal Tort Claims Act (FTCA), 28 U.S.C. §§ 1346(b), 2672, or by alternative benefits provided by the United States where the availability of such benefits precludes a remedy under the FTCA, for damage for personal injury, including death, resulting from the performance of medical, surgical, dental, or related functions by PHS employees while acting within the scope of such employment. This protection is exclusive of any other civil action or proceeding. Coverage extends to deemed entities and their (1) officers; (2) governing board members; (3) full- and part-time employees; and (4) contractors who are licensed or certified individual health care practitioners providing full-time services (i.e., on average at least 32½ hours per week for the entity for the period of the contract), or, if providing an average of less than 32½ hours per week of such service, are licensed or certified providers in the fields of family practice, general internal medicine, general pediatrics, or obstetrics/gynecology. Volunteers are neither employees nor contractors and therefore are not eligible for FTCA coverage under FSHCAA.

This Notice of Deeming Action (NDA) is also confirmation of medical malpractice coverage for both NEIGHBORHOOD HEALTHCARE and its covered individuals as described above. This NDA, along with documentation confirming employment or contractor status with the deemed entity, may be used to show liability coverage for damage for personal injury, including death, resulting from the performance of medical, surgical, dental, or related functions by PHS employees while acting within the scope of such employment.

In addition, FTCA coverage is comparable to an "occurrence" policy without a monetary cap. Therefore, any coverage limits that may be mandated by other organizations are met.

This action is based on the information provided in your FTCA deeming application, as required under 42 U.S.C. § 233(h), with regard to your entity's: (1) implementation of appropriate policies and procedures to reduce the risk of malpractice and litigation; (2) review and verification of professional credentials and privileges, references, claims history, fitness, professional review organization findings, and licensure status of health professionals; (3) cooperation with the Department of Justice (DOJ) in the defense of claims and actions to prevent claims in the future; and (4) cooperation with DOJ in providing information related to previous malpractice claims history.

Deemed health centers must continue to receive funding under Section 330 of the PHS Act, 42 U.S.C. § 254b, in order to maintain coverage as a deemed PHS employee. If the deemed entity loses its Section 330 funding, such coverage will end immediately upon termination of the grant. In addition to the relevant statutory and regulatory requirements, every deemed health center is expected to follow HRSA's FTCA-related policies and procedures, which may be found online at <http://www.bphc.hrsa.gov>.

For further information regarding FTCA, please contact the Health Center Program Support (Formally the BPHC Helpline) at 877-464-4772, option 1, or using the [BPHC Contact Form](#).

A printer version document only. The document may contain some accessibility challenges for the screen reader users. To access same information, a fully 508 compliant accessible HTML version is available on the HRSA Electronic Handbooks in the FTCA Folder. If you need more information, please contact the BPHC Helpline at 877-974-BPHC (2742); Weekdays from 8:30 AM to 5:30 PM ET.

EXHIBIT 3



August 18, 2021

Daniel T. Rockey
Partner
Direct: +1 415 268 1986
Fax: +1 415 430 4386
daniel.rockey@bclplaw.com

BRYAN CAVE LEIGHTON PAISNER LLP
Three Embarcadero Center
7th Floor
San Francisco CA 94111 4070
T: +1 415 675 3400
F: +1 415 675 3434
bclplaw.com

By United States Mail and Email

U.S. Department of Health and Human Services
Office of the General Counsel
General Law Division
Claims and Employment Law Branch
330 "C" Street, SW
Attention: CLAIMS
Switzer Building, Suite 2600
Washington, D.C. 20201
FAX No. 202-619-2922
HHS-FTCA-Claims@hhs.gov

Re: Federal Torts Claims Act - Notice of Suit by Deemed Entity pursuant to 42 USC 233(l) and 28 C.F.R. § 15.2

To Whom it May Concern:

I am an attorney with the law firm of Bryan Cave Leighton Paisner, LLP and counsel to Neighborhood Healthcare ("Neighborhood Healthcare"), a non-profit public benefit corporation and community health center that provides medical, dental, and behavioral health services to underserved communities in and around Escondido, California, where it is located. Neighborhood Healthcare is a federal grant recipient (Grant No. H80CS00285) and a "deemed entity" pursuant to 42 USC §233(g). See Exh. 1 HRSA Deeming Notice.

I am writing to provide notice pursuant to 42 USC 233(l), 28 C.F.R. § 15.2, and Health and Human Services Administration policy¹ that a complaint has been filed against Neighborhood Healthcare in San Diego Superior Court, captioned *Jane Doe v. Neighborhood Healthcare, et al.*, Case No. 37-2021-00023936-CU-BT-CTL. See Complaint attached as Exhibit 2. The complaint alleges that Neighborhood Healthcare violated the California Confidentiality of Medical Information Act ("CMIA") by sharing plaintiff Jane Doe's medical records without proper authorization (Ca. Civ. Code §56.10) and/or failing to maintain patient medical records in such a way as to ensure their confidentiality (Ca. Civ. Code § 56.101).

The Federally Supported Health Centers Assistance Act of 1992 (and as amended in 1995) (the "FSHCAA"), 42 U.S.C. § 233(g) *et seq.*, authorizes the Secretary of Health and Human Services to extend to certain federally funded health centers and their officers, directors, and employees the same protection that § 233(a) affords to Public Health Service ("PHS") employees. Under the Emergency Health Personnel Act of 1970, Pub. L. No. 91-623, § 4, 84 Stat. 1868, 1870-71 (1970), codified at 42 U.S.C. § 233, Public Health Service personnel are immunized from any civil action or proceeding arising out of the performance of medical, surgical, dental or related functions within the scope of their

¹ See <https://bphc.hrsa.gov/ftca/claimsfilings/healthcenterclaims.html> for complaint notice guidance.

Randy S. Grossman
 August 18, 2021
 Page 2



employment. 42 U.S.C. § 233(a). To facilitate the legislative objective of ensuring the availability of medical services in underserved areas, 42 U.S.C. § 233(a) shields PHS personnel from liability arising out of their medical and related duties by making the remedy for damages against the United States under the Federal Tort Claims Act the exclusive remedy for such actions. *Id.*

The protection offered to federally funded health centers by the FSHCAA grants “absolute immunity . . . for actions arising out of the performance of medical or related functions within the scope of . . . employment by barring all actions against them for such conduct.” *Hui v. Castaneda*, 559 U.S. 799, 806 (2010). Once a community health center is determined by the Health Resources and Services Administration (“HRSA”) to be a “deemed entity” pursuant to § 233(g), the FTCA is the exclusive remedy for damages resulting from the performance of medical, dental or “related functions.” 42 U.S.C. § 233(a). When the Secretary determines that a health center is a deemed entity for a given annual period, that “determination shall be final and binding upon the Secretary and the Attorney General and other parties to any civil action or proceeding.” 42 USC §233(g)(1)(F).

Upon the filing of a state court complaint, a deemed entity is directed to provide notice of the complaint to the appropriate federal agency -- in this case, the Health and Human Services Administration – which is itself directed to promptly provide notice to the United States Attorney for the district embracing the place where the action is brought, as well as the Branch Director of the Torts Branch, Civil Division, Department of Justice.² Because the *Doe* complaint filed against Neighborhood Healthcare was brought in San Diego County, the district embracing the filing location is the Southern District of California. Although the obligation to notify the United States Attorney falls upon HHS, for convenience and efficiency, we are copying the Acting U.S. Attorney for the Southern District of California, Randy S. Grossman, with this notice.³

Upon notification that a state court action is pending against a deemed entity, the Attorney General has a mandatory duty to appear in that court within 15 days of notice of the lawsuit to report whether the “Secretary has determined under subsections (g) and (h) of [Section 233], that such entity, officer, governing board member, employee, or contractor of the entity is deemed to be an employee of the Public Health Service for purposes of this section with respect to the actions or omissions that are the subject of such civil action or proceeding.” 42 USC § 233(l)(1).

Importantly, the immunity provided under § 233(a) is not limited to claims of medical malpractice, but encompasses liability arising out of “related functions”— *i.e.*, functions related to the performance of medical, surgical, or dental functions. 42 U.S.C. § 233(a); *Teresa T. v. Ragaglia* (D. Conn. 2001) 154 F.Supp.2d 290, 299-300 (immunity provided by Section 233(a) “is not limited to claims for medical malpractice” and extends to functions related to the provision of medical care); *Cuoco v. Moritsugu* (2d Cir. 2000) 222 F.3d 99, 108 (“Cuoco asserts that § 233(a) provides immunity only from medical malpractice claims. But there is nothing in the language of § 233(a) to support that conclusion.”); *Z.B. ex rel. Next Friend v. Ammonoosuc Community Health Services, Inc.* (D. Me., June 13, 2004, No. CIV. 03-540 (NH)) 2004 WL 1571988, at *3, *report and recommendation adopted sub nom. Z.B. ex rel. Kilmer v. Ammonoosuc Community Health Services, Inc.* (D. Me., Aug. 31, 2004, No. CIV. 04-34-P-S) 2004 WL 1925538 (holding that alleged failure to report domestic abuse in connection with home health visits subject to §233(a) immunity as such “negligence is ‘related to’ the provision of medical services because the duty to report arises out of the employees’ status as medical professionals.”); *Pinzon v. Mendocino Coast Clinics Inc.* (N.D. Cal., Aug. 20, 2015, No. 14-CV-05504-JST) 2015 WL 4967257, at *3 (holding that

² 28 C.F.R. § 15.2.

³ This notice is being simultaneously transmitted to Randy S. Grossman, Acting United States Attorney, U.S. Attorney’s Office Southern District of California, Federal Office Building, 889 Front Street, Room 6293, San Diego, California 92101-0720.

Randy S. Grossman
 August 18, 2021
 Page 3



plaintiff's claims for violation of the Americans with Disabilities Act, the Civil Rights Act of 1964, and the Health Insurance Portability and Accountability Act of 1996 were covered by §233(a) immunity because the remedy against the United States provided thereby is 'exclusive of any other civil action or proceeding by reason of the same subject-matter' against the employee.'). "Related functions" includes administrative or operational activities which relate to the provision of medical, dental, or surgical healthcare. *See, e.g., C. K. v. United States* (S.D. Cal., Nov. 12, 2020, No. 19-CV-2492 TWR (RBB)) 2020 WL 6684921, at *6 ("administrative or operational duties could qualify as related functions where they were connected to the provision of medical care.').

Maintaining medical records for patients receiving health care, and ensuring the confidentiality of such records, is a core administrative and operational function of providing healthcare and is thus a "medical ... or related function" within the meaning of 42 U.S.C. § 233(a). Indeed, maintaining the confidentiality of health records is a legally required function of providing health care under both state and federal law. For example, the California Confidentiality of Medical Information Act ("CMIA") requires health care providers to maintain patient health records and to provide a copy of such health records to the patient upon request. Civ. Code, § 56.07. The CMIA prohibits providers of healthcare from disclosing medical information without patient authorization, except for certain specified purposes, which includes diagnosis, treatment, and payment. Civ. Code § 56.10. The CMIA further provides that "[e]very provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Civ. Code, § 56.101. Similarly, the Health Insurance Portability and Accountability Act of 1996 also requires that healthcare providers maintain patient health records and disclose such records only with patient authorization (45 C.F.R. § 164.502) or "for treatment, payment, or health care operations" (45 C.F.R. § 164.506), and requires maintenance of administrative, physical, and technical safeguards for electronic patient health records to guard against unauthorized access or disclosure (45 C.F.R. § 164.302 *et seq.*). In fact, the statute which governs the federal health center program and which renders a health center eligible for §233(a) immunity, requires the center to have, among other things, "an ongoing quality improvement system that includes clinical services and management, and that maintains the confidentiality of patient records." 42 U.S.C. § 254b(b)(1)-(2), (k)(3)(C).

In *Mele v. Hill Health Center* (D. Conn., Jan. 8, 2008, No. 3:06CV455SRU) 2008 WL 160226, the District Court held that allegations the defendant improperly disclosed the plaintiff's medical records in violation of medical confidentiality laws fell within the "related functions" covered by §233(a). *Id.* at *2-4. The court explained:

Those claims concern the medical functions of providing treatment and the related function of ensuring the privacy of patient medical information. Thus, the claims are covered by section 233(a).

Id. Other courts have similarly assessed that §233(a) immunity applies to alleged breaches of patient confidentiality. For example, in *Kezer v. Penobscot Community Health Center*, 15-cv-225-JAW, 2019 BL 141566 at *6 (D. Me. Mar. 21, 2019), the court held that a claimed breach of patient confidentiality falls within the scope of § 233(a) immunity, as "the Plaintiffs' claim arose when the Defendants, who are all medical providers, fa[iled] to comply with their ongoing professional duty to keep Ms. Kezer's medical records confidential while performing health care services." In so holding, the court noted that under applicable state law, a breach of confidentiality fell within the rubric of professional medical negligence. *Id.* Notably, Judge Robinson of the US District Court for the Southern District of California, the district in which the complaint against Neighborhood Healthcare was brought, cited *Kezer* approvingly in rejecting the Department of Justice's argument that § 233(a) did not embrace a health center employee's alleged failure to report suspected abuse. *C. K.,* (S.D. Cal., Nov. 12, 2020, No. 19-CV-2492 TWR (RBB)) 2020 WL

Randy S. Grossman
August 18, 2021
Page 4



6684921, at *6 (“As in *Kezer*, applicable state law supports a medical malpractice claim,....”). *See also, Logan v. St. Charles Health Council, Inc.* (W.D. Va., May 1, 2006, No. 1:06CV00039) 2006 WL 1149214, at *1–3 (holding that FTCA embraces claims for breach of privacy statute, but finding that §233(a) did not apply because plaintiff sued based on employer/employee relationship, rather than patient/medical professional relationship); *Roberson v. Greater Hudson Valley Family Health Center, Inc.* (S.D.N.Y., June 12, 2018, No. 17-CV-7325 (NSR)) 2018 WL 2976024, at *1 (claim alleging that employee of defendant inappropriately accessed plaintiff’s medical records and disclosed information to people she knew must be dismissed for failure to file administrative claim as required by FTCA); *See also Brignac v. United States*, 239 F.Supp.3d 1367, 1377-78 (N.D. Ga. 2017) (applying § 233(a) where patient brought a negligent supervision claim against the health center alleging he was sexually assaulted by a doctor during treatment); *La Casa de Buena Salud v. United States*, No. CIV 07-238 JB/RHS, 2008 WL 2323495, at *20 (D.N.M. Mar. 21 2008) (applying § 233(a) to a negligent hiring claim brought by the estate of a deceased patient, as hiring was a “related function”).

Here, Plaintiff Doe, a patient of Neighborhood Healthcare, alleges that Neighborhood failed to ensure the confidentiality of her patient records, as required by Civil Code § 56.10 and § 56.101 of the CMIA. As the above courts have recognized, the maintenance of current, accurate, and accessible medical records is a “related function” to the provision of medical care, and ensuring the confidentiality of such records is a legally required function of healthcare providers under both the CMIA and HIPAA. The courts have further held that the alleged failure of a healthcare provider to maintain the confidentiality of medical records in violation of §56.10 of the CMIA constitutes a claim for professional negligence under California law. *See, e.g., Francies v. Kapla* (2005) 127 Cal.App.4th 1381, 1386, fn. 11, *as modified* (Apr. 8, 2005) (holding that claim for unauthorized disclosure of medical records in violation of CMIA is subject to cap on noneconomic damages under Medical Injury Compensation Reform Act); Civ. Code, § 3333.2 (MICRA applies to “any action for injury against a health care provider based on professional negligence.”). It is thus clear that the claims of Jane Doe asserted against Neighborhood Healthcare here fit squarely within the immunity provided by §233(a).

In view of the foregoing, Neighborhood Healthcare hereby requests that the United States promptly appear in *Doe v. Neighborhood Healthcare et al.*, and assume the defense of the matter. Please note that because not all parties have been served with the complaint, the plaintiff and Neighborhood Healthcare have stipulated to an extension of time to respond to the complaint up to and including September 8, 2021.

Randy S. Grossman
August 18, 2021
Page 5



If you wish to discuss the foregoing or have any questions concerning the lawsuit, please do not hesitate to reach out to me. I can provide any information that would be helpful understanding the allegations and the incident upon which they are premised, and am ready and willing to facilitate all necessary cooperation in the defense of the above-referenced claims.

Very truly yours,

A handwritten signature in blue ink, appearing to read "D. Rockey", is positioned below the closing. The signature is fluid and cursive.

Daniel T. Rockey

Partner

DTR
Enclosures

Cc: Randy S. Grossman, Acting United States Attorney for the Southern District of California
(Randy.Grossman@usdoj.gov)

EXHIBIT 1

1. ISSUE DATE: (MM/DD/YYYY) 8/29/2019
2a. FTCA DEEMING NOTICE NO.: 1-F00000167-19-01
2b. Supersedes: []
3. COVERAGE PERIOD: From: 1/1/2020 Through: 12/31/2020
4. NOTICE TYPE: Renewal
5. ENTITY NAME AND ADDRESS: NEIGHBORHOOD HEALTHCARE 425 N DATE ST ESCONDIDO, CA 92025
6. ENTITY TYPE: Grantee
7. EXECUTIVE DIRECTOR: Rakesh Patel
8a. GRANTEE ORGANIZATION: NEIGHBORHOOD HEALTHCARE
8b. GRANT NUMBER: H80CS00285

DEPARTMENT OF HEALTH AND HUMAN SERVICES
HEALTH RESOURCES AND SERVICES ADMINISTRATION



NOTICE OF DEEMING ACTION
FEDERAL TORT CLAIMS ACT AUTHORIZATION:
Federally Supported Health Centers Assistance Act(FSHCAA), as amended,
Sections 224(g)-(n) of the Public Health Service (PHS) Act, 42 U.S.C. § 233(g)-(n)

9. THIS ACTION IS BASED ON THE INFORMATION SUBMITTED TO, AND AS APPROVED BY HRSA, AS REQUIRED UNDER 42 U.S.C. § 233(h) FOR THE ABOVE TITLED ENTITY AND IS SUBJECT TO THE TERMS AND CONDITIONS INCORPORATED EITHER DIRECTLY OR BY REFERENCE IN THE FOLLOWING:

- a. The authorizing program legislation cited above.
- b. The program regulation cited above, and,
- c. HRSA's FTCA-related policies and procedures.

In the event there are conflicting or otherwise inconsistent policies applicable to the program, the above order of precedence shall prevail.

10. Remarks:

The check box [x] in the supersedes field indicates that this notice supersedes any and all active NDAs and rescinds any and all future NDAs issued prior to this notice.

Electronically signed by Tonya Bowers, Deputy Associate Administrator for Primary Health Care on: 8/29/2019 6:44:48 PM

A printer version document only. The document may contain some accessibility challenges for the screen reader users. To access same information, a fully 508 compliant accessible HTML version is available on the HRSA Electronic Handbooks in the FTCA Folder. If you need more information, please contact the BPHC Helpline at 877-974-BPHC (2742); Weekdays from 8:30 AM to 5:30 PM ET.

FTCA DEEMING NOTICE NO.:
1-F00000167-19-01

GRANT NUMBER:
H80CS00285



NEIGHBORHOOD HEALTHCARE
425 N DATE ST
ESCONDIDO, CA92025

Dear Rakesh Patel:

The Health Resources and Services Administration (HRSA), in accordance with the Federally Supported Health Centers Assistance Act (FSHCAA), as amended, sections 224(g)-(n) of the Public Health Service (PHS) Act, 42 U.S.C. §§ 233(g)-(n), deems NEIGHBORHOOD HEALTHCARE to be an employee of the PHS, for the purposes of section 224, effective 1/1/2020 through 12/31/2020.

Section 224(a) of the PHS Act provides liability protection under the Federal Tort Claims Act (FTCA), 28 U.S.C. §§ 1346(b), 2672, or by alternative benefits provided by the United States where the availability of such benefits precludes a remedy under the FTCA, for damage for personal injury, including death, resulting from the performance of medical, surgical, dental, or related functions by PHS employees while acting within the scope of such employment. This protection is exclusive of any other civil action or proceeding. Coverage extends to deemed entities and their (1) officers; (2) governing board members; (3) full- and part-time employees; and (4) contractors who are licensed or certified individual health care practitioners providing full-time services (i.e., on average at least 32½ hours per week for the entity for the period of the contract), or, if providing an average of less than 32½ hours per week of such service, are licensed or certified providers in the fields of family practice, general internal medicine, general pediatrics, or obstetrics/gynecology. Volunteers are neither employees nor contractors and therefore are not eligible for FTCA coverage under FSHCAA.

This Notice of Deeming Action (NDA) is also confirmation of medical malpractice coverage for both NEIGHBORHOOD HEALTHCARE and its covered individuals as described above. This NDA, along with documentation confirming employment or contractor status with the deemed entity, may be used to show liability coverage for damage for personal injury, including death, resulting from the performance of medical, surgical, dental, or related functions by PHS employees while acting within the scope of such employment.

In addition, FTCA coverage is comparable to an "occurrence" policy without a monetary cap. Therefore, any coverage limits that may be mandated by other organizations are met.

This action is based on the information provided in your FTCA deeming application, as required under 42 U.S.C. § 233(h), with regard to your entity's: (1) implementation of appropriate policies and procedures to reduce the risk of malpractice and litigation; (2) review and verification of professional credentials and privileges, references, claims history, fitness, professional review organization findings, and licensure status of health professionals; (3) cooperation with the Department of Justice (DOJ) in the defense of claims and actions to prevent claims in the future; and (4) cooperation with DOJ in providing information related to previous malpractice claims history.

Deemed health centers must continue to receive funding under Section 330 of the PHS Act, 42 U.S.C. § 254b, in order to maintain coverage as a deemed PHS employee. If the deemed entity loses its Section 330 funding, such coverage will end immediately upon termination of the grant. In addition to the relevant statutory and regulatory requirements, every deemed health center is expected to follow HRSA's FTCA-related policies and procedures, which may be found online at <http://www.bphc.hrsa.gov>.

For further information regarding FTCA, please contact the Health Center Program Support (Formally the BPHC Helpline) at 877-464-4772, option 1, or using the [BPHC Contact Form](#).

A printer version document only. The document may contain some accessibility challenges for the screen reader users. To access same information, a fully 508 compliant accessible HTML version is available on the HRSA Electronic Handbooks in the FTCA Folder. If you need more information, please contact the BPHC Helpline at 877-974-BPHC (2742); Weekdays from 8:30 AM to 5:30 PM ET.

EXHIBIT 2

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Telephone: (760) 929-9303
4 Facsimile: (760) 929-9260

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego
06/01/2021 at 04:40:18 PM
Clerk of the Superior Court
By Richard Day, Deputy Clerk

5 Attorneys for Plaintiff JANE DOE

6
7 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
8 **FOR THE COUNTY OF COUNTY OF SAN DIEGO**

9 JANE DOE, individually and on behalf of all
others similarly situated,

10 Plaintiff,

11 vs.

12 NEIGHBORHOOD HEALTHCARE; HEALTH
13 CENTER PARTNERS OF SOUTHERN
CALIFORNIA; NETGAIN TECHNOLOGY,
14 LLC; and DOE DEFENDANTS 1-100;

15 Defendants.
16

) Case No.: 37-2021-00023936-CU-BT-CTL
)

) **CLASS ACTION COMPLAINT FOR**
) **DAMAGES, RESTITUTION, AND**
) **INJUNCTIVE RELIEF FOR VIOLATIONS**
) **OF:**

-) (1) **THE CONFIDENTIALITY OF**
) **MEDICAL INFORMATION ACT,**
) **CIVIL CODE §§ 56, ET SEQ.;**
) (2) **BREACH OF CALIFORNIA**
) **SECURITY NOTIFICATION**
) **LAWS, CALIFORNIA CIVIL CODE**
) **§ 1798.82; AND**
) (3) **BUSINESS AND PROFESSIONS**
) **CODE §§ 17200, ET SEQ.**

) **JURY TRIAL DEMANDED**
)

17
18
19 Plaintiff Jane Doe (or “Plaintiff”), by and through her attorneys, bring this class action on
20 behalf of herself individually and all others similarly situated, against Defendants Neighborhood
21 Healthcare, Health Center Partners of Southern California, and Netgain Technology, LLC
22 (collectively referred to as “Defendants”), and alleges upon information and belief as follows:

23 **INTRODUCTION**

24 1. This class action arises from the negligent and failure of Defendants to properly
25 create, maintain, preserve, and/or store confidential, medical and personal identifying information
26 of Plaintiff¹ and all other persons similarly situated which allowed an unauthorized person to gain
27

28 ¹ California statutory law specifically allows a party to bring a lawsuit using a pseudonym in cases involving health care patients. Cal. Civ. Code § 3427.3 (West 2011). Specifically, section 3427.3

1 access to a computer database server of Defendants from October 22, 2020 to December 3, 2020,
2 causing unauthorized access, viewing, exfiltration, theft, and/or disclosure of unencrypted medical
3 and personal identifying information of Plaintiff and other persons similarly situated, to at least one
4 unauthorized person resulting in violations of the Confidentiality of Medical Information Act, Civil
5 Code §§ 56, *et seq.* (hereinafter referred to as the “Act”), the Security Notification Laws, Civil Code
6 § 1798.82, and the Business and Professions Code §§ 17200 *et seq.* Under the Act, Plaintiff, and
7 all other persons similarly situated, have the right to expect that the confidentiality of their medical
8 information in possession of Defendants and/or derived from Defendants to be reasonably
9 preserved and protected from unauthorized access, viewing, exfiltration, theft, and/or disclosure.

10 2. As alleged more fully below, failing to take adequate and reasonable measures to
11 ensure its data systems were protected against unauthorized intrusions, by failing to invest in cyber
12 security and data protection safeguards, failing to implement adequate and reasonable security
13 controls and user authorization and authentication processes, failing to limit the types of data
14 permitted to be transferred, failing to properly and adequately educate and train its employees, and
15 to put into place reasonable or adequate computer systems and security practices to safeguard
16 customers’ and patients’ medical and personal identifying information, Defendants negligently
17 created, maintained, preserved, and stored Plaintiff’s and the Class (defined *infra*) members’
18 medical and personal identifying information in possession of or derived from Defendants allowed
19 such information to be accessed and actually viewed by at least one unauthorized third party,
20 without Plaintiff’s and the Class members’ prior written authorization, which constitutes
21 unauthorized disclosure and/or release of their information in violation of Civil Code §§ 56.10(a)
22 and 56.101(a) of the Act. In fact, Defendant Health Center Partners of Southern California’s form

23
24
25 provides, “The court having jurisdiction over a civil proceeding under this title shall take all steps
26 ***reasonably necessary to safeguard the individual privacy and prevent harassment of a health care***
27 ***patient***, licensed health practitioner, or employee, client, or customer of a health care facility who is
28 a party or witness in the proceeding, including granting protective orders. ***Health care patients***,
licensed health practitioners, and employees, clients, and customers of the health care facility ***may***
use pseudonyms to protect their privacy.” Cal. Civ. Code § 3427.3 (emphasis added). Here, a
pseudonym has been used in place of the real name of Plaintiff because at all times relevant to this
action, Plaintiff is a health care patient under Civil Code § 56.05(k) and has individual privacy
concerns and a reasonable fear of harassment in light of the nature of the case.

1 letter, entitled “**Notice of Data Breach**,” dated April 12, 2021, signed by Henry Tuttle, President &
2 Chief Executive Officer, Health Center Partners of Southern California, sent to Plaintiff and all
3 other persons similarly situated, informing them, in part, of “a recent data security incident
4 experienced by Netgain Technology, LLC (‘Netgain’), the IT service provider for Health Center
5 Partners of Southern California (‘HCP’)” and stating, in part, “HCP supports community health
6 centers in a variety of ways, including collaborative grant-funded programs and services for
7 Neighborhood Healthcare.... **What Happened:** Netgain recently informed HCP that it had
8 experienced a data security incident that involved systems containing HCP data.... According to
9 Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital
10 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
11 obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the
12 attacker in exchange for assurances that the attacker will delete all copies of this data and that it will
13 not publish, sell, or otherwise disclose the data.... The information involved varies depending on the
14 individual but may include the following: name, address, date of birth, diagnosis/treatment
15 information and treatment cost information. Once we learned that HCP data may have been
16 involved in the incident, we worked with our cybersecurity experts to review the impacted files and
17 identify the individuals whose information was contained in such files so that we may notify such
18 individuals. Our investigation revealed that the impacted files contained your personal information.”
19 An exemplar of Defendant Health Center Partners of Southern California’s “**Notice of Data**
20 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
21 as **Exhibit A**.

22 3. Additionally, Defendant Neighborhood Healthcare caused a form letter sent on its
23 behalf, entitled “**Notice of Data Breach**,” dated April 8, 2021, signed by Rakesh Patel, CEO,
24 Neighborhood Healthcare, stating, in part, “We are writing to make you aware of an issue brought
25 to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud
26 hosting and managed services provider. Neighborhood Healthcare used Netgain to host some
27 Neighborhood Healthcare files. **What Happened** On November 24, 2020, Netgain became aware
28 of a security incident that involved unauthorized access to portions of the Netgain environment and

1 Netgain client environments and began taking steps to investigate this incident. But, on December
2 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files
3 owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain
4 took additional measures to contain the threat and address the issue. Netgain’s technical teams
5 worked closely with third-party experts to remove the threat in the impacted environments and
6 confirm that client and internal systems are protected. Neighborhood Healthcare learned of the
7 ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to
8 believe that the protected health information (“PHI”) of our patients had been impacted in the
9 incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some
10 information including, potentially, some files containing patient PHI may have been impacted in the
11 incident. Netgain could not confirm, at that time, what records may have been impacted in the
12 incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood
13 Healthcare that Netgain believed were impacted by the attackers. Those files came from a
14 Neighborhood Healthcare server accessible by the Netgain environment. Since that time,
15 Neighborhood Healthcare has worked to review those records, to identify individuals impacted,
16 conduct an investigation into the incident with the assistance outside experts, and to transmit this
17 letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood
18 Healthcare determined that the impacted files included some of your information. **What**
19 **Information Was Involved** The information involved may have included some of the following:
20 your name, date of birth, address, Social Security Number and information about the care that you
21 received from Neighborhood Healthcare such as insurance coverage information, physician you
22 saw, and treatment codes.” An exemplar of Defendant Neighborhood Healthcare’s “**Notice of Data**
23 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
24 as **Exhibit B**.

25 4. Additionally, Defendant Netgain Technology, LLC stated in a blog post, entitled
26 “What we learned as a ransomware victim – so you don’t become one,” that “late last year, Netgain
27 was the victim of a criminal ransomware attack.... to become a victim of such an attack is both
28 humbling and galvanizing.... we identified additional opportunities to strengthn our security posture

1 in a continuous journey with an ongoing commitment to ensure this remains top-of-mind. As part
2 of our incident response, we have implemented a number of these identified enhancements to our
3 security posture and have continued to progress a multipronged approach. We've deployed new
4 tools, revised policies and enforcement procedures, and implemented an advanced around-the-clock
5 managed detections and response service for proactive threat monitoring.”

6 5. Because the individually identifiable medical information and other personal
7 identifying information of Plaintiff and the Class was subject to unauthorized access and viewing by
8 at least one unauthorized third party and in violation of the Act, Plaintiff, individually and on behalf
9 of all others similarly situated, seeks from Defendants nominal damages in the amount of one
10 thousand dollars (\$1,000) for each violation under Civil Code §56.36(b)(1) and actual damages,
11 according to proof, for each violation pursuant to Civil Code § 56.36(b)(2). Further, because
12 Plaintiff also alleges Defendants' conduct violates Business & Professions Code §§ 17200, *et seq.*,
13 Plaintiff, individually and on behalf of others similarly situated, seeks injunctive relief and
14 restitution from Defendants under Business and Professions Code § 17203.

15 6. This action, if successful, will enforce an important right affecting the public interest
16 and would confer a significant benefit, whether pecuniary or non-pecuniary, on a large class of
17 persons. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff
18 in relation to Plaintiff's stake in the matter, and therefore class certification is appropriate in this
19 matter.

20 **JURISDICTION AND VENUE**

21 7. This Court has jurisdiction over this action under California Code of Civil Procedure
22 § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class in the aggregate
23 exceeds the \$25,000 jurisdictional minimum of this Court. Further, the amount in controversy as to
24 Plaintiff individually does not exceed \$75,000.

25 8. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of
26 Civil Procedure §§ 395(a) and 395.5 because Defendant Neighborhood Healthcare is incorporated
27 in and does business in the State of California, and employs persons located in the County of San
28 Diego and in this judicial district. Defendants have obtained medical information of Plaintiff and

1 the Class in the transaction of business in the State of California and in this judicial district, which
2 has caused both obligations and liability of Defendants to arise in the State of California and in this
3 judicial district.

4 9. Further, this action does not qualify for federal jurisdiction under the Class Action
5 Fairness Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies
6 to this action because (1) more than two-thirds of the members of the proposed Class and SubClass
7 are citizens of the State of California, and (2) Defendants are citizens of the State of California.

8 **PARTIES**

9 **A. PLAINTIFF**

10 10. Plaintiff Jane Doe is and was at all times relevant to this action a resident of the State
11 of California and citizen of the State of California. At all times relevant to this action, Plaintiff
12 JANE DOE was a patient of, received medical treatment and diagnosis from, and provided her
13 personal information, including her name, address, date of birth, social security number, phone
14 number and email address to Defendant Neighborhood Healthcare. Additionally, Plaintiff received
15 a letter addressed to her, sent on Defendant Health Center Partners of Southern California’s behalf,
16 entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle, President & Chief
17 Executive Officer, Health Center Partners of Southern California, informing her, in part, of “a
18 recent data security incident experienced by Netgain Technology, LLC (‘Netgain’), the IT service
19 provider for Health Center Partners of Southern California (‘HCP’)” and stating, in part, “HCP
20 supports community health centers in a variety of ways, including collaborative grant-funded
21 programs and services for Neighborhood Healthcare.... **What Happened:** Netgain recently
22 informed HCP that it had experienced a data security incident that involved systems containing
23 HCP data.... According to Netgain, in late September 2020, an unauthorized third party gained
24 access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the
25 unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an
26 undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies
27 of this data and that it will not publish, sell, or otherwise disclose the data.... The information
28 involved varies depending on the individual but may include the following: name, address, date of

1 birth, diagnosis/treatment information and treatment cost information. Once we learned that HCP
2 data may have been involved in the incident, we worked with our cybersecurity experts to review
3 the impacted files and identify the individuals whose information was contained in such files so that
4 we may notify such individuals. Our investigation revealed that the impacted files contained your
5 personal information.” As a result, Plaintiff reasonably fears that disclosure and/or release of her
6 medical information created, maintained, preserved and/or stored on Defendants’ computer
7 networks could subject her to harassment or abuse.

8 **B. DEFENDANTS**

9 11. Defendant Neighborhood Healthcare (“NH”) is a California corporation, is registered
10 to do business and does business in the State of California (CA Corp. No. C0667935), with its
11 principal business office located at 1540 E. Valley Parkway, Escondido CA 92026, and with its
12 registered agent of service of process located at 150 La Terraza Blvd, Suite 201, Escondido CA
13 92025. On or about April 8, 2021, NH caused a form letter sent on its behalf, entitled “**Notice of**
14 **Data Breach,**” dated April 8, 2021, signed by Rakesh Patel, CEO, Neighborhood Healthcare, an
15 exemplar of which is attached hereto as **Exhibit B**, to be submitted to the Attorney General of the
16 State of California. At all times relevant to this action, NH was and is a provider of health care, a
17 contractor, and/or other authorized recipient of personal and confidential medical information, as
18 that term is defined and set forth in the Act, including the names, addresses, dates of birth,
19 diagnosis/treatment information and treatment cost information of Plaintiff and the SubClass
20 (defined *infra*), and is subject to the requirements and mandates of the Act, including but not limited
21 to Civil Code §§ 56.10, 56.101 and 56.36. At all times relevant to this action, NH was and is a
22 provider of health care and employed and employs persons located in the County of San Diego
23 and in this judicial district.

24 12. Defendant Health Center Partners of Southern California (“HCP”) is a business
25 entity doing business in the State of California, with its principal business office located at 3710
26 Ruffin Road, San Diego, CA 92123. On or about April 12, 2021, HCP caused a form letter sent on
27 its behalf, entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle,
28 President & Chief Executive Officer, Health Center Partners of Southern California, an exemplar of

1 which is attached hereto as **Exhibit A**, to be submitted to the Attorney General of the State of
2 California and to be mailed to Plaintiff and the Class. At all times relevant to this action, HCP was
3 and is a “business” within the meaning of Civil Code § 1798.140(c)(1), owns or licenses
4 computerized data which includes Plaintiff’s and the Class’ personal information, within the
5 meaning of Civil Code § 1798.82(h), collected Plaintiff’s and the Class’ personal information
6 within the meaning of Civil Code § 1798.81.5(d)(1)(A).

7 13. Defendant Netgain Technology, LLC (“NETGAIN”) is a business entity doing
8 business in the State of California, with its principal business office located at 5353 Mission Center
9 Road, Suite 202, San Diego, CA 92108. At all times relevant to this action, NETGAIN was and is
10 NH’s and HCP’s third-party vendor. On March 24, 2021, NETGAIN posted on its website a blog,
11 entitled “What we learned as a ransomware victim – so you don’t become one,” which stated, in
12 part, “In our case, late last year, Netgain was the victim of a criminal ransomware attack.... to
13 become a victim of such an attack is both humbling and galvanizing.... we identified additional
14 opportunities to strengthn our security posture in a continuous journey with an ongoing commitment
15 to ensure this remains top-of-mind. As part of our incident response, we have implemented a
16 number of these identified enhancements to our security posture and have continued to progress a
17 multipronged approach. We’ve deployed new tools, revised policies and enforcement procedures,
18 and implemented an advanced around-the-clock managed detections and response service for
19 proactive threat monitoring.”

20 **C. DOE DEFENDANTS**

21 14. The true names and capacities, whether individual, corporate, associate, or otherwise,
22 of Defendants sued herein as Doe Defendants 1 through 100, inclusive, are currently unknown to
23 Plaintiff, who therefore sue the Defendants by such fictitious names under the Code of Civil
24 Procedure § 474. Each of the Defendants designated herein as a Doe Defendant is legally
25 responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of
26 court and/or amend this complaint to reflect the true names and capacities of the Defendants
27 designated hereinafter as Doe Defendants 1 through 100 when such identities become known. Any
28

1 reference made to a named Defendant by specific name or otherwise, individually or plural, is also a
2 reference to the actions or inactions of Doe Defendants 1 through 100, inclusive.

3 **D. AGENCY/AIDING AND ABETTING**

4 15. At all times herein mentioned, Defendants, and each of them, were an agent or joint
5 venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the
6 course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the
7 acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized
8 the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

9 16. Defendants, and each of them, aided and abetted, encouraged and rendered
10 substantial assistance to the other Defendants in breaching their obligations to Plaintiff and the
11 Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially
12 assist the commissions of these wrongful acts and other wrongdoings complained of, each of the
13 Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its
14 conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals,
15 and wrongdoing.

16 **FACTUAL ALLEGATIONS**

17 17. As a result, at all times relevant to this action, including the period from October 22,
18 2020 to December 3, 2020, HCP possessed Plaintiff's and the Class' medical information, in
19 electronic and physical form, in possession of or derived from Defendant regarding their medical
20 history, mental or physical condition, or treatment. Such medical information included or contained
21 an element of personal identifying information sufficient to allow identification of Plaintiff and the
22 Class, such as their names, date of birth, addresses, medical record numbers, insurance provider,
23 electronic mail addresses, telephone numbers, or social security numbers, or other information that,
24 alone or in combination with other publicly available information, reveals their identity. At all
25 times relevant to this action, including the period from October 22, 2020 to December 3, 2020, HCP
26 maintained and continues to maintain "medical information," within the meaning of Civil Code §
27 56.05(j), of Plaintiff and the Class, each of which are "patients" within the meaning of Civil Code §
28 56.05(k).

1 18. As a result, at all times relevant to this action, including the period from October 22,
2 2020 to December 3, 2020, NH possessed Plaintiff’s and the SubClass’ medical information, in
3 electronic and physical form, in possession of or derived from Defendant regarding their medical
4 history, mental or physical condition, or treatment. Such medical information included or contained
5 an element of personal identifying information sufficient to allow identification of Plaintiff and the
6 SubClass, such as their names, date of birth, addresses, medical record numbers, insurance provider,
7 electronic mail addresses, telephone numbers, or social security numbers, or other information that,
8 alone or in combination with other publicly available information, reveals their identity. At all
9 times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH
10 maintained and continues to maintain “medical information,” within the meaning of Civil Code §
11 56.05(j), of Plaintiff and the SubClass, each of which are “patients” within the meaning of Civil
12 Code § 56.05(k). At all times relevant to this action, including the period from October 22, 2020 to
13 December 3, 2020, NH was and is a “provider of health care” within the meaning of Civil Code §
14 56.05(m). At all times relevant to this action, including the period from October 22, 2020 to
15 December 3, 2020, Plaintiff and SubClass members were patients, within the meaning of Civil Code
16 § 56.05(k).

17 19. As a result, at all times relevant to this action, including the period from October 22,
18 2020 to December 3, 2020, NETGAIN possessed Plaintiff’s, the SubClass’ and the Class’ medical
19 information, in electronic and physical form, in possession of or derived from Defendant regarding
20 their medical history, mental or physical condition, or treatment. Such medical information
21 included or contained an element of personal identifying information sufficient to allow
22 identification of Plaintiff, the SubClass and the Class, such as their names, date of birth, addresses,
23 medical record numbers, insurance provider, electronic mail addresses, telephone numbers, or social
24 security numbers, or other information that, alone or in combination with other publicly available
25 information, reveals their identity. At all times relevant to this action, including the period from
26 October 22, 2020 to December 3, 2020, NETGAIN maintained and continues to maintain “medical
27 information,” within the meaning of Civil Code § 56.05(j), of Plaintiff and the Class, each of which
28 are “patients” within the meaning of Civil Code § 56.05(k).

1 20. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, pursuant to Civil Code § 56.06(a), HCP, as a business that created, maintained,
3 preserved, and stored records of the care, products and services that Plaintiff and the Class members
4 received in the State of California from HCP’s over 16 member community health centers, 140
5 member practice sites, 857,757 patients served, and/or other providers of health care, health care
6 service plans, pharmaceutical companies, and contractors, as defined by the Act, is and was
7 organized for the purpose of maintaining medical information, within the meaning of Civil Code §
8 56.05(j), in order to make the information available to Plaintiff and the Class members or to a
9 provider of health care at the request of Plaintiff and the Class members or a provider of health care,
10 for purposes of allowing Plaintiff and the Class members to manage their information, or for the
11 diagnosis and treatment of Plaintiff and the Class members, is and was deemed to be a “provider of
12 health care,” within the meaning of Civil Code § 56.05(m).

13 21. Alternatively, at all times relevant to this action, including the period from October
14 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), HCP, as an entity that is a
15 medical group, independent practice association, pharmaceutical benefits manager, or a medical
16 service organization, and is not a health care service plan or provider of health care to Plaintiff and
17 the Class members, is and was a “contractor” under Civil Code § 56.05(d).

18 22. Alternatively, at all times relevant to this action, including the period from October
19 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, HCP is and was a recipient of
20 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
21 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
22 further disclosing that medical information except in accordance with a new authorization that
23 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
24 of this chapter or by law.

25 23. Alternatively, at all times relevant to this action, including the period from October
26 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, HCP is and was a recipient of
27 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
28 the Act, and was prohibited from further disclosing such medical information unless in accordance

1 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
2 permitted by other provisions of this chapter or by law.

3 24. Additionally, at all times relevant to this action, including prior to the period from
4 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), HCP is and was an entity
5 engaged in the business of furnishing administrative services to programs that provide payment for
6 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
7 or permitting its employees or agents to use or disclose Plaintiff's and the Class members' medical
8 information possessed in connection with performing administrative functions for a program, except
9 as reasonably necessary in connection with the administration or maintenance of the program, or as
10 required by law, or with an authorization.

11 25. As a provider of health care, a contractor, and/or other authorized recipient of
12 personal and confidential medical information, HCP is required by the Act to ensure that medical
13 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
14 patients' authorization, and to protect and preserve the confidentiality of the medical information
15 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

16 26. At all times relevant to this action, including the period from October 22, 2020 to
17 December 3, 2020, pursuant to Civil Code § 56.06(a), NH, as a business that created, maintained,
18 preserved, and stored records of the care, products and services that Plaintiff and the Class members
19 received in the State of California from NH and/or other providers of health care, health care service
20 plans, pharmaceutical companies, and contractors, as defined by the Act, is and was organized for
21 the purpose of maintaining medical information, within the meaning of Civil Code § 56.05(j), in
22 order to make the information available to Plaintiff and the Class members or to a provider of health
23 care at the request of Plaintiff and the Class members or a provider of health care, for purposes of
24 allowing Plaintiff and the Class members to manage their information, or for the diagnosis and
25 treatment of Plaintiff and the Class members, is and was deemed to be a "provider of health care,"
26 within the meaning of Civil Code § 56.05(m).

27 27. Alternatively, at all times relevant to this action, including the period from October
28 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), NH, as an entity that is a medical

1 group, independent practice association, pharmaceutical benefits manager, or a medical service
2 organization, and is not a health care service plan or provider of health care to Plaintiff and the
3 Class members, is and was a “contractor” under Civil Code § 56.05(d).

4 28. Alternatively, at all times relevant to this action, including the period from October
5 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NH is and was a recipient of
6 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
7 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
8 further disclosing that medical information except in accordance with a new authorization that
9 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
10 of this chapter or by law.

11 29. Alternatively, at all times relevant to this action, including the period from October
12 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NH is and was a recipient of
13 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
14 the Act, and was prohibited from further disclosing such medical information unless in accordance
15 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
16 permitted by other provisions of this chapter or by law.

17 30. Additionally, at all times relevant to this action, including prior to the period from
18 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), NH is and was an entity
19 engaged in the business of furnishing administrative services to programs that provide payment for
20 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
21 or permitting its employees or agents to use or disclose Plaintiff’s and the Class members’ medical
22 information possessed in connection with performing administrative functions for a program, except
23 as reasonably necessary in connection with the administration or maintenance of the program, or as
24 required by law, or with an authorization.

25 31. As a provider of health care, a contractor, and/or other authorized recipient of
26 personal and confidential medical information, NH is required by the Act to ensure that medical
27 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
28

1 patients' authorization, and to protect and preserve the confidentiality of the medical information
2 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

3 32. At all times relevant to this action, including the period from October 22, 2020 to
4 December 3, 2020, pursuant to Civil Code § 56.06(a), NETGAIN, as a business that created,
5 maintained, preserved, and stored records of the care, products and services that Plaintiff and the
6 Class members received in the State of California from NH and/or other providers of health care,
7 health care service plans, pharmaceutical companies, and contractors, as defined by the Act, is and
8 was organized for the purpose of maintaining medical information, within the meaning of Civil
9 Code § 56.05(j), in order to make the information available to Plaintiff and the Class members or to
10 a provider of health care at the request of Plaintiff and the Class members or a provider of health
11 care, for purposes of allowing Plaintiff and the Class members to manage their information, or for
12 the diagnosis and treatment of Plaintiff and the Class members, is and was deemed to be a "provider
13 of health care," within the meaning of Civil Code § 56.05(m).

14 33. Alternatively, at all times relevant to this action, including the period from October
15 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NETGAIN is and was a recipient of
16 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
17 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
18 further disclosing that medical information except in accordance with a new authorization that
19 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
20 of this chapter or by law.

21 34. Alternatively, at all times relevant to this action, including the period from October
22 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NETGAIN is and was a recipient
23 of medical information of Plaintiff and the Class members pursuant to an authorization as provided
24 by the Act, and was prohibited from further disclosing such medical information unless in
25 accordance with a new authorization that meets the requirements of Section 56.21, or as specifically
26 required or permitted by other provisions of this chapter or by law.

27 35. As a provider of health care and/or other authorized recipient of personal and
28 confidential medical information, NETGAIN is required by the Act to ensure that medical

1 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
2 patients' authorization, and to protect and preserve the confidentiality of the medical information
3 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

4 36. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, HCP created, maintained, preserved, and stored records of the care, services and
6 products, including the names, addresses, dates of birth, diagnosis/treatment information and
7 treatment cost information of Plaintiff and the Class (all of which constitutes medical information,
8 as that term is defined and set forth in the Act), that Plaintiff and other Class members received in
9 the State of California from NH and other HCP providers of health care on its computer server.

10 37. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, NH created, maintained, preserved, and stored records of the care, services and
12 products, including the names, addresses, dates of birth, diagnosis/treatment information and
13 treatment cost information of Plaintiff and the SubClass (all of which constitutes medical
14 information, as that term is defined and set forth in the Act), that Plaintiff and other SubClass
15 members received in the State of California from NH on its computer network.

16 38. As a result, on or before October 30, 2020, Defendants possessed Plaintiff's,
17 SubClass' and the Class' medical information, in electronic and physical form, in possession of or
18 derived from Defendants regarding their medical history, mental or physical condition, or treatment.
19 Such medical information included or contained an element of personal identifying information
20 sufficient to allow identification of Plaintiff, the SubClass and the Class, such as their names,
21 addresses, dates of birth, social security numbers, phone numbers and/or email addresses, or other
22 information that, alone or in combination with other publicly available information, reveals their
23 identity.

24 39. As providers of health care, contractors, and/or other recipients of medical
25 information, Defendants are required by the Act to ensure that medical information regarding a
26 patient is not disclosed or disseminated or released without their patients' authorization, and to
27 protect and preserve the confidentiality of the medical information regarding a patient, under Civil
28 Code §§ 56.10, 56.26, 56.36, and 56.101.

1 40. As providers of health care, contractors, and/or other recipients of medical
2 information, Defendants are required by the Act not to disclose medical information regarding a
3 patient without first obtaining an authorization under Civil Code §§ 56.10 and 56.26.

4 41. As providers of health care, contractors, and/or other recipients of medical
5 information, Defendants are required by the Act to create, maintain, preserve, and store medical
6 information in a manner that preserves the confidentiality of the information contained therein
7 under Civil Code § 56.101(a).

8 42. As providers of health care, contractors, and/or other recipients of medical
9 information, Defendants are required by the Act to protect and preserve confidentiality of electronic
10 medical information of Plaintiff and the Class in its possession under Civil Code § 56.101(b)(1)(A).

11 43. As providers of health care, contractors, and/or other recipients of medical
12 information, Defendants are required by the Act to take appropriate preventive actions to protect the
13 confidential information or records against release consistent with Defendants' obligations under
14 the Act, under Civil Code § 56.36(e)(2)(E), or other applicable state law, and the Health Insurance
15 Portability and Accountability Act of 1996 (Public Law 104-191) (HIPAA) and all HIPAA
16 Administrative Simplification Regulations in effect on January 1, 2012, contained in Parts 160, 162,
17 and 164 of Title 45 of the Code of Federal Regulations, and Part 2 of Title 42 of the Code of
18 Federal Regulations, including, but not limited to, all of the following:

- 19 i. Developing and implementing security policies and procedures.
- 20 ii. Designating a security official who is responsible for developing and implementing
21 its security policies and procedures, including educating and training the workforce.
- 22 iii. Encrypting the information or records, and protecting against the release or use of
23 the encryption key and passwords, or transmitting the information or records in a
24 manner designed to provide equal or greater protections against improper
25 disclosures.

26 44. At all times relevant to this action, including the period from October 22, 2020 to
27 December 3, 2020, HCP created, maintained, preserved, and stored Plaintiff's and the Class
28 members' medical information in an un-encrypted format.

1 45. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, NH created, maintained, preserved, and stored Plaintiff’s and the SubClass
3 members’ medical information in an un-encrypted format.

4 46. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, NH disclosed and/or delivered Plaintiff’s and the SubClass members’ medical
6 information to HCP and NETGAIN. At all times relevant to this action, NH did not obtain written
7 authorization from the Plaintiff and the SubClass prior to disclosing and/or delivering Plaintiff’s and
8 the SubClass members’ medical information to HCP and NETGAIN. Furthermore, NH’s disclosure
9 of and/or delivery of Plaintiff’s and the SubClass members’ medical information to HCP and
10 NETGAIN was not permissible without written authorization from the Plaintiff and the SubClass or
11 under any exemption under Civil Code § 56.10(c).

12 47. At all times relevant to this action, including the period from October 22, 2020 to
13 December 3, 2020, HCP created, maintained, preserved, stored, disclosed and/or delivered
14 Plaintiff’s and the Class members’ medical information to NETGAIN on its computer servers. At
15 all times relevant to this action, HCP did not obtain written authorization from the Plaintiff and the
16 Class prior to creating, maintaining, preserving, storing, disclosing and/or delivering Plaintiff’s and
17 the Class members’ medical information to NETGAIN on its computer servers. Furthermore,
18 NETGAIN’s disclosure of and/or delivery of Plaintiff’s and the Class members’ medical
19 information to NETGAIN on its computer servers was not permissible without written authorization
20 from the Plaintiff and the Class or under any exemption under Civil Code § 56.10(c).

21 48. By law, the HIPAA Privacy Rule applies only to covered entities, e.g. health care
22 providers. However, most health care providers do not carry out all of their health care activities
23 and functions by themselves. Instead, they often use the services of a variety of other persons or
24 businesses. The Privacy Rule allows covered providers to disclose protected health information
25 (PHI) to these “business associates” if the providers obtain assurances that the business associate
26 will use the information only for the purposes for which it was engaged by the covered entity, will
27 safeguard the information from misuse, and will help the covered entity comply with some of the
28 covered entity’s duties under the Privacy Rule. Covered entities may disclose PHI to an entity in its

1 role as a business associate only to help the covered entity carry out its health care functions – not
2 for the business associate’s independent use or purposes, except as needed for the proper
3 management and administration of the business associate. The Privacy Rule requires that a covered
4 entity obtain assurances from its business associate that the business associate will appropriately
5 safeguard the PHI it receives or creates on behalf of the covered entity. The satisfactory assurances
6 must be in writing, whether in the form of a contract or other agreement between the covered entity
7 and the business associate.

8 49. When hiring and monitoring a service provider or business associate such as
9 NETGAIN, HCP and NH knew or should have known that they had a duty to inquire about
10 potential service providers’ and business associates’ cybersecurity programs and how such
11 programs are maintained. HCP and NH knew or should have known that they had a duty to
12 compare potential service providers’ and business associates’ cybersecurity programs to the
13 industry standards adopted by other healthcare providers, and should evaluate potential service
14 providers’ track records in the industry by reviewing public information about data security
15 incidents and litigation. HCP and NH knew or should have known that they had a duty to also ask
16 potential service providers and business associates about whether they have experienced any
17 cybersecurity incidents and how such incidents were handled, as well as whether the potential
18 service provider has an insurance policy in place that would cover losses caused by cybersecurity
19 breaches (including losses caused by internal and external threats). HCP and NH knew or should
20 have known that they had a duty to review service provider and business associates contracts to
21 ensure that the contracts require the service providers to comply, on an ongoing basis, with
22 cybersecurity and information security standards (and avoid contract provisions that limit service
23 providers’ responsibility for cybersecurity and information technology breaches). Finally, HCP and
24 NH knew or should have known that they had a duty to pay particular attention to contract terms
25 relating to confidentiality, the use and sharing of information, notice by the vendor of cybersecurity
26 risk assessments and audit reports, cybersecurity breaches and records retention and destruction.

27 50. Alternatively, Plaintiff alleges on information and belief that HCP’s and NH’s
28 disclosure of and/or delivery of Plaintiff’s, the Class’ and the SubClass’ medical information to

1 NETGAIN was either without a business associate agreement or pursuant to a business associate
2 agreement that was not permissible under the Privacy Rule or any exemption under Civil Code §
3 56.10(c), and/or because HCP and NH negligently failed to obtain reasonable assurances and
4 negligently failed to monitor and conduct assessments of NETGAIN to verify that NETGAIN
5 would comply with HIPAA privacy regulations and to follow guidelines and policies to maintain
6 the privacy, confidentiality, including by encryption, and otherwise reasonably protect Plaintiff’s
7 and the Class’ medical information from disclosure and/or release to at least one unauthorized third
8 party “user” prior to and after HCP’s and NH’s disclosure of and/or delivery of Plaintiff’s and the
9 Class members’ medical information to NETGAIN.

10 51. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, at least one “unauthorized third party gained access to Netgain’s digital
12 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
13 obtained certain files” containing including Plaintiff’s, the SubClass’ and the Class’ medical
14 information (i.e., their names, addresses, dates of birth, diagnosis/treatment information and
15 treatment cost information) that was located on a NETGAIN server in an un-encrypted format, as
16 represented in HCP’s “**Notice of Data Breach**” form letter submitted to the Attorney General of the
17 State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**.

18 52. Defendants had the resources necessary to protect and preserve confidentiality of
19 electronic medical information of Plaintiff, the SubClass and the Class in their possession, but
20 neglected to adequately implement data security measures as required by HIPPA and the Act,
21 despite their obligation to do so.

22 53. Additionally, the risk of vulnerabilities in its computer and data systems of being
23 exploited by an unauthorized third party trying to steal Plaintiff’s, the SubClass’ and the Class’
24 electronic personally identifying and medical information was foreseeable and/or known to
25 Defendants. The California Data Breach Report 2012-2015, issued in February 2016 by Attorney
26 General, Kamala D. Harris, reported, “Malware and hacking presents the greatest threat, both in the
27 number of breaches and the number of records breached” and “Social Security numbers and
28 medical information – was breached than other data types.” Moreover, as Attorney General further

1 reported, just because “[e]xternal adversaries cause most data breaches, [] this does not mean that
2 organizations are solely victims; they are also stewards of the data they collect and maintain. People
3 entrust businesses and other organizations with their data on the understanding that the
4 organizations have a both an ethical and a legal obligation to protect it from unauthorized access.
5 Neglecting to secure systems and data opens a gateway for attackers, who take advantage of
6 uncontrolled vulnerabilities.” Regarding encryption, Attorney General instructed in California Data
7 Breach Report 2012-2015, “As we have said in the past, breaches of this type are preventable.
8 Affordable solutions are widely available: strong full-disk encryption on portable devices and
9 desktop computers when not in use.[] Even small businesses that lack full time information security
10 and IT staff can do this. They owe it to their patients, customers, and employees to do it now.”

11 54. More recently the HIPAA Journal posted on November 1, 2018 warned, “Healthcare
12 organization[s] need to ensure that their systems are well protected against cyberattacks, which
13 means investing in technologies to secure the network perimeter, detect intrusions, and block
14 malware and phishing threats.”

15 55. Further, it also was foreseeable and/or known to Defendants that negligently
16 creating, maintaining, preserving, and/or storing Plaintiff’s, the SubClass’ and the Class’ medical
17 and personal identifying information, in electronic form, onto Defendants’ computer networks in a
18 manner that did not preserve the confidentiality of the information could have a devastating effect
19 on them. As reported in the California Data Breach Report 2012-2015, “There are real costs to
20 individuals. Victims of a data breach are more likely to experience fraud than the general public,
21 according to Javelin Strategy & Research. In 2014, 67 percent of breach victims in the U.S. were
22 also victims of fraud, compared to just 25 percent of all consumers.”

23 56. To be successful, phishing relies on a series of affirmative acts by a company and its
24 employees such as clicking a link, downloading a file, or providing sensitive information. Once
25 criminals gained access to the email accounts of a company and its employees, the email servers
26 communicated—that is, disclosed—the contents of those accounts to the criminals. “Phishing
27 scams are one of the most common ways hackers gain access to sensitive or confidential
28 information. Phishing involves sending fraudulent emails that appear to be from a reputable

1 company, with the goal of deceiving recipients into either clicking on a malicious link or
2 downloading an infected attachment, usually to steal financial or confidential information.”
3 (<https://www.varonis.com/blog/data-breach-statistics/>). As posted on April 21, 2020, the FBI had
4 issued a fresh warning [Alert Number MI-000122-MW] following an increase in COVID-19
5 phishing scams targeting healthcare providers.

6 57. At all times relevant to this action, including the period from October 22, 2020 to
7 December 3, 2020, Defendants negligently created, maintained, preserved, and/or stored Plaintiff’s,
8 the SubClass’ and the Class’ medical information, including Plaintiff’s, the SubClass’ and the
9 Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
10 information, in electronic form, onto Defendants’ computer networks in a manner that did not
11 preserve the confidentiality of the information, and negligently failed to protect and preserve
12 confidentiality of electronic medical information of Plaintiff, the SubClass and the Class in their
13 possession, as required by HIPPA and the Act, and specifically, under Civil Code §§ 56.10(a),
14 56.26(a), 56.36(e)(2)(E), 56.101(a), and 56.101(b)(1)(A), and according to their written
15 representations to Plaintiff and the Class.

16 58. Had Defendants taken such appropriate preventive actions, fix the deficiencies in
17 their data security systems and adopted security measures as required by HIPPA and the Act from
18 October 22, 2020 to December 3, 2020, Defendants could have prevented Plaintiff’s and the Class’
19 electronic medical information within Defendants’ computer networks from being accessed and
20 actually viewed by unauthorized third parties.

21 59. At all times relevant to this action, including the period of from October 22, 2020 to
22 December 3, 2020, NH, by disclosing and/or delivering Plaintiff’s and the SubClass’ personal
23 identifying and medical information to HCP, allowed Plaintiff’s and the SubClass’ personal
24 identifying and medical information to be accessed and actually viewed by at least one unauthorized
25 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
26 Code § 56.10(a).

27 60. At all times relevant to this action, including the period of from October 22, 2020 to
28 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic

1 medical information of Plaintiff and the SubClass on NETGAIN's computer server, allowed
2 Plaintiff's and the SubClass' medical and personal identifying information to be accessed and
3 actually viewed by at least one unauthorized third party, without first obtaining an authorization,
4 constituting a disclosure in violation of Civil Code § 56.10(a).

5 61. At all times relevant to this action, including the period from October 22, 2020 to
6 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
7 medical information of Plaintiff and the Class on NETGAIN's computer server, allowed Plaintiff's
8 and the Class' medical and personal identifying information to be accessed and actually viewed by
9 at least one unauthorized third party, without first obtaining an authorization, constituting a
10 disclosure in violation of Civil Code § 56.10(a).

11 62. At all times relevant to this action, including the period from October 22, 2020 to
12 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
13 medical information of Plaintiff and the Class on NETGAIN's computer server, allowed Plaintiff's
14 and the Class' medical and personal identifying information to be accessed and actually viewed by
15 at least one unauthorized third party, without first obtaining an authorization, constituting a
16 disclosure in violation of Civil Code § 56.26(a).

17 63. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, NH, by disclosing and/or delivering Plaintiff's and the SubClass members'
19 medical and personal identifying information to HCP, allowed Plaintiff's and the SubClass' medical
20 and personal identifying information to be accessed and actually viewed by at least one
21 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

22 64. At all times relevant to this action, including the period from October 22, 2020 to
23 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic
24 medical information of Plaintiff and the SubClass on NETGAIN's computer server, allowed
25 Plaintiff's and the SubClass' medical and personal identifying information to be accessed and
26 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
27 Code § 56.101(a).

28

1 65. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
3 medical information of Plaintiff and the Class on NETGAIN’s computer server, allowed Plaintiff’s
4 and the Class’ medical and personal identifying information to be accessed and actually viewed by
5 at least one unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

6 66. At all times relevant to this action, including the period from October 22, 2020 to
7 December 3, 2020, NH, by disclosing and/or delivering Plaintiff’s and the SubClass members’
8 medical and personal identifying information to HCP, allowed Plaintiff’s and the SubClass’ medical
9 and personal identifying information to be accessed and actually viewed by at least one
10 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

11 67. At all times relevant to this action, including the period from October 22, 2020 to
12 December 3, 2020, NH’s negligent failure to protect and preserve confidentiality of electronic
13 medical information of Plaintiff and the SubClass, on NETGAIN’s computer server, allowed
14 Plaintiff’s and the SubClass’ medical and personal identifying information to be accessed and
15 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
16 Code § 56.101(b)(1)(A).

17 68. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, HCP’s negligent failure to protect and preserve confidentiality of electronic
19 medical information of Plaintiff and the Class, on NETGAIN’s computer server, allowed Plaintiff’s
20 and the Class’ medical and personal identifying information to be accessed and actually viewed by
21 at least one unauthorized third party, constituting a release in violation of Civil Code §
22 56.101(b)(1)(A).

23 69. On or about April 12, 2021, HCP caused a form letter, entitled “**Notice of Data**
24 **Breach,**” dated April 12, 2021, signed by Henry Tuttle, President & Chief Executive Officer,
25 Health Center Partners of Southern California, to be mailed to Plaintiff and the Class, informing
26 them, in part, of “a recent data security incident experienced by Netgain Technology, LLC
27 (‘Netgain’), the IT service provider for Health Center Partners of Southern California (‘HCP’)” and
28 stating, in part, “HCP supports community health centers in a variety of ways, including

1 collaborative grant-funded programs and services for Neighborhood Healthcare.... **What**
2 **Happened:** Netgain recently informed HCP that it had experienced a data security incident that
3 involved systems containing HCP data.... According to Netgain, in late September 2020, an
4 unauthorized third party gained access to Netgain’s digital environment, and between October 22,
5 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data.
6 Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the
7 attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the
8 data.... The information involved varies depending on the individual but may include the following:
9 name, address, date of birth, diagnosis/treatment information and treatment cost information. Once
10 we learned that HCP data may have been involved in the incident, we worked with our
11 cybersecurity experts to review the impacted files and identify the individuals whose information
12 was contained in such files so that we may notify such individuals. Our investigation revealed that
13 the impacted files contained your personal information.” An exemplar of HCP’s “**Notice of Data**
14 **Breach**” form letter submitted to the Attorney General of the State of California and mailed to
15 Plaintiff and the Class is attached hereto as **Exhibit A**. Plaintiff received in the mail a HCP “**Notice**
16 **of Data Breach**” form letter, addressed to her, which alerted Plaintiff that her medical and personal
17 identifying information, along with other Class members, was improperly accessed by at least one
18 unauthorized third party. As a result, Plaintiff fears that disclosure and/or release of her medical
19 and personal identifying information created, maintained, preserved, and/or stored on Defendants’
20 computer networks could subject her to harassment or abuse. Moreover, although thereafter, on
21 May 4, 2021, Plaintiff wrote both HCP and NH separately requesting further information about this
22 security incident, neither HCP nor NH provided a substantive response to her requests.

23 70. HCP’s “**Notice of Data Breach**” form letter submitted to the Attorney General of
24 the State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**, further
25 states, “**What We Are Doing:** [] We are providing you with steps that you can take to help protect
26 your personal information, and as an added precaution, we are offering you complimentary identity
27 protection services through IDX, a leader in risk mitigation and response.”
28

1 71. HCP’s “**Notice of Data Breach**” form letter concludes by making the following
2 hollow gesture, “The security of your information is a top priority for HCP, and we are committed
3 to safeguarding your data and privacy.” Other than offering “steps that you can take to help protect
4 your personal information” and “complimentary identity protection services through IDX” “as an
5 added precaution,” HCP’s “**Notice of Data Breach**” form letter does nothing to further protect
6 Plaintiff and the Class from future incidents of identity theft despite the severity of the unauthorized
7 access, viewing, exfiltration, theft, disclosure and/or release of their electronic medical and personal
8 information caused by Defendants’ violations of their duty to implement and maintain reasonable
9 security procedures and practices.

10 72. To date, other than offering “steps that you can take to help protect your personal
11 information” and “complimentary identity protection services through IDX” “as an added
12 precaution,” HCP has not offered any monetary compensation for the unauthorized disclosure
13 and/or release of Plaintiff’s and the Class’ electronic medical information under the Act. In effect,
14 HCP is shirking its responsibility for the harm it has caused, while shifting the burdens and costs of
15 its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

16 73. To date, NH has not offered any compensation for the unauthorized disclosure and/or
17 release of Plaintiff’s and SubClass’ electronic medical information under the Act. In effect, NH is
18 shirking its responsibility for the harm it has caused, while shifting the burdens and costs of its
19 wrongful conduct onto its patients, i.e. Plaintiff and the SubClass.

20 74. To date, NETGAIN has not offered any monetary compensation for the unauthorized
21 disclosure and/or release of Plaintiff’s and the Class’ electronic medical information under the Act.
22 In effect, NETGAIN is shirking its responsibility for the harm it has caused, while shifting the
23 burdens and costs of its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

24 75. Based upon the information posted on the U.S. Department of Health and Human
25 Services’ official website, HCP reported on “04/09/2021” a “Hacking/IT Incident” involving
26 “Network Server” affecting “293,516” persons, which involved a “Business Associate,” to the U.S.
27 Department of Health & Human Services’ Office for Civil Rights.

28

1 76. Based upon the information posted on the U.S. Department of Health and Human
2 Services' official website, NH reported on "04/14/2021" a "Hacking/IT Incident" involving
3 "Network Server" affecting "45,200" persons, which involved a "Business Associate," to the U.S.
4 Department of Health & Human Services' Office for Civil Rights.

5 77. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA
6 covered entities to provide notification following a breach of unsecured protected health
7 information. Following a breach of unsecured protected health information, covered entities must
8 provide notification of the breach to affected individuals. Covered entities must *only* provide the
9 required notifications if the breach involved unsecured protected health information. Unsecured
10 protected health information is protected health information (PHI) that has not been rendered
11 unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or
12 methodology specified by the Secretary of the U.S. Department of Health and Human Services in
13 guidance. Under approved guidance of the U.S. Department of Health and Human Services, PHI is
14 rendered unusable, unreadable, or indecipherable to unauthorized individuals if (1) electronic PHI
15 has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process
16 to transform data into a form in which there is a low probability of assigning meaning without use
17 of a confidential process or key" (45 CFR 164.304 definition of encryption) and (2) such
18 confidential process or key that might enable decryption has not been breached. By reporting this
19 incident to the U.S. Department of Health and Human Services, HCP and NH each has separately
20 determined and is affirming that Plaintiff's, the Class' and the SubClass' electronic PHI was either
21 not encrypted at all, or if it was encrypted, the encryption has been breached by the unauthorized
22 third party. Further, because Plaintiff's, the Class' and the SubClass' identifiable medical
23 information contained in NETGAIN's computer server was not rendered unusable, unreadable, or
24 indecipherable, the unauthorized third party or parties who "obtained" and downloaded Plaintiff's
25 and the Class' identifiable medical information was able to and did actually view Plaintiff's, the
26 Class' and the SubClass' electronic medical information contained in and "obtained" and
27 downloaded from NETGAIN's computer server. As a result, HCP and NH each has separately
28 determined and have affirmed that Plaintiff's, the Class' and the SubClass' identifiable medical

1 information contained in NETGAIN’s computer server was unencrypted and thus, the unauthorized
2 third party or parties who “obtained” and downloaded Plaintiff’s, the Class’ and the SubClass’
3 identifiable medical information was able to and did actually view Plaintiff’s, the Class’ and the
4 SubClass’ electronic medical information contained in and “obtained” and downloaded from
5 NETGAIN’s computer server. Therefore, HCP, NH and NETGAIN was negligent for failing to
6 encrypt or adequately encrypt Plaintiff’s, the Class’ and the SubClass’ electronic medical
7 information contained in NETGAIN’s computer server.

8 78. As a result, Defendants were negligent for failing to encrypt or adequately encrypt
9 Plaintiff’s, the Class’ and the SubClass’ electronic medical information on their computer networks.
10 Further, because Plaintiff’s, the Class’ and the SubClass’ identifiable medical information on
11 Defendants’ computer networks was not rendered unusable, unreadable, or indecipherable, the
12 unauthorized third party or parties who accessed Plaintiff’s, the Class’ and the SubClass’
13 identifiable medical information was able to and did view Plaintiff’s, the Class’ and the SubClass’
14 electronic medical information contained within NETGAIN’s computer server.

15 CLASS ACTION ALLEGATIONS

16 79. Plaintiff brings this action on behalf of herself individually and on behalf of all
17 others similarly situated. The putative class and subclass that Plaintiff seeks to represent is defined
18 as follows:

19 Class: All persons to whom Health Center Partners of Southern California sent a
20 notification letter of a data security incident that has occurred between October
21 22, 2020 to December 3, 2020, an exemplar of which is attached hereto as
Exhibit A.

22 SubClass: All persons to whom Neighborhood Healthcare sent a notification
23 letter of a data security incident that has occurred between November 24, 2020 to
December 3, 2020, an exemplar of which is attached hereto as **Exhibit B**.

24 The officers, directors, employees, and agents of Defendants and any “affiliate,” “principal” or
25 “subsidiary” of Defendants, as defined in the Corporations Code §§ 150, 175, and 189, respectively,
26 are excluded from the Class and the SubClass. Plaintiff reserves the right under California Rule of
27 Court 3.765 to amend or modify the Class definition with greater particularity or further division
28

1 into subclasses or limitation to particular issues as warranted, and as additional facts are discovery
2 by Plaintiff during her future investigations.

3 80. This action is properly maintainable as a class action. The members of the Class and
4 the SubClass are so numerous that joinder of all members is impracticable, if not completely
5 impossible. While the exact number of the Class is unknown to Plaintiff at this time, HCP filed a
6 report with the U.S. Department of Health & Human Services' Office for Civil Rights, on or about
7 December 28, 2020, that this incident affected 293,516 persons. The disposition of the claims of
8 the members of Class through this class action will benefit both the parties and this Court. In
9 addition, the Class and the SubClass is readily identifiable from information and records in the
10 possession of Defendants and their agents, and the Class and the SubClass is defined in objective
11 terms that make the eventual identification of the Class and the SubClass members possible and/or
12 sufficient to allow members of the Class and the SubClass identify themselves as having a right to
13 recover.

14 81. There is a well-defined community of interest among the members of the Class and
15 the SubClass because common questions of law and fact predominate, Plaintiff's claims are typical
16 of the members of the class, and Plaintiff can fairly and adequately represent the interests of the
17 Class.

18 82. Common questions of law and fact exist as to all members of the Class and the
19 SubClass and predominate over any questions affecting solely individual members of the Class and
20 the SubClass. Among the questions of law and fact common to the Class that predominate over
21 questions which may affect individual Class members, including the following:

- 22 a) Whether Defendants possessed Plaintiff's, the SubClass' and the Class' medical and
23 personal identifying information from October 22, 2020 to December 3, 2020;
24 b) Whether Defendants created, maintained, preserved and/or stored Plaintiff's, the
25 SubClass' and the Class' medical and personal identifying information, in electronic
26 form, onto Defendants' computer networks from October 22, 2020 to December 3,
27 2020;

- 1 c) Whether Defendants implemented and maintained reasonable security procedures
2 and practices to protect Plaintiff's, the SubClass' and the Class' medical and
3 personal identifying information, in electronic form, within Defendants' computer
4 networks from October 22, 2020 to December 3, 2020;
- 5 d) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
6 information, in electronic form, within Defendants' computer networks from October
7 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
8 exposed by an unauthorized third party;
- 9 e) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
10 information, in electronic form, within Defendants' computer networks from October
11 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
12 exposed by an unauthorized third party without the prior written authorization of
13 Plaintiff, the SubClass and the Class, as required by Civil Code §§ 56.10 and 56.26;
- 14 f) Whether Defendants' creation, maintenance, preservation and/or storage of
15 Plaintiff's, the SubClass' and the Class' medical and personal identifying
16 information, in electronic form, within Defendants' computer networks, accessed,
17 viewed, exfiltrated and/or publicly exposed by an unauthorized third party was
18 permissible without written authorization from Plaintiff, the SubClass and the Class
19 or under any exemption under Civil Code § 56.10(c);
- 20 g) Whether Defendants' creation, maintenance, preservation and/or storage of
21 Plaintiff's, the SubClass' and the Class' medical and personal identifying
22 information, in electronic form, within Defendants' computer networks, accessed,
23 viewed, exfiltrated and/or publicly exposed by an unauthorized third party
24 constitutes a release in violation of Civil Code §56.101;
- 25 h) Whether the timing of HCP's notice that Plaintiff's and the Class' medical and
26 personal identifying information, in electronic form, was accessed, viewed,
27 exfiltrated and/or publicly exposed by an unauthorized third party, was given in the
28 most expedient time possible and without reasonable delay;

1 i) Whether Defendants' conduct constitute unlawful, fraudulent or unfair practices in
2 violation of Business and Professions Code §§ 17200, *et seq.*; and

3 j) Whether Plaintiff, the SubClass and the Class are entitled to actual, nominal or
4 statutory damages, injunctive relief and/or restitution.

5 83. Plaintiff's claims are typical of those of the other SubClass and Class members
6 because Plaintiff, like every other SubClass and Class member, were exposed to virtually identical
7 conduct and now suffer from the same violations of the law as other SubClass and Class members.

8 84. Plaintiff will fairly and adequately protect the interests of the SubClass and the
9 Class. Moreover, Plaintiff has no interest that is contrary to or in conflict with those of the
10 SubClass and the Class, she seeks to represent. In addition, Plaintiff has retained competent counsel
11 experienced in class action litigation to further ensure such protection and intend to prosecute this
12 action vigorously.

13 85. The nature of this action and the nature of laws available to Plaintiff and the other
14 SubClass and Class members make the use of the class action format a particularly efficient and
15 appropriate procedure to afford relief to Plaintiff and the other SubClass and Class members for the
16 claims alleged and the disposition of whose claims in a class action will provide substantial benefits
17 to both the parties and the Court because:

18 a) If each of the SubClass and the Class members were required to file an individual
19 lawsuit, the Defendants would necessarily gain an unconscionable advantage since
20 they would be able to exploit and overwhelm the limited resources of each individual
21 member of the SubClass and Class with its vastly superior financial and legal
22 resources;

23 b) The costs of individual suits could unreasonably consume the amounts that would be
24 recovered;

25 c) Proof of a common business practice or factual pattern which Plaintiff experienced is
26 representative of that experienced by the SubClass and the Class and will establish
27 the right of each of the members to recover on the causes of action alleged;

28

- 1 d) Individual actions would create a risk of inconsistent results and would be
- 2 unnecessary and duplicative of this litigation; and
- 3 e) The disposition of the claims of the members of the SubClass and the Class through
- 4 this class action will produce salutary by-products, including a therapeutic effect
- 5 upon those who indulge in fraudulent practices, and aid to legitimate business
- 6 enterprises by curtailing illegitimate competition.

7 86. The prosecution of separate actions by individual members of the SubClass and the
8 Class would create a risk of inconsistent or varying adjudications with respect to individual
9 members of the SubClass and the Class, which would establish incompatible standards of conduct
10 for the Defendants in the State of California and would lead to repetitious trials of the numerous
11 common questions of fact and law in the State of California. Plaintiff knows of no difficulty that
12 will be encountered in the management of this litigation that would preclude its maintenance as a
13 class action. As a result, a class action is superior to other available methods for the fair and
14 efficient adjudication of this controversy.

15 87. Notice to the members of the SubClass and the Class may be made by e-mail or first-
16 class mail addressed to all persons who have been individually identified by Defendants and who
17 have been given notice of the data breach.

18 88. Plaintiff, the SubClass and the Class have suffered irreparable harm and damages
19 because of Defendants' wrongful conduct as alleged herein. Absent certification, Plaintiff, the
20 SubClass and the Class will continue to be damaged and to suffer by the unauthorized disclosure
21 and/or release of their medical and personal identifying information, thereby allowing these
22 violations of law to proceed without remedy.

23 89. Moreover, Plaintiff's, the SubClass' and the Class' individual damages are
24 insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendants'
25 violations of law inflicting substantial damages in the aggregate would go unremedied. In addition,
26 Defendants have acted or refused to act on grounds generally applicable to Plaintiff, the SubClass
27 and the Class, thereby making appropriate final injunctive relief with respect to, the Class as a
28 whole.

FIRST CAUSE OF ACTION
Violations of the Confidentiality of Medical Information Act
California Civil Code §§ 56, et seq.
(On Behalf of Plaintiff and the SubClass Against NH)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

90. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if fully stated herein.

91. At all times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH is considered a “provider of health care,” within the meaning of Civil Code § 56.05(m), and maintained and continues to maintain “medical information” within the meaning of Civil Code § 56.05(j), of Plaintiff and the SubClass.

92. Plaintiff and the SubClass are “patients” of NH within the meaning of Civil Code § 56.05(k) and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure and/or release of their medical information could subject them to harassment or abuse.

93. At all times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH negligently created, maintained, preserved, and/or stored Plaintiff’s and the SubClass’ medical information, including Plaintiff’s and the SubClass’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in electronic form, onto Defendants’ computer networks in a manner that did not preserve the confidentiality of the information, and negligently failed to protect and preserve confidentiality of electronic medical information of Plaintiff and the SubClass in its possession, as required by the Act, and specifically, under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and 56.36(e)(2)(E), and according to their written representations to Plaintiff and the SubClass.

94. Due to NH’s disclosure and/or delivery Plaintiff’s and the SubClass members’ medical and personal identifying information to HCP without written authorization from Plaintiff and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff’s and the SubClass’ medical information, including Plaintiff’s and the SubClass’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be accessed and actually viewed by at least one unauthorized third party, without first obtaining an

1 authorization, constituting a disclosure in violation of Civil Code §§ 56.10, 56.13, 56.245, and
2 56.26(a).

3 95. Due to NH's negligent creation, maintenance, preservation and/or storage of
4 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server, NH
5 allowed Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass'
6 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
7 electronic form, to be accessed and actually viewed by at least one unauthorized third party, without
8 first obtaining an authorization, constituting a disclosure in violation of Civil Code §§ 56.10, 56.13,
9 56.245, and 56.26(a).

10 96. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass members'
11 medical and personal identifying information to HCP without written authorization from Plaintiff
12 and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff's and
13 the SubClass' medical information, including Plaintiff's and the SubClass' names, addresses, dates
14 of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be
15 accessed and actually viewed by at least one unauthorized third party, constituting a release in
16 violation of Civil Code § 56.101(a).

17 97. Due to NH's negligent creation, maintenance, preservation and/or storage of
18 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server,
19 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
20 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
21 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
22 constituting a release in violation of Civil Code § 56.101(a).

23 98. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass' medical
24 information and personal identifying information to HCP without written authorization from
25 Plaintiff and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed
26 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
27 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
28

1 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
2 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

3 99. Due to NH’s negligent creation, maintenance, preservation and/or storage of
4 Plaintiff’s and the SubClass members’ medical information on NETGAIN’s computer server, NH
5 allowed Plaintiff’s and the SubClass’ medical information, including Plaintiff’s and the SubClass’
6 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
7 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
8 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

9 100. As a result of NH’s above-described conduct in violation of the Act, Plaintiff and the
10 SubClass have suffered damages from the unauthorized disclosure and/or release of their medical
11 and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

12 101. As a result of NHs’ above-described conduct in violation of the Act, Plaintiff and the
13 SubClass seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
14 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
15 Code § 56.36(b)(2).

16 **SECOND CAUSE OF ACTION**
17 **Violations of the Confidentiality of Medical Information Act**
18 **California Civil Code §§ 56, et seq.**
19 **(On Behalf of Plaintiff and the Class Against HCP)**

20 102. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
21 fully stated herein.

22 103. At all times relevant to this action, including the period from October 22, 2020 to
23 December 3, 2020, HCP is considered a “provider of health care” within the meaning of Civil Code
24 § 56.05(m), a “contractor” under Civil Code § 56.05(d), and/or “engaged in the business of
25 furnishing administrative services to programs that provide payment for health care services” under
26 Civil Code § 56.26(a), and maintained and continues to maintain “medical information” within the
27 meaning of Civil Code § 56.05(j), of Plaintiff and the Class.
28

1 104. Plaintiff and the Class are “patients” within the meaning of Civil Code § 56.05(k)
2 and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure
3 and/or release of their medical information could subject them to harassment or abuse.

4 105. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, HCP negligently created, maintained, preserved, and/or stored Plaintiff’s and the
6 Class’ medical information, including Plaintiff’s and the Class’ names, addresses, dates of birth,
7 diagnosis/treatment information and treatment cost information, in electronic form, onto
8 NETGAIN’s computer server in a manner that did not preserve the confidentiality of the
9 information, and negligently failed to protect and preserve confidentiality of electronic medical
10 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
11 under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
12 56.36(e)(2)(E).

13 106. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
14 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
15 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
16 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
17 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
18 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
19 Code §§ 56.10, 56.13, 56.245, and 56.26(a).

20 107. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
21 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
22 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
23 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
24 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
25 third party, constituting a release in violation of Civil Code § 56.101(a).

26 108. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
27 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
28 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s

1 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
2 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
3 third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

4 109. As a result of HCP’s above-described conduct in violation of the Act, Plaintiff and
5 the Class have suffered damages from the unauthorized disclosure and/or release of their medical
6 and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

7 110. As a result of HCP’s above-described conduct in violation of the Act, Plaintiff and
8 the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
9 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
10 Code § 56.36(b)(2).

11 **THIRD CAUSE OF ACTION**
12 **Violations of the Confidentiality of Medical Information Act**
13 **California Civil Code §§ 56, et seq.**
14 **(On Behalf of Plaintiff and the Class Against NETGAIN)**

15 111. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
16 fully stated herein.

17 112. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, NETGAIN is considered a “provider of health care” within the meaning of Civil
19 Code § 56.05(m), and maintained and continues to maintain “medical information” within the
20 meaning of Civil Code § 56.05(j), of Plaintiff and the Class.

21 113. Plaintiff and the Class are “patients” within the meaning of Civil Code § 56.05(k)
22 and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure
23 and/or release of their medical information could subject them to harassment or abuse.

24 114. At all times relevant to this action, including the period from October 22, 2020 to
25 December 3, 2020, NETGAIN negligently created, maintained, preserved, and/or stored Plaintiff’s
26 and the Class’ medical information, including Plaintiff’s and the Class’ names, addresses, dates of
27 birth, diagnosis/treatment information and treatment cost information, in electronic form, onto
28 NETGAIN’s computer server in a manner that did not preserve the confidentiality of the
information, and negligently failed to protect and preserve confidentiality of electronic medical

1 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
2 under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
3 56.36(e)(2)(E).

4 115. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
5 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
6 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
7 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
8 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
9 unauthorized third party, without first obtaining an authorization, constituting a disclosure in
10 violation of Civil Code §§ 56.10, 56.13, 56.245, and 56.26(a).

11 116. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
12 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
13 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
14 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
15 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
16 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

17 117. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
18 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
19 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
20 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
21 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
22 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

23 118. As a result of NETGAIN's above-described conduct in violation of the Act, Plaintiff
24 and the Class have suffered damages from the unauthorized disclosure and/or release of their
25 medical and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

26 119. As a result of NETGAIN's above-described conduct in violation of the Act, Plaintiff
27 and the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
28

1 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
2 Code § 56.36(b)(2).

3 **FOURTH CAUSE OF ACTION**
4 **Breach of California Security Notification Laws**
5 **California Civil Code § 1798.82**
6 **(On Behalf of Plaintiff and the Class Against HCP)**

7 120. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
8 fully stated herein.

9 121. Pursuant to Civil Code § 1798.82(a), “A person or business that conducts business in
10 California, and that owns or licenses computerized data that includes personal information, shall
11 disclose a breach of the security of the system following discovery or notification of the breach in
12 the security of the data to a resident of California (1) whose unencrypted personal information was,
13 or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted
14 personal information was, or is reasonably believed to have been, acquired by an unauthorized
15 person and the encryption key or security credential was, or is reasonably believed to have been,
16 acquired by an unauthorized person and the person or business that owns or licenses the encrypted
17 information has a reasonable belief that the encryption key or security credential could render that
18 personal information readable or usable. The disclosure shall be made in the most expedient time
19 possible and without unreasonable delay, consistent with the legitimate needs of law enforcement,
20 as provided in subdivision (c), or any measures necessary to determine the scope of the breach and
21 restore the reasonable integrity of the data system.” Prior to passages of such statute, the California
22 State Assembly cited an incident where authorities knew of the breach in security for 21 days
23 “before state workers were told” as an example of “late notice.”

24 122. Civil Code § 1798.82 further provides, “(h) For purposes of this section, ‘personal
25 information’ means an individual’s first name or first initial and last name in combination with any
26 one or more of the following data elements, when either the name or the data elements are not
27 encrypted: (1) Social security number. (2) Driver’s license number or California Identification Card
28 number. (3) Account number, credit or debit card number, in combination with any required
security code, access code, or password that would permit access to an individual's financial

1 account. (4) Medical information. (5) Health insurance information. (i) (2) For purposes of this
2 section, ‘medical information’ means any information regarding an individual’s medical history,
3 mental or physical condition, or medical treatment or diagnosis by a health care professional. (3)
4 For purposes of this section, ‘health insurance information’ means an individual’s health insurance
5 policy number or subscriber identification number, any unique identifier used by a health insurer to
6 identify the individual, or any information in an individual’s application and claims history,
7 including any appeals records.”

8 123. HCP conducts business in California and owns or licenses computerized data which
9 includes the personal information, within the meaning of Civil Code § 1798.82(h), of Plaintiff and
10 the Class.

11 124. Based upon NH’s “**Notice of Data Breach**” form letter, HCP was aware that
12 Plaintiff’s and the Class’ unencrypted personal information on NETGAIN’s computer server was,
13 or is reasonably believed to have been, acquired by an unauthorized person no later than December
14 3, 2020, but did not begin to mail notification letters to Plaintiff and the Class until April 12, 2021.
15 Thus, HCP waited at least 131 days before *beginning* to inform Plaintiff and the Class of this
16 incident and the subsequent threat to Plaintiff’s and the Class’ personal information. As a result,
17 HCP did not disclose to Plaintiff and the Class that their personal information was, or was
18 reasonably believed to have been, acquired by an unauthorized person, in the most expedient time
19 possible and without reasonable delay in violation of Civil Code § 1798.82(a). Given the example
20 of the Legislature finding that a delay of 21 days to be “late notice” under the statute, HCP’s delay
21 of 131 days before *beginning* to inform Plaintiff and the Class that their personal information was,
22 or was reasonably believed to have been, acquired by an unauthorized person by mailing HCP’s
23 form letter to Plaintiff and the Class is presumptively unreasonable notice in violation of Civil Code
24 § 1798.82(a).

25 125. Plaintiff and the Class have been injured by fact that HCP did not disclose their
26 personal information was, or was reasonably believed to have been, acquired by an unauthorized
27 person in the most expedient time possible and without reasonable delay in violation of Civil Code
28 § 1798.82(a). HCP’s delays in informing required by Civil Code § 1798.82(a) and providing all of

1 the information required by Civil Code § 1798.82(d) to Plaintiff and the Class that their personal
2 information was, or was reasonably believed to have been, acquired by an unauthorized person,
3 have prevented Plaintiff and the Class from taking steps to protect their personal information from
4 unauthorized use and/or identify theft.

5 126. Plaintiff and the Class seek recovery of their damages pursuant to Civil Code §
6 1798.84(b) and injunctive relief pursuant to Civil Code § 1798.84(e).

7 **FIFTH CAUSE OF ACTION**
8 **Unlawful and Unfair Business Acts and Practices in Violation of**
9 **California Business & Professions Code §17200, *et seq.***
10 **(On Behalf of Plaintiff, the SubClass and the Class Against All Defendants)**

11 127. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
12 fully stated herein.

13 128. The acts, misrepresentations, omissions, practices, and non-disclosures of
14 Defendants as alleged herein constituted unlawful and unfair business acts and practices within the
15 meaning of California Business & Professions Code §§ 17200, *et seq.*

16 129. By the aforementioned business acts or practices, Defendants have engaged in
17 “unlawful” business acts and practices in violation of the aforementioned statutes, including Civil
18 Code §§ 56.10(a), 56.26(a), 56.36(e)(2)(E), 56.101(a), 56.101(b)(1)(A), 1798.82(a) and 1798.82(d).
19 Plaintiff reserves the right to allege other violations of law committed by Defendants which
20 constitute unlawful acts or practices within the meaning of California Business & Professions Code
21 §§ 17200, *et seq.*

22 130. By the aforementioned business acts or practices, Defendants have also engaged in
23 “unfair” business acts or practices in that the harm caused by Defendants’ failure to maintain
24 adequate information security procedures and practices, including but not limited to, failing to take
25 adequate and reasonable measures to ensure its data systems were protected against unauthorized
26 intrusions, failing to properly and adequately educate and train its employees, failing to put into
27 place reasonable or adequately computer systems and security practices to safeguard patients’
28 identifiable medical information including access restrictions and encryption, failing to have
adequate privacy policies and procedures in place that did not preserve the confidentiality of the

1 medical and personal identifying information of Plaintiff, the SubClass and the Class in their
2 possession, and failing to protect and preserve confidentiality of electronic medical information of
3 Plaintiff, the SubClass and the Class in their possession against disclosure and/or release, outweighs
4 the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous,
5 unethical, deceitful and offensive, and causes substantial injury to Plaintiff, the SubClass and the
6 Class.

7 131. Defendants have obtain money and property from Plaintiff, the SubClass and the
8 Class because of the payment of the services and products they received from Defendants. Plaintiff,
9 the SubClass and the Class have suffered an injury in fact by acquiring less in their transactions
10 with Defendants for the services and products they received from Defendants than they otherwise
11 would have if Defendants would had adequately protected the confidentiality of their medical and
12 personal identifying information.

13 132. Pursuant to the Business & Professions Code § 17203, Plaintiff, the SubClass and the
14 Class seek an order of this Court requiring Defendants awarding Plaintiff and the Class restitution
15 of monies wrongfully acquired by Defendants in the form of payments for services by means of
16 such unlawful, fraudulent and unfair business acts and practices, so as to restore any and all monies
17 to Plaintiff, the SubClass and the Class which were acquired and obtained by means of such
18 unlawful, fraudulent and unfair business acts and practices, which ill-gotten gains are still retained
19 by Defendants.

20 133. The aforementioned unlawful, fraudulent and unfair business acts or practices
21 conducted by Defendants have been committed in the past and continues to this day. Defendants
22 have failed to acknowledge the wrongful nature of their actions. Defendants have not corrected or
23 publicly issued comprehensive corrective notices to Plaintiff, the SubClass and the Class, and have
24 not corrected or enacted adequate privacy policies and procedures to protect and preserve
25 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
26 Class in their possession.

27
28

1 134. Because of Defendants' aforementioned conduct, Plaintiff, the SubClass and the
2 Class have no other adequate remedy of law in that absent injunctive relief from the Court and
3 Defendants are likely to continue to injure Plaintiff, the SubClass and the Class.

4 135. Pursuant to Business & Professions Code § 17203, Plaintiff, the SubClass and the
5 Class also seek an order of this Court for equitable and/or injunctive relief in the form of requiring
6 Defendants to correct its illegal conduct that is necessary and proper to prevent Defendants from
7 repeating their illegal and wrongful practices as alleged above and protect and preserve
8 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
9 Class in Defendants' possession that has already been accessed, viewed, exfiltrated and/or publicly
10 exposed by at least one unauthorized third party because by way of Defendants' illegal and
11 wrongful practices set forth above. Pursuant to Business & Professions Code § 17203, Plaintiff, the
12 SubClass and the Class further seek an order of this Court for equitable and/or injunctive relief in
13 the form of requiring Defendants to publicly issue comprehensive corrective notices.

14 136. Because this case is brought for the purposes of enforcing important rights affecting
15 the public interest, Plaintiff, the SubClass and the Class also seek the recovery of attorneys' fees
16 and costs in prosecuting this action against Defendants under Code of Civil Procedure § 1021.5 and
17 other applicable law.

18 **PRAYER FOR RELIEF**

19 WHEREFORE, Plaintiff respectfully request that the Court grant Plaintiff and the proposed
20 SubClass and Class the following relief against Defendants, and each of them:

21 **As for the First, Second and Third Causes of Action**

- 22 1. For nominal damages in the amount of one thousand dollar (\$1,000) per violation to Plaintiff
23 individually and to each member of the SubClass and the Class pursuant to Civil Code §
24 56.36(b)(1);
- 25 2. For actual damages according to proof per violation pursuant to Civil Code § 56.36(b)(2);

26 **As for the Fourth Cause of Action**

- 27 3. For damages according to proof to Plaintiff individually and to each member of the Class
28 pursuant to California Civil Code § Civil Code § 1798.84(b);

1 4. For injunctive relief pursuant to California Civil Code § Civil Code § 1798.84(e);

2 **As for the Fifth Cause of Action**

3 5. For an order awarding Plaintiff, the SubClass and the Class restitution of all monies
4 wrongfully acquired by Defendants by means of such unlawful, fraudulent and unfair
5 business acts and practices;

6 6. For injunctive relief in the form of an order instructing Defendants to prohibit the
7 unauthorized release of medical and personal identifying information of Plaintiff, the
8 SubClass and the Class, and to adequately maintain the confidentiality of the medical and
9 personal identifying information of Plaintiff and the Class;

10 7. For injunctive relief in the form of an order enjoining Defendants from disclosing the
11 medical and personal identifying information of Plaintiff, the SubClass and the Class
12 without the prior written authorization of each Plaintiff, the SubClass and the Class member;

13 **As to All Causes of Action**

14 8. That the Court issue an Order certifying this action be certified as a class action on behalf of
15 the proposed SubClass and Class, appointing Plaintiff as representative of the proposed
16 SubClass and Class, and appointing Plaintiff's attorneys, as counsel for members of the
17 proposed SubClass and Class;

18 9. For an award of attorneys' fees as authorized by statute, including, but not limited to, the
19 provisions of California Code of Civil Procedure § 1021.5, and as authorized under the
20 "common fund" doctrine, and as authorized by the "substantial benefit" doctrine;

21 10. For costs of the suit;

22 11. For prejudgment interest at the legal rate; and

23 12. Any such further relief as this Court deems necessary, just, and proper.

24 Dated: June 1, 2021

KEEGAN & BAKER LLP

25 By: 
26 Patrick N. Keegan, Esq.
27 Attorney for Plaintiff
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

Plaintiff, the SubClass and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

Dated: June 1, 2021

KEEGAN & BAKER LLP

By: 
Patrick N. Keegan, Esq.
Attorney for Plaintiff

Exhibit A



C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE



NAME

ADDRESS1

ADDRESS2

CSZ

COUNTRY



SEQ
CODE 2D
Ver 1

BREAK

To Enroll, Please Call:
1-833-416-0926
Or Visit:
<https://response.idx.us/hcp-netgain-incident>
Enrollment Code: <<XXXXXXXXXX>>

April 12, 2021

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by Netgain Technology, LLC (“Netgain”), the IT service provider for Health Center Partners of Southern California (“HCP”). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTHCENTER>>. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, we engaged our own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, our health center members and partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain’s cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

Once we learned that HCP data may have been involved in the incident, we worked with our cybersecurity experts to review the impacted files and identify the individuals whose information was contained in such files so that we may notify such individuals. Our investigation revealed that the impacted files contained your personal information. **Again, we are not aware of any misuse of your personal information as a result of this incident.** Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your information.

What Information Was Involved: The information involved varies depending on the individual but may include the following: <<VARPARAGRAPH>>.

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, we have reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and we are committed to assisting their investigation into the matter.

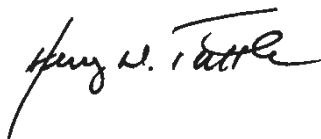
We are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include xx months of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What You Can Do: As we have stated, we are not aware of any misuse of your information as a result of this incident. However, we encourage you to follow the recommendations on the next page to help protect your information. We also encourage you to enroll in the complimentary services offered by going to <https://response.idx.us/hcp-netgain-incident> or calling 1-833-416-0926 and using the enrollment code provided above. Please note that the deadline to enroll is July 12, 2021.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-833-416-0926 between 6:00 a.m. and 6:00 p.m. Pacific Time.

The security of your information is a top priority for HCP, and we are committed to safeguarding your data and privacy.

Sincerely,

A handwritten signature in black ink, appearing to read "Henry W. Tuttle". The signature is written in a cursive, flowing style.

Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
www.consumer.ftc.gov ,	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
and	1-888-743-0023	1-877-566-7226	1-401-274-4400
www.ftc.gov/idtheft			
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Exhibit B



To Enroll, Please Call:
(833) 903-3642
Or Visit:
<https://response.idx.us/nhc-netgain-incident>
Enrollment Code: <<ENROLLMENT>>

C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

April 8, 2021

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

The privacy and security of your personal information is very important to Neighborhood Healthcare. We are writing to make you aware of an issue brought to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud hosting and managed services provider. Neighborhood Healthcare used Netgain to host some Neighborhood Healthcare files.

What Happened

On November 24, 2020, Netgain became aware of a security incident that involved unauthorized access to portions of the Netgain environment and Netgain client environments and began taking steps to investigate this incident. But, on December 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain took additional measures to contain the threat and address the issue. Netgain’s technical teams worked closely with third-party experts to remove the threat in the impacted environments and confirm that client and internal systems are protected.

Neighborhood Healthcare learned of the ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to believe that the protected health information (“PHI”) of our patients had been impacted in the incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some information including, potentially, some files containing patient PHI may have been impacted in the incident. Netgain could not confirm, at that time, what records may have been impacted in the incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood Healthcare that Netgain believed were impacted by the attackers. Those files came from a Neighborhood Healthcare server accessible by the Netgain environment. Since that time, Neighborhood Healthcare has worked to review those records, to identify individuals impacted, conduct an investigation into the incident with the assistance outside experts, and to transmit this letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood Healthcare determined that the impacted files included some of your information.

What Information Was Involved

The information involved may have included some of the following: your name, date of birth, address, Social Security Number and information about the care that you received from Neighborhood Healthcare such as insurance coverage information, physician you saw, and treatment codes. Neighborhood Healthcare is offering credit monitoring services to you at no charge. Please see the **What You Can Do** section below for information about these services including how to enroll. Please also see the **Additional Important Information** section below for further precautionary measures you may wish to take. Netgain has received assurances that the data has not gone beyond the attacker, that the data was not and will not be misused, and that the data will not be disseminated or otherwise be made publicly available.

What We Are Doing

Please know that we take this incident and the security of your personal information very seriously. Ensuring the safety of our patients' data is of the utmost importance to us. Since we learned of this incident, we have been working with Netgain to seek assurances that they are taking appropriate steps to respond to this incident. We have also conducted an investigation of the incident with the help of outside experts, and we have transitioned to a new hosting provider (a transition that was already in process when this incident occurred).

In addition, we are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include <<12/24 months>> of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What Netgain Is Doing

Netgain took several steps to strengthen its environment following the incident, including international Geo-fencing for Azure-hosted environments, deploying additional log monitoring across all servers, and additional hardening of network security rules and protocols to restrict lateral movement across environments. Netgain stated that it paid a significant amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

What You Can Do

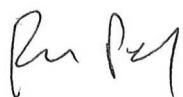
We recommend that you review the additional information enclosed. Additionally, we encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 903-3642 or going to <https://response.idx.us/nhc-netgain-incident> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 8, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

We very much regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, please call (833) 903-3642, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely



Rakesh Patel
CEO
Neighborhood Healthcare

Additional Important Information

1. Website and Enrollment. Go to <https://response.idx.us/nhc-netgain-incident> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 903-3642 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Generally. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing financial account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state's Attorney General.

5. The FTC. You can obtain information from Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

6. Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

7. Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788 equifax.com/personal/credit-report-services/ 800-525-6285	Experian Security Freeze P.O. Box 9554 Allen, TX 75013-9544 experian.com/freeze/center.html 888-397-3742	TransUnion (FVAD) P.O. Box 160 Woodlyn, PA 19094 transunion.com/credit-freeze 888-909-8872
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

More information can also be obtained by contacting the Federal Trade Commission listed above.

8. Protecting Medical Information: To date, we have no reason to believe that your PHI potentially involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following steps can help protect you from medical identity theft issues.

- Do not share health insurance cards with anyone apart from your care providers and other family members who are covered under the insurance plan or who help you with your medical care.
- Review the “explanation of benefits statements” that you receive from your health insurance company. If you see something amiss, follow up with your insurance company or the health care provider identified on the explanation of benefits to request further information.
- Ask your health insurance company for a report on all services they have paid for you for the current year. If you do not recognize an item in that list, speak with your insurance company to verify it.

9. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Telephone: (760) 929-9303
4 Facsimile: (760) 929-9260

5 Attorneys for Plaintiff JANE DOE

6
7 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
8 **FOR THE COUNTY OF COUNTY OF SAN DIEGO**

9 JANE DOE, individually and on behalf of all
others similarly situated,

10 Plaintiff,

11 vs.

12 NEIGHBORHOOD HEALTHCARE; HEALTH
13 CENTER PARTNERS OF SOUTHERN
CALIFORNIA; NETGAIN TECHNOLOGY,
14 LLC; and DOE DEFENDANTS 1-100;

15 Defendants.
16

) Case No. 37-2021-00023936-CU-BT-CTL
)

) **FIRST AMENDED CLASS ACTION**
) **COMPLAINT FOR DAMAGES,**
) **RESTITUTION, AND INJUNCTIVE**
) **RELIEF FOR VIOLATIONS OF:**

-) (1) **THE CONFIDENTIALITY OF**
) **MEDICAL INFORMATION ACT,**
) **CIVIL CODE §§ 56, ET SEQ.;**
) (2) **BREACH OF CALIFORNIA**
) **SECURITY NOTIFICATION**
) **LAWS, CALIFORNIA CIVIL CODE**
) **§ 1798.82; AND**
) (3) **BUSINESS AND PROFESSIONS**
) **CODE §§ 17200, ET SEQ.**

) **JURY TRIAL DEMANDED**
)

17
18
19 Plaintiff Jane Doe (or “Plaintiff”), by and through her attorneys, bring this class action on
20 behalf of herself individually and all others similarly situated, against Defendants Neighborhood
21 Healthcare, Health Center Partners of Southern California, and Netgain Technology, LLC
22 (collectively referred to as “Defendants”), and alleges upon information and belief as follows:

23 **INTRODUCTION**

24 1. This class action arises from the negligent and failure of Defendants to properly
25 create, maintain, preserve, and/or store confidential, medical and personal identifying information
26 of Plaintiff¹ and all other persons similarly situated which allowed an unauthorized person to gain
27

28 ¹ Pursuant to the Court’s Order Granting Plaintiff’s Ex Parte Application to Appear by Pseudonym
(ROA #14), a pseudonym has been used in place of the real name of Plaintiff because at all times

1 access to a computer database server of Defendants from October 22, 2020 to December 3, 2020,
2 causing unauthorized access, viewing, exfiltration, theft, and/or disclosure of unencrypted medical
3 and personal identifying information of Plaintiff and other persons similarly situated, to at least one
4 unauthorized person resulting in violations of the Confidentiality of Medical Information Act, Civil
5 Code §§ 56, *et seq.* (hereinafter referred to as the “Act”), the Security Notification Laws, Civil Code
6 § 1798.82, and the Business and Professions Code §§ 17200 *et seq.* Under the Act, Plaintiff, and
7 all other persons similarly situated, have the right to expect that the confidentiality of their medical
8 information in possession of Defendants and/or derived from Defendants to be reasonably
9 preserved and protected from unauthorized access, viewing, exfiltration, theft, and/or disclosure.

10 2. As alleged more fully below, failing to take adequate and reasonable measures to
11 ensure its data systems were protected against unauthorized intrusions, by failing to invest in cyber
12 security and data protection safeguards, failing to implement adequate and reasonable security
13 controls and user authorization and authentication processes, failing to limit the types of data
14 permitted to be transferred, failing to properly and adequately educate and train its employees, and
15 to put into place reasonable or adequate computer systems and security practices to safeguard
16 customers’ and patients’ medical and personal identifying information, Defendants negligently
17 created, maintained, preserved, and stored Plaintiff’s and the Class (defined *infra*) members’
18 medical and personal identifying information in possession of or derived from Defendants allowed
19 such information to be accessed and actually viewed by at least one unauthorized third party,
20 without Plaintiff’s and the Class members’ prior written authorization, which constitutes
21 unauthorized disclosure and/or release of their information in violation of Civil Code §§ 56.10(a)
22 and 56.101(a) of the Act. In fact, Defendant Health Center Partners of Southern California’s form
23 letter, entitled “**Notice of Data Breach**,” dated April 12, 2021, signed by Henry Tuttle, President &
24 Chief Executive Officer, Health Center Partners of Southern California, sent to Plaintiff and all
25 other persons similarly situated, informing them, in part, of “a recent data security incident
26 experienced by Netgain Technology, LLC (‘Netgain’), the IT service provider for Health Center
27

28 relevant to this action, Plaintiff is a health care patient under Civil Code § 56.05(k) and has individual privacy concerns and a reasonable fear of harassment in light of the nature of the case.

1 Partners of Southern California (“HCP”)) and stating, in part, “HCP supports community health
2 centers in a variety of ways, including collaborative grant-funded programs and services for
3 Neighborhood Healthcare.... **What Happened:** Netgain recently informed HCP that it had
4 experienced a data security incident that involved systems containing HCP data.... According to
5 Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital
6 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
7 obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the
8 attacker in exchange for assurances that the attacker will delete all copies of this data and that it will
9 not publish, sell, or otherwise disclose the data.... The information involved varies depending on the
10 individual but may include the following: name, address, date of birth, diagnosis/treatment
11 information and treatment cost information. Once we learned that HCP data may have been
12 involved in the incident, we worked with our cybersecurity experts to review the impacted files and
13 identify the individuals whose information was contained in such files so that we may notify such
14 individuals. Our investigation revealed that the impacted files contained your personal information.”
15 An exemplar of Defendant Health Center Partners of Southern California’s “**Notice of Data**
16 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
17 as **Exhibit A**.

18 3. Additionally, Defendant Neighborhood Healthcare caused a form letter sent on its
19 behalf, entitled “**Notice of Data Breach**,” dated April 8, 2021, signed by Rakesh Patel, CEO,
20 Neighborhood Healthcare, stating, in part, “We are writing to make you aware of an issue brought
21 to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud
22 hosting and managed services provider. Neighborhood Healthcare used Netgain to host some
23 Neighborhood Healthcare files. **What Happened** On November 24, 2020, Netgain became aware
24 of a security incident that involved unauthorized access to portions of the Netgain environment and
25 Netgain client environments and began taking steps to investigate this incident. But, on December
26 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files
27 owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain
28 took additional measures to contain the threat and address the issue. Netgain’s technical teams

1 worked closely with third-party experts to remove the threat in the impacted environments and
2 confirm that client and internal systems are protected. Neighborhood Healthcare learned of the
3 ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to
4 believe that the protected health information (“PHI”) of our patients had been impacted in the
5 incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some
6 information including, potentially, some files containing patient PHI may have been impacted in the
7 incident. Netgain could not confirm, at that time, what records may have been impacted in the
8 incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood
9 Healthcare that Netgain believed were impacted by the attackers. Those files came from a
10 Neighborhood Healthcare server accessible by the Netgain environment. Since that time,
11 Neighborhood Healthcare has worked to review those records, to identify individuals impacted,
12 conduct an investigation into the incident with the assistance outside experts, and to transmit this
13 letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood
14 Healthcare determined that the impacted files included some of your information. **What**
15 **Information Was Involved** The information involved may have included some of the following:
16 your name, date of birth, address, Social Security Number and information about the care that you
17 received from Neighborhood Healthcare such as insurance coverage information, physician you
18 saw, and treatment codes.” An exemplar of Defendant Neighborhood Healthcare’s “**Notice of Data**
19 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
20 as **Exhibit B**.

21 4. Additionally, Defendant Netgain Technology, LLC stated in a blog post, entitled
22 “What we learned as a ransomware victim – so you don’t become one,” that “late last year, Netgain
23 was the victim of a criminal ransomware attack.... to become a victim of such an attack is both
24 humbling and galvanizing.... we identified additional opportunities to strengthn our security posture
25 in a continuous journey with an ongoing commitment to ensure this remains top-of-mind. As part
26 of our incident response, we have implemented a number of these identified enhancements to our
27 security posture and have continued to progress a multipronged approach. We’ve deployed new
28

1 tools, revised policies and enforcement procedures, and implemented an advanced around-the-clock
2 managed detections and response service for proactive threat monitoring.”

3 5. Because the individually identifiable medical information and other personal
4 identifying information of Plaintiff and the Class was subject to unauthorized access and viewing by
5 at least one unauthorized third party and in violation of the Act, Plaintiff, individually and on behalf
6 of all others similarly situated, seeks from Defendants nominal damages in the amount of one
7 thousand dollars (\$1,000) for each violation under Civil Code §56.36(b)(1) and actual damages,
8 according to proof, for each violation pursuant to Civil Code § 56.36(b)(2). Further, because
9 Plaintiff also alleges Defendants’ conduct violates Business & Professions Code §§ 17200, *et seq.*,
10 Plaintiff, individually and on behalf of others similarly situated, seeks injunctive relief and
11 restitution from Defendants under Business and Professions Code § 17203.

12 6. This action, if successful, will enforce an important right affecting the public interest
13 and would confer a significant benefit, whether pecuniary or non-pecuniary, on a large class of
14 persons. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff
15 in relation to Plaintiff’s stake in the matter, and therefore class certification is appropriate in this
16 matter.

17 **JURISDICTION AND VENUE**

18 7. This Court has jurisdiction over this action under California Code of Civil Procedure
19 § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class in the aggregate
20 exceeds the \$25,000 jurisdictional minimum of this Court. Further, the amount in controversy as to
21 Plaintiff individually does not exceed \$75,000.

22 8. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of
23 Civil Procedure §§ 395(a) and 395.5 because Defendant Neighborhood Healthcare is incorporated
24 in and does business in the State of California, and employs persons located in the County of San
25 Diego and in this judicial district. Defendants have obtained medical information of Plaintiff and
26 the Class in the transaction of business in the State of California and in this judicial district, which
27 has caused both obligations and liability of Defendants to arise in the State of California and in this
28 judicial district.

1 9. Further, this action does not qualify for federal jurisdiction under the Class Action
2 Fairness Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies
3 to this action because (1) more than two-thirds of the members of the proposed Class and SubClass
4 are citizens of the State of California, and (2) Defendants are citizens of the State of California.

5 **PARTIES**

6 **A. PLAINTIFF**

7 10. Plaintiff Jane Doe is and was at all times relevant to this action a resident of the State
8 of California and citizen of the State of California. At all times relevant to this action, Plaintiff
9 JANE DOE was a patient of, received medical treatment and diagnosis from, and provided her
10 personal information, including her name, address, date of birth, social security number, phone
11 number and email address to Defendant Neighborhood Healthcare. Additionally, Plaintiff received
12 a letter addressed to her, sent on Defendant Health Center Partners of Southern California's behalf,
13 entitled "**Notice of Data Breach**," dated April 12, 2021, signed by Henry Tuttle, President & Chief
14 Executive Officer, Health Center Partners of Southern California, informing her, in part, of "a
15 recent data security incident experienced by Netgain Technology, LLC ('Netgain'), the IT service
16 provider for Health Center Partners of Southern California ('HCP')" and stating, in part, "HCP
17 supports community health centers in a variety of ways, including collaborative grant-funded
18 programs and services for Neighborhood Healthcare.... **What Happened:** Netgain recently
19 informed HCP that it had experienced a data security incident that involved systems containing
20 HCP data.... According to Netgain, in late September 2020, an unauthorized third party gained
21 access to Netgain's digital environment, and between October 22, 2020 to December 3, 2020, the
22 unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an
23 undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies
24 of this data and that it will not publish, sell, or otherwise disclose the data.... The information
25 involved varies depending on the individual but may include the following: name, address, date of
26 birth, diagnosis/treatment information and treatment cost information. Once we learned that HCP
27 data may have been involved in the incident, we worked with our cybersecurity experts to review
28 the impacted files and identify the individuals whose information was contained in such files so that

1 we may notify such individuals. Our investigation revealed that the impacted files contained your
2 personal information.” As a result, Plaintiff reasonably fears that disclosure and/or release of her
3 medical information created, maintained, preserved and/or stored on Defendants’ computer
4 networks could subject her to harassment or abuse.

5 **B. DEFENDANTS**

6 11. Defendant Neighborhood Healthcare (“NH”) is a California corporation, is registered
7 to do business and does business in the State of California (CA Corp. No. C0667935), with its
8 principal business office located at 1540 E. Valley Parkway, Escondido CA 92026, and with its
9 registered agent of service of process located at 150 La Terraza Blvd, Suite 201, Escondido CA
10 92025. On or about April 8, 2021, NH caused a form letter sent on its behalf, entitled “**Notice of**
11 **Data Breach,**” dated April 8, 2021, signed by Rakesh Patel, CEO, Neighborhood Healthcare, an
12 exemplar of which is attached hereto as **Exhibit B**, to be submitted to the Attorney General of the
13 State of California. At all times relevant to this action, NH was and is a provider of health care, a
14 contractor, and/or other authorized recipient of personal and confidential medical information, as
15 that term is defined and set forth in the Act, including the names, addresses, dates of birth,
16 diagnosis/treatment information and treatment cost information of Plaintiff and the SubClass
17 (defined *infra*), and is subject to the requirements and mandates of the Act, including but not limited
18 to Civil Code §§ 56.10, 56.101 and 56.36. At all times relevant to this action, NH was and is a
19 provider of health care and employed and employs persons located in the County of San Diego
20 and in this judicial district.

21 12. Defendant Health Center Partners of Southern California (“HCP”) is a business
22 entity doing business in the State of California, with its principal business office located at 3710
23 Ruffin Road, San Diego, CA 92123. On or about April 12, 2021, HCP caused a form letter sent on
24 its behalf, entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle,
25 President & Chief Executive Officer, Health Center Partners of Southern California, an exemplar of
26 which is attached hereto as **Exhibit A**, to be submitted to the Attorney General of the State of
27 California and to be mailed to Plaintiff and the Class. At all times relevant to this action, HCP was
28 and is a “business” within the meaning of Civil Code § 1798.140(c)(1), owns or licenses

1 computerized data which includes Plaintiff’s and the Class’ personal information, within the
2 meaning of Civil Code § 1798.82(h), collected Plaintiff’s and the Class’ personal information
3 within the meaning of Civil Code § 1798.81.5(d)(1)(A).

4 13. Defendant Netgain Technology, LLC (“NETGAIN”) is a business entity doing
5 business in the State of California, with a principal business office located at 5353 Mission Center
6 Road, Suite 202, San Diego, CA 92108. At all times relevant to this action, NETGAIN was and is
7 NH’s and HCP’s third-party vendor. On March 24, 2021, NETGAIN posted on its website a blog,
8 entitled “What we learned as a ransomware victim – so you don’t become one,” which stated, in
9 part, “In our case, late last year, Netgain was the victim of a criminal ransomware attack.... to
10 become a victim of such an attack is both humbling and galvanizing.... we identified additional
11 opportunities to strengthn our security posture in a continuous journey with an ongoing commitment
12 to ensure this remains top-of-mind. As part of our incident response, we have implemented a
13 number of these identified enhancements to our security posture and have continued to progress a
14 multipronged approach. We’ve deployed new tools, revised policies and enforcement procedures,
15 and implemented an advanced around-the-clock managed detections and response service for
16 proactive threat monitoring.”

17 **C. DOE DEFENDANTS**

18 14. The true names and capacities, whether individual, corporate, associate, or otherwise,
19 of Defendants sued herein as Doe Defendants 1 through 100, inclusive, are currently unknown to
20 Plaintiff, who therefore sue the Defendants by such fictitious names under the Code of Civil
21 Procedure § 474. Each of the Defendants designated herein as a Doe Defendant is legally
22 responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of
23 court and/or amend this complaint to reflect the true names and capacities of the Defendants
24 designated hereinafter as Doe Defendants 1 through 100 when such identities become known. Any
25 reference made to a named Defendant by specific name or otherwise, individually or plural, is also a
26 reference to the actions or inactions of Doe Defendants 1 through 100, inclusive.

27 ///

28 ///

1 **D. AGENCY/AIDING AND ABETTING**

2 15. At all times herein mentioned, Defendants, and each of them, were an agent or joint
3 venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the
4 course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the
5 acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized
6 the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

7 16. Defendants, and each of them, aided and abetted, encouraged and rendered
8 substantial assistance to the other Defendants in breaching their obligations to Plaintiff and the
9 Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially
10 assist the commissions of these wrongful acts and other wrongdoings complained of, each of the
11 Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its
12 conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals,
13 and wrongdoing.

14 **FACTUAL ALLEGATIONS**

15 17. Plaintiff alleges on information and belief that at all times relevant to this action,
16 including the period from October 22, 2020 to December 3, 2020, NH disclosed and/or released
17 Plaintiff's and the Class' medical information, in electronic and physical form, in possession of or
18 derived from NH, regarding their medical history, mental or physical condition, or treatment, to
19 HCP, pursuant to a business associate agreement. Such medical information included or contained
20 an element of personal identifying information sufficient to allow identification of Plaintiff and the
21 Class, such as their names, date of birth, addresses, medical record numbers, insurance provider,
22 electronic mail addresses, telephone numbers, or social security numbers, or other information that,
23 alone or in combination with other publicly available information, reveals their identity. As a
24 result, at all times relevant to this action, including the period from October 22, 2020 to December
25 3, 2020, HCP possessed Plaintiff's and the Class' medical information, in electronic and physical
26 form, in possession of or derived from Defendant regarding their medical history, mental or
27 physical condition, or treatment. Such medical information included or contained an element of
28 personal identifying information sufficient to allow identification of Plaintiff and the Class, such as

1 their names, date of birth, addresses, medical record numbers, insurance provider, electronic mail
 2 addresses, telephone numbers, or social security numbers, or other information that, alone or in
 3 combination with other publicly available information, reveals their identity. On its website, HCP
 4 represents that “[o]ur members collectively serve 917,000 unduplicated patients each year, for 3.9
 5 million patient visits each year, at 160 practice sites across San Diego, Riverside, Imperial
 6 counties.”² At all times relevant to this action, including the period from October 22, 2020 to
 7 December 3, 2020, HCP maintained and continues to maintain “medical information,” within the
 8 meaning of Civil Code § 56.05(j), of Plaintiff and the Class, each of which are “patients” within the
 9 meaning of Civil Code § 56.05(k).

10 18. On its website, NH represents, “At Neighborhood, our vision is a community where
 11 everyone is healthy and happy. That includes you. Our innovative services include quality care for
 12 every stage of life—from prenatal to pediatrics to primary care and beyond. From your head to your
 13 feet and everything in between, we’ve got you covered. We’re in this together.”³ On its website, NH
 14 represents that, “Primary Care [¶] Our friendly doctors are here for you when you’re sick—and
 15 when you’re feeling well and want to stay that way.”⁴ On its website, NH maintains an online
 16 Patient Portal⁵ and represents on its website that, “Neighborhood’s Patient Portal is a secure and
 17 personal way to manage your health care online. Through the Patient Portal, you can review
 18 doctor’s notes, get your lab results, update your personal information, request refills for your
 19 prescriptions, send and receive messages from your Care Team, and schedule an appointment. The
 20 Patient Portal is available online, as well as on Apple and Android devices through the dedicated
 21 Patient Portal companion app. Sign up today or call 1-833-867-4642 for more information.”⁶ At all
 22 times relevant to this action, including the period from October 22, 2020 to December 3, 2020,
 23 Plaintiff and the Class were patients of, received medical treatment and diagnosis from, and
 24 provided their personal information, including her name, address, date of birth, social security

25 _____
 26 ² (<https://hcpsocal.org/members/>)

27 ³ (<https://www.nhcare.org/services/>)

28 ⁴ (<https://www.nhcare.org/services/>)

⁵ **(Error! Main Document**

Only https://mycw32.eclinicalweb.com/portal3449/jsp/100mp/login_otp.jsp).

⁶ (<https://www.nhcare.org/programs-resources/>)

1 number, phone number and email address to NH. As a result, at all times relevant to this action,
2 including the period from October 22, 2020 to December 3, 2020, NH possessed Plaintiff's and the
3 SubClass' medical information, in electronic and physical form, in possession of or derived
4 from Defendant regarding their medical history, mental or physical condition, or treatment. Such
5 medical information included or contained an element of personal identifying information sufficient
6 to allow identification of Plaintiff and the SubClass, such as their names, date of birth, addresses,
7 medical record numbers, insurance provider, electronic mail addresses, telephone numbers, or social
8 security numbers, or other information that, alone or in combination with other publicly available
9 information, reveals their identity. At all times relevant to this action, including the period from
10 October 22, 2020 to December 3, 2020, NH maintained and continues to maintain "medical
11 information," within the meaning of Civil Code § 56.05(j), of Plaintiff and the SubClass, each of
12 which are "patients" within the meaning of Civil Code § 56.05(k). At all times relevant to this
13 action, including the period from October 22, 2020 to December 3, 2020, NH was and is a "provider
14 of health care" within the meaning of Civil Code § 56.05(m). At all times relevant to this action,
15 including the period from October 22, 2020 to December 3, 2020, Plaintiff and SubClass members
16 were patients, within the meaning of Civil Code § 56.05(k).

17 19. Plaintiff alleges on information and belief that at all times relevant to this action,
18 including the period from October 22, 2020 to December 3, 2020, NH and HCP disclosed and/or
19 released Plaintiff's, the Class' and the SubClass' medical information, in electronic and physical
20 form, in possession of or derived from NH and/or other providers of health care, regarding their
21 medical history, mental or physical condition, or treatment, to NETGAIN, pursuant to their business
22 associate agreement and/or a service provider agreement. As a result, at all times relevant to this
23 action, including the period from October 22, 2020 to December 3, 2020, NETGAIN possessed
24 Plaintiff's, the SubClass' and the Class' medical information, in electronic and physical form, in
25 possession of or derived from Defendant regarding their medical history, mental or physical
26 condition, or treatment. Such medical information included or contained an element of personal
27 identifying information sufficient to allow identification of Plaintiff, the SubClass and the Class,
28 such as their names, date of birth, addresses, medical record numbers, insurance provider, electronic

1 mail addresses, telephone numbers, or social security numbers, or other information that, alone or in
2 combination with other publicly available information, reveals their identity. At all times relevant
3 to this action, including the period from October 22, 2020 to December 3, 2020, NETGAIN
4 maintained and continues to maintain “medical information,” within the meaning of Civil Code §
5 56.05(j), of Plaintiff and the Class, each of which are “patients” within the meaning of Civil Code §
6 56.05(k).

7 20. At all times relevant to this action, including the period from October 22, 2020 to
8 December 3, 2020, pursuant to Civil Code § 56.06(a), HCP qualifies as a provider of health care
9 because it created, maintained, preserved, and stored records of the care, products and services that
10 Plaintiff and the Class members received in the State of California from HCP’s over 16 member
11 community health centers, 160 member practice sites, 917,000 patients served, and/or other
12 providers of health care, health care service plans, pharmaceutical companies, and contractors, as
13 defined by the Act, is and was organized for the purpose of maintaining medical information, within
14 the meaning of Civil Code § 56.05(j), in order to make the information available to Plaintiff and the
15 Class members or to a provider of health care at the request of Plaintiff and the Class members or a
16 provider of health care, for purposes of allowing Plaintiff and the Class members to manage their
17 information, or for the diagnosis and treatment of Plaintiff and the Class members.

18 21. Alternatively, at all times relevant to this action, including the period from October
19 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.06(b), HCP qualifies as a provider of
20 health care because it offers software and hardware to consumers (including NH) (1) in order to
21 make the information available to an individual or a provider of health care at the request of the
22 individual or a provider of health care, (2) for purposes of allowing the individual to manage his or
23 her information, and (3) for the diagnosis, treatment, or management of a medical condition of the
24 individual.

25 22. Alternatively, at all times relevant to this action, including the period from October
26 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), HCP, as an entity that is a
27 medical group, independent practice association, pharmaceutical benefits manager, or a medical
28

1 service organization, and is not a health care service plan or provider of health care to Plaintiff and
2 the Class members, is and was a “contractor” under Civil Code § 56.05(d).

3 23. Alternatively, at all times relevant to this action, including the period from October
4 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, HCP is and was a recipient of
5 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
6 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
7 further disclosing that medical information except in accordance with a new authorization that
8 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
9 of this chapter or by law.

10 24. Alternatively, at all times relevant to this action, including the period from October
11 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, HCP is and was a recipient of
12 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
13 the Act, and was prohibited from further disclosing such medical information unless in accordance
14 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
15 permitted by other provisions of this chapter or by law.

16 25. Additionally, at all times relevant to this action, including prior to the period from
17 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), HCP is and was an entity
18 engaged in the business of furnishing administrative services to programs that provide payment for
19 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
20 or permitting its employees or agents to use or disclose Plaintiff’s and the Class members’ medical
21 information possessed in connection with performing administrative functions for a program, except
22 as reasonably necessary in connection with the administration or maintenance of the program, or as
23 required by law, or with an authorization.

24 26. As a provider of health care, a contractor, and/or other authorized recipient of
25 personal and confidential medical information, HCP is required by the Act to ensure that medical
26 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
27 patients’ authorization, and to protect and preserve the confidentiality of the medical information
28 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

1 27. Alternatively, at all times relevant to this action, including the period from October
2 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.06(a), NH qualifies as a provider of
3 health care because it created, maintained, preserved, and stored records of the care, products and
4 services that Plaintiff and the Class members received in the State of California from NH and/or
5 other providers of health care, health care service plans, pharmaceutical companies, and contractors,
6 as defined by the Act, is and was organized for the purpose of maintaining medical information,
7 within the meaning of Civil Code § 56.05(j), in order to make the information available to Plaintiff
8 and the Class members or to a provider of health care at the request of Plaintiff and the Class
9 members or a provider of health care, for purposes of allowing Plaintiff and the Class members to
10 manage their information, or for the diagnosis and treatment of Plaintiff and the Class members.

11 28. Alternatively, at all times relevant to this action, including the period from October
12 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.06(b), NH qualifies as a provider of
13 health care because it offers software (an app) to consumers (1) in order to make the information
14 available to an individual or a provider of health care at the request of the individual or a provider of
15 health care, (2) for purposes of allowing the individual to manage his or her information, and (3) for
16 the diagnosis, treatment, or management of a medical condition of the individual.

17 29. Alternatively, at all times relevant to this action, including the period from October
18 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), NH, as an entity that is a medical
19 group, independent practice association, pharmaceutical benefits manager, or a medical service
20 organization, and is not a health care service plan or provider of health care to Plaintiff and the
21 Class members, is and was a “contractor” under Civil Code § 56.05(d).

22 30. Alternatively, at all times relevant to this action, including the period from October
23 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NH is and was a recipient of
24 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
25 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
26 further disclosing that medical information except in accordance with a new authorization that
27 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
28 of this chapter or by law.

1 31. Alternatively, at all times relevant to this action, including the period from October
2 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NH is and was a recipient of
3 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
4 the Act, and was prohibited from further disclosing such medical information unless in accordance
5 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
6 permitted by other provisions of this chapter or by law.

7 32. Additionally, at all times relevant to this action, including prior to the period from
8 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), NH is and was an entity
9 engaged in the business of furnishing administrative services to programs that provide payment for
10 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
11 or permitting its employees or agents to use or disclose Plaintiff's and the Class members' medical
12 information possessed in connection with performing administrative functions for a program, except
13 as reasonably necessary in connection with the administration or maintenance of the program, or as
14 required by law, or with an authorization.

15 33. As a provider of health care, a contractor, and/or other authorized recipient of
16 personal and confidential medical information, NH is required by the Act to ensure that medical
17 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
18 patients' authorization, and to protect and preserve the confidentiality of the medical information
19 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

20 34. At all times relevant to this action, including the period from October 22, 2020 to
21 December 3, 2020, pursuant to Civil Code § 56.06(a), NETGAIN qualifies as a provider of health
22 care because it created, maintained, preserved, and stored records of the care, products and services
23 that Plaintiff and the Class members received in the State of California from NH and/or other
24 providers of health care, health care service plans, pharmaceutical companies, and contractors, as
25 defined by the Act, is and was organized for the purpose of maintaining medical information, within
26 the meaning of Civil Code § 56.05(j), in order to make the information available to Plaintiff and the
27 Class members or to a provider of health care at the request of Plaintiff and the Class members or a
28

1 provider of health care, for purposes of allowing Plaintiff and the Class members to manage their
2 information, or for the diagnosis and treatment of Plaintiff and the Class members.

3 35. Alternatively, at all times relevant to this action, including the period from October
4 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.06(b), NETGAIN qualifies as a provider
5 of health care because it offers software and hardware to consumers (NH and HCP included) (1) in
6 order to make the information available to an individual or a provider of health care at the request of
7 the individual or a provider of health care, (2) for purposes of allowing the individual to manage his
8 or her information, and (3) for the diagnosis, treatment, or management of a medical condition of
9 the individual.

10 36. Alternatively, at all times relevant to this action, including the period from October
11 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NETGAIN is and was a recipient of
12 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
13 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
14 further disclosing that medical information except in accordance with a new authorization that
15 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
16 of this chapter or by law.

17 37. Alternatively, at all times relevant to this action, including the period from October
18 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NETGAIN is and was a recipient
19 of medical information of Plaintiff and the Class members pursuant to an authorization as provided
20 by the Act, and was prohibited from further disclosing such medical information unless in
21 accordance with a new authorization that meets the requirements of Section 56.21, or as specifically
22 required or permitted by other provisions of this chapter or by law.

23 38. As a provider of health care and/or other authorized recipient of personal and
24 confidential medical information, NETGAIN is required by the Act to ensure that medical
25 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
26 patients' authorization, and to protect and preserve the confidentiality of the medical information
27 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

28

1 39. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, HCP created, maintained, preserved, and stored records of the care, services and
3 products, including the names, addresses, dates of birth, diagnosis/treatment information and
4 treatment cost information of Plaintiff and the Class (all of which constitutes medical information,
5 as that term is defined and set forth in the Act), that Plaintiff and other Class members received in
6 the State of California from NH and other HCP providers of health care on its computer server.

7 40. At all times relevant to this action, including the period from October 22, 2020 to
8 December 3, 2020, NH created, maintained, preserved, and stored records of the care, services and
9 products, including the names, addresses, dates of birth, diagnosis/treatment information and
10 treatment cost information of Plaintiff and the SubClass (all of which constitutes medical
11 information, as that term is defined and set forth in the Act), that Plaintiff and other SubClass
12 members received in the State of California from NH on its computer network.

13 41. As a result, on or before October 30, 2020, Defendants possessed Plaintiff's,
14 SubClass' and the Class' medical information, in electronic and physical form, in possession of or
15 derived from Defendants regarding their medical history, mental or physical condition, or treatment.
16 Such medical information included or contained an element of personal identifying information
17 sufficient to allow identification of Plaintiff, the SubClass and the Class, such as their names,
18 addresses, dates of birth, social security numbers, phone numbers and/or email addresses, or other
19 information that, alone or in combination with other publicly available information, reveals their
20 identity.

21 42. As providers of health care, contractors, and/or other recipients of medical
22 information, Defendants are required by the Act to ensure that medical information regarding a
23 patient is not disclosed or disseminated or released without their patients' authorization, and to
24 protect and preserve the confidentiality of the medical information regarding a patient, under Civil
25 Code §§ 56.10, 56.26, 56.36, and 56.101.

26 43. As providers of health care, contractors, and/or other recipients of medical
27 information, Defendants are required by the Act not to disclose medical information regarding a
28 patient without first obtaining an authorization under Civil Code §§ 56.10 and 56.26.

1 44. As providers of health care, contractors, and/or other recipients of medical
2 information, Defendants are required by the Act to create, maintain, preserve, and store medical
3 information in a manner that preserves the confidentiality of the information contained therein
4 under Civil Code § 56.101(a).

5 45. As providers of health care, contractors, and/or other recipients of medical
6 information, Defendants are required by the Act to protect and preserve confidentiality of electronic
7 medical information of Plaintiff and the Class in its possession under Civil Code § 56.101(b)(1)(A).

8 46. As providers of health care, contractors, and/or other recipients of medical
9 information, Defendants are required by the Act to take appropriate preventive actions to protect the
10 confidential information or records against release consistent with Defendants' obligations under
11 the Act, under Civil Code § 56.36(e)(2)(E), or other applicable state law, and the Health Insurance
12 Portability and Accountability Act of 1996 (Public Law 104-191) (HIPAA) and all HIPAA
13 Administrative Simplification Regulations in effect on January 1, 2012, contained in Parts 160, 162,
14 and 164 of Title 45 of the Code of Federal Regulations, and Part 2 of Title 42 of the Code of
15 Federal Regulations, including, but not limited to, all of the following:

- 16 i. Developing and implementing security policies and procedures.
17 ii. Designating a security official who is responsible for developing and implementing
18 its security policies and procedures, including educating and training the workforce.
19 iii. Encrypting the information or records, and protecting against the release or use of
20 the encryption key and passwords, or transmitting the information or records in a
21 manner designed to provide equal or greater protections against improper
22 disclosures.

23 47. At all times relevant to this action, including the period from October 22, 2020 to
24 December 3, 2020, HCP created, maintained, preserved, and stored Plaintiff's and the Class
25 members' medical information in an un-encrypted format.

26 48. At all times relevant to this action, including the period from October 22, 2020 to
27 December 3, 2020, NH created, maintained, preserved, and stored Plaintiff's and the SubClass
28 members' medical information in an un-encrypted format.

1 49. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, NH disclosed and/or delivered Plaintiff's and the SubClass members' medical
3 information to HCP and NETGAIN. At all times relevant to this action, NH did not obtain written
4 authorization from the Plaintiff and the SubClass prior to disclosing and/or delivering Plaintiff's and
5 the SubClass members' medical information to HCP and NETGAIN. Furthermore, NH's disclosure
6 of and/or delivery of Plaintiff's and the SubClass members' medical information to HCP and
7 NETGAIN was not permissible without written authorization from the Plaintiff and the SubClass or
8 under any exemption under Civil Code § 56.10(c).

9 50. At all times relevant to this action, including the period from October 22, 2020 to
10 December 3, 2020, HCP created, maintained, preserved, stored, disclosed and/or delivered
11 Plaintiff's and the Class members' medical information to NETGAIN on its computer servers. At
12 all times relevant to this action, HCP did not obtain written authorization from the Plaintiff and the
13 Class prior to creating, maintaining, preserving, storing, disclosing and/or delivering Plaintiff's and
14 the Class members' medical information to NETGAIN on its computer servers. Furthermore,
15 NETGAIN's disclosure of and/or delivery of Plaintiff's and the Class members' medical
16 information to NETGAIN on its computer servers was not permissible without written authorization
17 from the Plaintiff and the Class or under any exemption under Civil Code § 56.10(c).

18 51. By law, the HIPAA Privacy Rule applies only to covered entities, e.g. health care
19 providers. However, most health care providers do not carry out all of their health care activities
20 and functions by themselves. Instead, they often use the services of a variety of other persons or
21 businesses. The Privacy Rule allows covered providers to disclose protected health information
22 (PHI) to these "business associates" if the providers obtain assurances that the business associates
23 will use the information only for the purposes for which it was engaged by the covered entity, will
24 safeguard the information from misuse, and will help the covered entity comply with some of the
25 covered entity's duties under the Privacy Rule. Covered entities may disclose PHI to an entity in its
26 role as a business associate only to help the covered entity carry out its health care functions – not
27 for the business associate's independent use or purposes, except as needed for the proper
28 management and administration of the business associate. The Privacy Rule requires that a covered

1 entity obtain assurances from its business associate that the business associate will appropriately
2 safeguard the PHI it receives or creates on behalf of the covered entity. The satisfactory assurances
3 must be in writing, whether in the form of a contract or other agreement between the covered entity
4 and the business associate, and requires a covered entity to obtain satisfactory assurances, on an
5 ongoing basis, that the business associate is complying, on an ongoing basis, with cybersecurity and
6 information security standards, and appropriately safeguarding the PHI it receives or creates on
7 behalf of the covered entity.

8 52. When hiring and monitoring a service provider or business associate such as
9 NETGAIN, HCP and NH knew or should have known that they had a duty to inquire about
10 potential service providers' and business associates' cybersecurity programs and how such
11 programs are maintained. HCP and NH knew or should have known that they had a duty to
12 compare potential service providers' and business associates' cybersecurity programs to the
13 industry standards adopted by other healthcare providers, and should evaluate potential service
14 providers' track records in the industry by reviewing public information about data security
15 incidents and litigation. HCP and NH knew or should have known that they had a duty to also ask
16 potential service providers and business associates about whether they have experienced any
17 cybersecurity incidents and how such incidents were handled, as well as whether the potential
18 service provider has an insurance policy in place that would cover losses caused by cybersecurity
19 breaches (including losses caused by internal and external threats). HCP and NH knew or should
20 have known that they had a duty to review service provider and business associate contracts to
21 ensure that the contracts require the service providers to comply, on an ongoing basis, with
22 cybersecurity and information security standards (and avoid contract provisions that limit service
23 providers' responsibility for cybersecurity and information technology breaches). HCP and NH
24 knew or should have known that they had a duty to obtain satisfactory assurances that their service
25 providers and business associates were complying, on an ongoing basis, with cybersecurity and
26 information security standards, and were properly creating, maintaining, preserving, and/or storing
27 the PHI it receives or creates on behalf of HCP and NH, including the confidential, medical and
28 personal identifying information of Plaintiff and the Class. Finally, HCP and NH knew or should

1 have known that they had a duty to pay particular attention to contract terms relating to
2 confidentiality, the use and sharing of information, notice by the vendor of cybersecurity risk
3 assessments and audit reports, cybersecurity breaches and records retention and destruction.

4 53. Plaintiff alleges on information and belief that HCP's and NH's disclosure and/or
5 release of Plaintiff's, the Class' and the SubClass' medical information to NETGAIN was pursuant
6 to their business associate agreement and/or a service provider agreement that was not permissible
7 under the Privacy Rule or any exemption under Civil Code § 56.10(c), and/or because HCP and NH
8 negligently entered into an agreement with NETGAIN that contained provisions that purport or seek
9 to limit NETGAIN's financial responsibility for cybersecurity and information technology breaches,
10 and negligently failed to obtain reasonable assurances and negligently failed to monitor and conduct
11 assessments of NETGAIN to verify that NETGAIN was properly creating, maintaining, preserving,
12 and/or storing the PHI it receives or creates on behalf of HCP and NH, including the confidential,
13 medical and personal identifying information of Plaintiff and the Class, NETGAIN would comply
14 with HIPAA privacy regulations and to follow guidelines and policies to maintain the privacy,
15 confidentiality, including by encryption, and otherwise reasonably protect Plaintiff's and the Class'
16 medical information from disclosure and/or release to at least one unauthorized third party "user"
17 prior to and after HCP's and NH's disclosure and/or release of Plaintiff's and the Class members'
18 medical information to NETGAIN.

19 54. At all times relevant to this action, including the period from October 22, 2020 to
20 December 3, 2020, at least one "unauthorized third party gained access to Netgain's digital
21 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
22 obtained certain files" containing including Plaintiff's, the SubClass' and the Class' medical
23 information (i.e., their names, addresses, dates of birth, diagnosis/treatment information and
24 treatment cost information) that was located on a NETGAIN server in an un-encrypted format, as
25 represented in HCP's "Notice of Data Breach" form letter submitted to the Attorney General of the
26 State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**.

27 55. Defendants had the resources necessary to protect and preserve confidentiality of
28 electronic medical information of Plaintiff, the SubClass and the Class in their possession, but

1 neglected to adequately implement data security measures as required by HIPPA and the Act,
2 despite their obligation to do so.

3 56. Additionally, the risk of vulnerabilities in its computer and data systems of being
4 exploited by an unauthorized third party trying to steal Plaintiff's, the SubClass' and the Class'
5 electronic personally identifying and medical information was foreseeable and/or known to
6 Defendants. The California Data Breach Report 2012-2015, issued in February 2016 by Attorney
7 General, Kamala D. Harris, reported, "Malware and hacking presents the greatest threat, both in the
8 number of breaches and the number of records breached" and "Social Security numbers and
9 medical information – was breached than other data types." Moreover, as Attorney General further
10 reported, just because "[e]xternal adversaries cause most data breaches, [] this does not mean that
11 organizations are solely victims; they are also stewards of the data they collect and maintain. People
12 entrust businesses and other organizations with their data on the understanding that the
13 organizations have a both an ethical and a legal obligation to protect it from unauthorized access.
14 Neglecting to secure systems and data opens a gateway for attackers, who take advantage of
15 uncontrolled vulnerabilities." Regarding encryption, Attorney General instructed in California Data
16 Breach Report 2012-2015, "As we have said in the past, breaches of this type are preventable.
17 Affordable solutions are widely available: strong full-disk encryption on portable devices and
18 desktop computers when not in use.[] Even small businesses that lack full time information security
19 and IT staff can do this. They owe it to their patients, customers, and employees to do it now."

20 57. More recently the HIPAA Journal posted on November 1, 2018 warned, "Healthcare
21 organization[s] need to ensure that their systems are well protected against cyberattacks, which
22 means investing in technologies to secure the network perimeter, detect intrusions, and block
23 malware and phishing threats."

24 58. Further, it also was foreseeable and/or known to Defendants that negligently
25 creating, maintaining, preserving, and/or storing Plaintiff's, the SubClass' and the Class' medical
26 and personal identifying information, in electronic form, onto Defendants' computer networks in a
27 manner that did not preserve the confidentiality of the information could have a devastating effect
28 on them. As reported in the California Data Breach Report 2012-2015, "There are real costs to

1 individuals. Victims of a data breach are more likely to experience fraud than the general public,
2 according to Javelin Strategy & Research. In 2014, 67 percent of breach victims in the U.S. were
3 also victims of fraud, compared to just 25 percent of all consumers.”

4 59. To be successful, phishing relies on a series of affirmative acts by a company and its
5 employees such as clicking a link, downloading a file, or providing sensitive information. Once
6 criminals gained access to the email accounts of a company and its employees, the email servers
7 communicated—that is, disclosed—the contents of those accounts to the criminals. “Phishing
8 scams are one of the most common ways hackers gain access to sensitive or confidential
9 information. Phishing involves sending fraudulent emails that appear to be from a reputable
10 company, with the goal of deceiving recipients into either clicking on a malicious link or
11 downloading an infected attachment, usually to steal financial or confidential information.”
12 (<https://www.varonis.com/blog/data-breach-statistics/>). As posted on April 21, 2020, the FBI had
13 issued a fresh warning [Alert Number MI-000122-MW] following an increase in COVID-19
14 phishing scams targeting healthcare providers.

15 60. At all times relevant to this action, including the period from October 22, 2020 to
16 December 3, 2020, Defendants negligently created, maintained, preserved, and/or stored Plaintiff’s,
17 the SubClass’ and the Class’ medical information, including Plaintiff’s, the SubClass’ and the
18 Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
19 information, in electronic form, onto Defendants’ computer networks in a manner that did not
20 preserve the confidentiality of the information, and negligently failed to protect and preserve
21 confidentiality of electronic medical information of Plaintiff, the SubClass and the Class in their
22 possession, as required by HIPPA and the Act, and specifically, under Civil Code §§ 56.10(a),
23 56.26(a), 56.36(e)(2)(E), 56.101(a), and 56.101(b)(1)(A), and according to their written
24 representations to Plaintiff and the Class.

25 61. Had Defendants taken such appropriate preventive actions, fix the deficiencies in
26 their data security systems and adopted security measures as required by HIPPA and the Act from
27 October 22, 2020 to December 3, 2020, Defendants could have prevented Plaintiff’s and the Class’
28

1 electronic medical information within Defendants' computer networks from being accessed and
2 actually viewed by unauthorized third parties.

3 62. At all times relevant to this action, including the period of from October 22, 2020 to
4 December 3, 2020, NH, by disclosing and/or delivering Plaintiff's and the SubClass' personal
5 identifying and medical information to HCP, allowed Plaintiff's and the SubClass' personal
6 identifying and medical information to be accessed and actually viewed by at least one unauthorized
7 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
8 Code § 56.10(a).

9 63. At all times relevant to this action, including the period of from October 22, 2020 to
10 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic
11 medical information of Plaintiff and the SubClass on NETGAIN's computer server, allowed
12 Plaintiff's and the SubClass' medical and personal identifying information to be accessed and
13 actually viewed by at least one unauthorized third party, without first obtaining an authorization,
14 constituting a disclosure in violation of Civil Code § 56.10(a).

15 64. At all times relevant to this action, including the period from October 22, 2020 to
16 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
17 medical information of Plaintiff and the Class on NETGAIN's computer server, allowed Plaintiff's
18 and the Class' medical and personal identifying information to be accessed and actually viewed by
19 at least one unauthorized third party, without first obtaining an authorization, constituting a
20 disclosure in violation of Civil Code § 56.10(a).

21 65. At all times relevant to this action, including the period from October 22, 2020 to
22 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
23 medical information of Plaintiff and the Class on NETGAIN's computer server, allowed Plaintiff's
24 and the Class' medical and personal identifying information to be accessed and actually viewed by
25 at least one unauthorized third party, without first obtaining an authorization, constituting a
26 disclosure in violation of Civil Code § 56.26(a).

27 66. At all times relevant to this action, including the period from October 22, 2020 to
28 December 3, 2020, NH, by disclosing and/or delivering Plaintiff's and the SubClass members'

1 medical and personal identifying information to HCP, allowed Plaintiff's and the SubClass' medical
2 and personal identifying information to be accessed and actually viewed by at least one
3 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

4 67. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic
6 medical information of Plaintiff and the SubClass on NETGAIN's computer server, allowed
7 Plaintiff's and the SubClass' medical and personal identifying information to be accessed and
8 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
9 Code § 56.101(a).

10 68. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
12 medical information of Plaintiff and the Class on NETGAIN's computer server, allowed Plaintiff's
13 and the Class' medical and personal identifying information to be accessed and actually viewed by
14 at least one unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

15 69. At all times relevant to this action, including the period from October 22, 2020 to
16 December 3, 2020, NH, by disclosing and/or delivering Plaintiff's and the SubClass members'
17 medical and personal identifying information to HCP, allowed Plaintiff's and the SubClass' medical
18 and personal identifying information to be accessed and actually viewed by at least one
19 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

20 70. At all times relevant to this action, including the period from October 22, 2020 to
21 December 3, 2020, NH's negligent failure to protect and preserve confidentiality of electronic
22 medical information of Plaintiff and the SubClass, on NETGAIN's computer server, allowed
23 Plaintiff's and the SubClass' medical and personal identifying information to be accessed and
24 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
25 Code § 56.101(b)(1)(A).

26 71. At all times relevant to this action, including the period from October 22, 2020 to
27 December 3, 2020, HCP's negligent failure to protect and preserve confidentiality of electronic
28 medical information of Plaintiff and the Class, on NETGAIN's computer server, allowed Plaintiff's

1 and the Class' medical and personal identifying information to be accessed and actually viewed by
2 at least one unauthorized third party, constituting a release in violation of Civil Code §
3 56.101(b)(1)(A).

4 72. On or about April 12, 2021, HCP caused a form letter, entitled "**Notice of Data**
5 **Breach**," dated April 12, 2021, signed by Henry Tuttle, President & Chief Executive Officer,
6 Health Center Partners of Southern California, to be mailed to Plaintiff and the Class, informing
7 them, in part, of "a recent data security incident experienced by Netgain Technology, LLC
8 ('Netgain'), the IT service provider for Health Center Partners of Southern California ('HCP')" and
9 stating, in part, "HCP supports community health centers in a variety of ways, including
10 collaborative grant-funded programs and services for Neighborhood Healthcare.... **What**
11 **Happened:** Netgain recently informed HCP that it had experienced a data security incident that
12 involved systems containing HCP data.... According to Netgain, in late September 2020, an
13 unauthorized third party gained access to Netgain's digital environment, and between October 22,
14 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data.
15 Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the
16 attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the
17 data.... The information involved varies depending on the individual but may include the following:
18 name, address, date of birth, diagnosis/treatment information and treatment cost information. Once
19 we learned that HCP data may have been involved in the incident, we worked with our
20 cybersecurity experts to review the impacted files and identify the individuals whose information
21 was contained in such files so that we may notify such individuals. Our investigation revealed that
22 the impacted files contained your personal information." An exemplar of HCP's "**Notice of Data**
23 **Breach**" form letter submitted to the Attorney General of the State of California and mailed to
24 Plaintiff and the Class is attached hereto as **Exhibit A**. Plaintiff received in the mail a HCP "**Notice**
25 **of Data Breach**" form letter, addressed to her, which alerted Plaintiff that her medical and personal
26 identifying information, along with other Class members, was improperly accessed by at least one
27 unauthorized third party. As a result, Plaintiff fears that disclosure and/or release of her medical
28 and personal identifying information created, maintained, preserved, and/or stored on Defendants'

1 computer networks could subject her to harassment or abuse. Moreover, although thereafter, on
2 May 4, 2021, Plaintiff wrote both HCP and NH separately requesting further information about this
3 security incident, neither HCP nor NH provided a substantive response to her requests.

4 73. HCP's "**Notice of Data Breach**" form letter submitted to the Attorney General of
5 the State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**, further
6 states, "**What We Are Doing:** [] We are providing you with steps that you can take to help protect
7 your personal information, and as an added precaution, we are offering you complimentary identity
8 protection services through IDX, a leader in risk mitigation and response."

9 74. HCP's "**Notice of Data Breach**" form letter concludes by making the following
10 hollow gesture, "The security of your information is a top priority for HCP, and we are committed
11 to safeguarding your data and privacy." Other than offering "steps that you can take to help protect
12 your personal information" and "complimentary identity protection services through IDX" "as an
13 added precaution," HCP's "**Notice of Data Breach**" form letter does nothing to further protect
14 Plaintiff and the Class from future incidents of identity theft despite the severity of the unauthorized
15 access, viewing, exfiltration, theft, disclosure and/or release of their electronic medical and personal
16 information caused by Defendants' violations of their duty to implement and maintain reasonable
17 security procedures and practices.

18 75. To date, other than offering "steps that you can take to help protect your personal
19 information" and "complimentary identity protection services through IDX" "as an added
20 precaution," HCP has not offered any monetary compensation for the unauthorized disclosure
21 and/or release of Plaintiff's and the Class' electronic medical information under the Act. In effect,
22 HCP is shirking its responsibility for the harm it has caused, while shifting the burdens and costs of
23 its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

24 76. To date, NH has not offered any compensation for the unauthorized disclosure and/or
25 release of Plaintiff's and SubClass' electronic medical information under the Act. In effect, NH is
26 shirking its responsibility for the harm it has caused, while shifting the burdens and costs of its
27 wrongful conduct onto its patients, i.e. Plaintiff and the SubClass.

28

1 77. To date, NETGAIN has not offered any monetary compensation for the unauthorized
2 disclosure and/or release of Plaintiff’s and the Class’ electronic medical information under the Act.
3 In effect, NETGAIN is shirking its responsibility for the harm it has caused, while shifting the
4 burdens and costs of its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

5 78. Based upon the information posted on the U.S. Department of Health and Human
6 Services’ official website, HCP reported on “04/09/2021” a “Hacking/IT Incident” involving
7 “Network Server” affecting “293,516” persons, which involved a “Business Associate,” to the U.S.
8 Department of Health & Human Services’ Office for Civil Rights.

9 79. Based upon the information posted on the U.S. Department of Health and Human
10 Services’ official website, NH reported on “04/14/2021” a “Hacking/IT Incident” involving
11 “Network Server” affecting “45,200” persons, which involved a “Business Associate,” to the U.S.
12 Department of Health & Human Services’ Office for Civil Rights.

13 80. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA
14 covered entities to provide notification following a breach of unsecured protected health
15 information. Following a breach of unsecured protected health information, covered entities must
16 provide notification of the breach to affected individuals. Covered entities must *only* provide the
17 required notifications if the breach involved unsecured protected health information. Unsecured
18 protected health information is protected health information (PHI) that has not been rendered
19 unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or
20 methodology specified by the Secretary of the U.S. Department of Health and Human Services in
21 guidance. Under approved guidance of the U.S. Department of Health and Human Services, PHI is
22 rendered unusable, unreadable, or indecipherable to unauthorized individuals if (1) electronic PHI
23 has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process
24 to transform data into a form in which there is a low probability of assigning meaning without use
25 of a confidential process or key” (45 CFR 164.304 definition of encryption) and (2) such
26 confidential process or key that might enable decryption has not been breached. By reporting this
27 incident to the U.S. Department of Health and Human Services, HCP and NH each has separately
28 determined and is affirming that Plaintiff’s, the Class’ and the SubClass’ electronic PHI was either

1 not encrypted at all, or if it was encrypted, the encryption has been breached by the unauthorized
2 third party. Further, because Plaintiff's, the Class' and the SubClass' identifiable medical
3 information contained in NETGAIN's computer server was not rendered unusable, unreadable, or
4 indecipherable, the unauthorized third party or parties who "obtained" and downloaded Plaintiff's
5 and the Class' identifiable medical information was able to and did actually view Plaintiff's, the
6 Class' and the SubClass' electronic medical information contained in and "obtained" and
7 downloaded from NETGAIN's computer server. As a result, HCP and NH each has separately
8 determined and have affirmed that Plaintiff's, the Class' and the SubClass' identifiable medical
9 information contained in NETGAIN's computer server was unencrypted and thus, the unauthorized
10 third party or parties who "obtained" and downloaded Plaintiff's, the Class' and the SubClass'
11 identifiable medical information was able to and did actually view Plaintiff's, the Class' and the
12 SubClass' electronic medical information contained in and "obtained" and downloaded from
13 NETGAIN's computer server. Therefore, HCP, NH and NETGAIN was negligent for failing to
14 encrypt or adequately encrypt Plaintiff's, the Class' and the SubClass' electronic medical
15 information contained in NETGAIN's computer server.

16 81. As a result, Defendants were negligent for failing to encrypt or adequately encrypt
17 Plaintiff's, the Class' and the SubClass' electronic medical information on their computer networks.
18 Further, because Plaintiff's, the Class' and the SubClass' identifiable medical information on
19 Defendants' computer networks was not rendered unusable, unreadable, or indecipherable, the
20 unauthorized third party or parties who accessed Plaintiff's, the Class' and the SubClass'
21 identifiable medical information was able to and did view Plaintiff's, the Class' and the SubClass'
22 electronic medical information contained within NETGAIN's computer server.

23 **CLASS ACTION ALLEGATIONS**

24 82. Plaintiff brings this action on behalf of herself individually and on behalf of all
25 others similarly situated. The putative class and subclass that Plaintiff seeks to represent is defined
26 as follows:

27 Class: All persons to whom Health Center Partners of Southern California sent a
28 notification letter of a data security incident that has occurred between October

1 22, 2020 to December 3, 2020, an exemplar of which is attached hereto as
2 **Exhibit A.**

3 SubClass: All persons to whom Neighborhood Healthcare sent a notification
4 letter of a data security incident that has occurred between November 24, 2020 to
December 3, 2020, an exemplar of which is attached hereto as **Exhibit B.**

5 The officers, directors, employees, and agents of Defendants and any “affiliate,” “principal” or
6 “subsidiary” of Defendants, as defined in the Corporations Code §§ 150, 175, and 189, respectively,
7 are excluded from the Class and the SubClass. Plaintiff reserves the right under California Rule of
8 Court 3.765 to amend or modify the Class definition with greater particularity or further division
9 into subclasses or limitation to particular issues as warranted, and as additional facts are discovery
10 by Plaintiff during her future investigations.

11
12 83. This action is properly maintainable as a class action. The members of the Class and
13 the SubClass are so numerous that joinder of all members is impracticable, if not completely
14 impossible. While the exact number of the Class is unknown to Plaintiff at this time, HCP filed a
15 report with the U.S. Department of Health & Human Services’ Office for Civil Rights, on or about
16 December 28, 2020, that this incident affected 293,516 persons. The disposition of the claims of
17 the members of Class through this class action will benefit both the parties and this Court. In
18 addition, the Class and the SubClass is readily identifiable from information and records in the
19 possession of Defendants and their agents, and the Class and the SubClass is defined in objective
20 terms that make the eventual identification of the Class and the SubClass members possible and/or
21 sufficient to allow members of the Class and the SubClass identify themselves as having a right to
22 recover.

23 84. There is a well-defined community of interest among the members of the Class and
24 the SubClass because common questions of law and fact predominate, Plaintiff’s claims are typical
25 of the members of the class, and Plaintiff can fairly and adequately represent the interests of the
26 Class.

27 85. Common questions of law and fact exist as to all members of the Class and the
28 SubClass and predominate over any questions affecting solely individual members of the Class and

1 the SubClass. Among the questions of law and fact common to the Class that predominate over
2 questions which may affect individual Class members, including the following:

- 3 a) Whether Defendants possessed Plaintiff's, the SubClass' and the Class' medical and
4 personal identifying information from October 22, 2020 to December 3, 2020;
- 5 b) Whether Defendants created, maintained, preserved and/or stored Plaintiff's, the
6 SubClass' and the Class' medical and personal identifying information, in electronic
7 form, onto Defendants' computer networks from October 22, 2020 to December 3,
8 2020;
- 9 c) Whether Defendants implemented and maintained reasonable security procedures
10 and practices to protect Plaintiff's, the SubClass' and the Class' medical and
11 personal identifying information, in electronic form, within Defendants' computer
12 networks from October 22, 2020 to December 3, 2020;
- 13 d) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
14 information, in electronic form, within Defendants' computer networks from October
15 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
16 exposed by an unauthorized third party;
- 17 e) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
18 information, in electronic form, within Defendants' computer networks from October
19 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
20 exposed by an unauthorized third party without the prior written authorization of
21 Plaintiff, the SubClass and the Class, as required by Civil Code §§ 56.10 and 56.26;
- 22 f) Whether Defendants' creation, maintenance, preservation and/or storage of
23 Plaintiff's, the SubClass' and the Class' medical and personal identifying
24 information, in electronic form, within Defendants' computer networks, accessed,
25 viewed, exfiltrated and/or publicly exposed by an unauthorized third party was
26 permissible without written authorization from Plaintiff, the SubClass and the Class
27 or under any exemption under Civil Code § 56.10(c);
- 28

- 1 g) Whether Defendants' creation, maintenance, preservation and/or storage of
2 Plaintiff's, the SubClass' and the Class' medical and personal identifying
3 information, in electronic form, within Defendants' computer networks, accessed,
4 viewed, exfiltrated and/or publicly exposed by an unauthorized third party
5 constitutes a release in violation of Civil Code §56.101;
- 6 h) Whether the timing of HCP's notice that Plaintiff's and the Class' medical and
7 personal identifying information, in electronic form, was accessed, viewed,
8 exfiltrated and/or publicly exposed by an unauthorized third party, was given in the
9 most expedient time possible and without reasonable delay;
- 10 i) Whether Defendants' conduct constitute unlawful, fraudulent or unfair practices in
11 violation of Business and Professions Code §§ 17200, *et seq.*; and
- 12 j) Whether Plaintiff, the SubClass and the Class are entitled to actual, nominal or
13 statutory damages, injunctive relief and/or restitution.

14 86. Plaintiff's claims are typical of those of the other SubClass and Class members
15 because Plaintiff, like every other SubClass and Class member, were exposed to virtually identical
16 conduct and now suffer from the same violations of the law as other SubClass and Class members.

17 87. Plaintiff will fairly and adequately protect the interests of the SubClass and the
18 Class. Moreover, Plaintiff has no interest that is contrary to or in conflict with those of the
19 SubClass and the Class, she seeks to represent. In addition, Plaintiff has retained competent counsel
20 experienced in class action litigation to further ensure such protection and intend to prosecute this
21 action vigorously.

22 88. The nature of this action and the nature of laws available to Plaintiff and the other
23 SubClass and Class members make the use of the class action format a particularly efficient and
24 appropriate procedure to afford relief to Plaintiff and the other SubClass and Class members for the
25 claims alleged and the disposition of whose claims in a class action will provide substantial benefits
26 to both the parties and the Court because:

- 27 a) If each of the SubClass and the Class members were required to file an individual
28 lawsuit, the Defendants would necessarily gain an unconscionable advantage since

- 1 they would be able to exploit and overwhelm the limited resources of each individual
2 member of the SubClass and Class with its vastly superior financial and legal
3 resources;
- 4 b) The costs of individual suits could unreasonably consume the amounts that would be
5 recovered;
- 6 c) Proof of a common business practice or factual pattern which Plaintiff experienced is
7 representative of that experienced by the SubClass and the Class and will establish
8 the right of each of the members to recover on the causes of action alleged;
- 9 d) Individual actions would create a risk of inconsistent results and would be
10 unnecessary and duplicative of this litigation; and
- 11 e) The disposition of the claims of the members of the SubClass and the Class through
12 this class action will produce salutary by-products, including a therapeutic effect
13 upon those who indulge in fraudulent practices, and aid to legitimate business
14 enterprises by curtailing illegitimate competition.

15 89. The prosecution of separate actions by individual members of the SubClass and the
16 Class would create a risk of inconsistent or varying adjudications with respect to individual
17 members of the SubClass and the Class, which would establish incompatible standards of conduct
18 for the Defendants in the State of California and would lead to repetitious trials of the numerous
19 common questions of fact and law in the State of California. Plaintiff knows of no difficulty that
20 will be encountered in the management of this litigation that would preclude its maintenance as a
21 class action. As a result, a class action is superior to other available methods for the fair and
22 efficient adjudication of this controversy.

23 90. Notice to the members of the SubClass and the Class may be made by e-mail or first-
24 class mail addressed to all persons who have been individually identified by Defendants and who
25 have been given notice of the data breach.

26 91. Plaintiff, the SubClass and the Class have suffered irreparable harm and damages
27 because of Defendants' wrongful conduct as alleged herein. Absent certification, Plaintiff, the
28 SubClass and the Class will continue to be damaged and to suffer by the unauthorized disclosure

1 and/or release of their medical and personal identifying information, thereby allowing these
2 violations of law to proceed without remedy.

3 92. Moreover, Plaintiff’s, the SubClass’ and the Class’ individual damages are
4 insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendants’
5 violations of law inflicting substantial damages in the aggregate would go unremedied. In addition,
6 Defendants have acted or refused to act on grounds generally applicable to Plaintiff, the SubClass
7 and the Class, thereby making appropriate final injunctive relief with respect to, the Class as a
8 whole.

9 **FIRST CAUSE OF ACTION**
10 **Violations of the Confidentiality of Medical Information Act**
11 **California Civil Code §§ 56, et seq.**
12 **(On Behalf of Plaintiff and the SubClass Against NH)**

13 93. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
14 fully stated herein.

15 94. At all times relevant to this action, including the period from October 22, 2020 to
16 December 3, 2020, NH is considered a “provider of health care,” within the meaning of Civil Code
17 §§ 56.05(m) and 56.06(a) & (b), and maintained and continues to maintain “medical information”
18 within the meaning of Civil Code § 56.05(j), of Plaintiff and the SubClass.

19 95. Plaintiff and the SubClass are “patients” of NH within the meaning of Civil Code §
20 56.05(k) and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that
21 disclosure and/or release of their medical information could subject them to harassment or abuse.

22 96. At all times relevant to this action, including the period from October 22, 2020 to
23 December 3, 2020, NH negligently created, maintained, preserved, and/or stored Plaintiff’s and the
24 SubClass’ medical information, including Plaintiff’s and the SubClass’ names, addresses, dates of
25 birth, diagnosis/treatment information and treatment cost information, in electronic form, onto
26 Defendants’ computer networks in a manner that did not preserve the confidentiality of the
27 information, and negligently failed to protect and preserve confidentiality of electronic medical
28 information of Plaintiff and the SubClass in its possession, as required by the Act, and specifically,

1 under Civil Code §§ 56.06(d), 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
2 56.36(e)(2)(E), and according to their written representations to Plaintiff and the SubClass.

3 97. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass members'
4 medical and personal identifying information to HCP without written authorization from Plaintiff
5 and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff's and
6 the SubClass' medical information, including Plaintiff's and the SubClass' names, addresses, dates
7 of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be
8 accessed and actually viewed by at least one unauthorized third party, without first obtaining an
9 authorization, constituting a disclosure in violation of Civil Code §§ 56.06(d), 56.10, 56.13, 56.245,
10 and 56.26(a).

11 98. Due to NH's negligent creation, maintenance, preservation and/or storage of
12 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server, NH
13 allowed Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass'
14 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
15 electronic form, to be accessed and actually viewed by at least one unauthorized third party, without
16 first obtaining an authorization, constituting a disclosure in violation of Civil Code §§ 56.06(d),
17 56.10, 56.13, 56.245, and 56.26(a).

18 99. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass members'
19 medical and personal identifying information to HCP without written authorization from Plaintiff
20 and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff's and
21 the SubClass' medical information, including Plaintiff's and the SubClass' names, addresses, dates
22 of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be
23 accessed and actually viewed by at least one unauthorized third party, constituting a release in
24 violation of Civil Code § 56.101(a).

25 100. Due to NH's negligent creation, maintenance, preservation and/or storage of
26 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server,
27 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
28 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in

1 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
2 constituting a release in violation of Civil Code § 56.101(a).

3 101. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass' medical
4 information and personal identifying information to HCP without written authorization from
5 Plaintiff and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed
6 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
7 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
8 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
9 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

10 102. Due to NH's negligent creation, maintenance, preservation and/or storage of
11 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server, NH
12 allowed Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass'
13 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
14 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
15 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

16 103. As a result of NH's above-described conduct in violation of the Act, Plaintiff and the
17 SubClass have suffered damages from the unauthorized disclosure and/or release of their medical
18 and personal identifying information made unlawful by Civil Code §§ 56.06(d), 56.10, 56.101.

19 104. As a result of NHs' above-described conduct in violation of the Act, Plaintiff and the
20 SubClass seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
21 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
22 Code § 56.36(b)(2).

23 **SECOND CAUSE OF ACTION**
24 **Violations of the Confidentiality of Medical Information Act**
25 **California Civil Code §§ 56, et seq.**
(On Behalf of Plaintiff and the Class Against HCP)

26 105. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
27 fully stated herein.

28

1 106. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, HCP is considered a “provider of health care” within the meaning of Civil Code
3 § 56.05(m) and 56.06(a) & (b), a “contractor” under Civil Code § 56.05(d), and/or “engaged in the
4 business of furnishing administrative services to programs that provide payment for health care
5 services” under Civil Code § 56.26(a), and maintained and continues to maintain “medical
6 information” within the meaning of Civil Code § 56.05(j), of Plaintiff and the Class.

7 107. Plaintiff and the Class are “patients” within the meaning of Civil Code § 56.05(k)
8 and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure
9 and/or release of their medical information could subject them to harassment or abuse.

10 108. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, HCP negligently created, maintained, preserved, and/or stored Plaintiff’s and the
12 Class’ medical information, including Plaintiff’s and the Class’ names, addresses, dates of birth,
13 diagnosis/treatment information and treatment cost information, in electronic form, onto
14 NETGAIN’s computer server in a manner that did not preserve the confidentiality of the
15 information, and negligently failed to protect and preserve confidentiality of electronic medical
16 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
17 under Civil Code §§ 56.06(d), 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
18 56.36(e)(2)(E).

19 109. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
20 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
21 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
22 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
23 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
24 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
25 Code §§ 56.06(d), 56.10, 56.13, 56.245, and 56.26(a).

26 110. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
27 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
28 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s

1 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
2 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
3 third party, constituting a release in violation of Civil Code § 56.101(a).

4 111. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
5 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
6 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
7 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
8 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
9 third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

10 112. As a result of HCP’s above-described conduct in violation of the Act, Plaintiff and
11 the Class have suffered damages from the unauthorized disclosure and/or release of their medical
12 and personal identifying information made unlawful by Civil Code §§ 56.06(d), 56.10, 56.101.

13 113. As a result of HCP’s above-described conduct in violation of the Act, Plaintiff and
14 the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
15 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
16 Code § 56.36(b)(2).

17 **THIRD CAUSE OF ACTION**
18 **Violations of the Confidentiality of Medical Information Act**
19 **California Civil Code §§ 56, et seq.**
20 **(On Behalf of Plaintiff and the Class Against NETGAIN)**

21 114. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
22 fully stated herein.

23 115. At all times relevant to this action, including the period from October 22, 2020 to
24 December 3, 2020, NETGAIN is considered a “provider of health care” within the meaning of Civil
25 Code §§ 56.05(m) and 56.06(a) & (b), and maintained and continues to maintain “medical
26 information” within the meaning of Civil Code § 56.05(j), of Plaintiff and the Class.

27 116. Plaintiff and the Class are “patients” within the meaning of Civil Code § 56.05(k)
28 and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure
and/or release of their medical information could subject them to harassment or abuse.

1 117. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, NETGAIN negligently created, maintained, preserved, and/or stored Plaintiff's
3 and the Class' medical information, including Plaintiff's and the Class' names, addresses, dates of
4 birth, diagnosis/treatment information and treatment cost information, in electronic form, onto
5 NETGAIN's computer server in a manner that did not preserve the confidentiality of the
6 information, and negligently failed to protect and preserve confidentiality of electronic medical
7 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
8 under Civil Code §§ 56.06(d), 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
9 56.36(e)(2)(E).

10 118. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
11 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
12 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
13 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
14 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
15 unauthorized third party, without first obtaining an authorization, constituting a disclosure in
16 violation of Civil Code §§ 56.06(d), 56.10, 56.13, 56.245, and 56.26(a).

17 119. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
18 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
19 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
20 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
21 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
22 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

23 120. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
24 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
25 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
26 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
27 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
28 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

1 125. Civil Code § 1798.82 further provides, “(h) For purposes of this section, ‘personal
2 information’ means an individual’s first name or first initial and last name in combination with any
3 one or more of the following data elements, when either the name or the data elements are not
4 encrypted: (1) Social security number. (2) Driver’s license number or California Identification Card
5 number. (3) Account number, credit or debit card number, in combination with any required
6 security code, access code, or password that would permit access to an individual’s financial
7 account. (4) Medical information. (5) Health insurance information. (i) (2) For purposes of this
8 section, ‘medical information’ means any information regarding an individual’s medical history,
9 mental or physical condition, or medical treatment or diagnosis by a health care professional. (3)
10 For purposes of this section, ‘health insurance information’ means an individual’s health insurance
11 policy number or subscriber identification number, any unique identifier used by a health insurer to
12 identify the individual, or any information in an individual’s application and claims history,
13 including any appeals records.”

14 126. HCP conducts business in California and owns or licenses computerized data which
15 includes the personal information, within the meaning of Civil Code § 1798.82(h), of Plaintiff and
16 the Class.

17 127. Based upon NH’s “**Notice of Data Breach**” form letter, HCP was aware that
18 Plaintiff’s and the Class’ unencrypted personal information on NETGAIN’s computer server was,
19 or is reasonably believed to have been, acquired by an unauthorized person no later than December
20 3, 2020, but did not begin to mail notification letters to Plaintiff and the Class until April 12, 2021.
21 Thus, HCP waited at least 131 days before *beginning* to inform Plaintiff and the Class of this
22 incident and the subsequent threat to Plaintiff’s and the Class’ personal information. As a result,
23 HCP did not disclose to Plaintiff and the Class that their personal information was, or was
24 reasonably believed to have been, acquired by an unauthorized person, in the most expedient time
25 possible and without reasonable delay in violation of Civil Code § 1798.82(a). Given the example
26 of the Legislature finding that a delay of 21 days to be “late notice” under the statute, HCP’s delay
27 of 131 days before *beginning* to inform Plaintiff and the Class that their personal information was,
28 or was reasonably believed to have been, acquired by an unauthorized person by mailing HCP’s

1 form letter to Plaintiff and the Class is presumptively unreasonable notice in violation of Civil Code
2 § 1798.82(a).

3 128. Plaintiff and the Class have been injured by fact that HCP did not disclose their
4 personal information was, or was reasonably believed to have been, acquired by an unauthorized
5 person in the most expedient time possible and without reasonable delay in violation of Civil Code
6 § 1798.82(a). HCP’s delays in informing required by Civil Code § 1798.82(a) and providing all of
7 the information required by Civil Code § 1798.82(d) to Plaintiff and the Class that their personal
8 information was, or was reasonably believed to have been, acquired by an unauthorized person,
9 have prevented Plaintiff and the Class from taking steps to protect their personal information from
10 unauthorized use and/or identify theft.

11 129. Plaintiff and the Class seek recovery of their damages pursuant to Civil Code §
12 1798.84(b) and injunctive relief pursuant to Civil Code § 1798.84(e).

13 **FIFTH CAUSE OF ACTION**
14 **Unlawful and Unfair Business Acts and Practices in Violation of**
15 **California Business & Professions Code §17200, *et seq.***
16 **(On Behalf of Plaintiff, the SubClass and the Class Against All Defendants)**

17 130. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
18 fully stated herein.

19 131. The acts, misrepresentations, omissions, practices, and non-disclosures of
20 Defendants as alleged herein constituted unlawful and unfair business acts and practices within the
21 meaning of California Business & Professions Code §§ 17200, *et seq.*

22 132. By the aforementioned business acts or practices, Defendants have engaged in
23 “unlawful” business acts and practices in violation of the aforementioned statutes, including Civil
24 Code §§ 56.06(d), 56.10(a), 56.26(a), 56.36(e)(2)(E), 56.101(a), 56.101(b)(1)(A), 1798.82(a) and
25 1798.82(d). Plaintiff reserves the right to allege other violations of law committed by Defendants
26 which constitute unlawful acts or practices within the meaning of California Business & Professions
27 Code §§ 17200, *et seq.*

28 133. By the aforementioned business acts or practices, Defendants have also engaged in
“unfair” business acts or practices in that the harm caused by Defendants’ failure to maintain

1 adequate information security procedures and practices, including but not limited to, failing to take
2 adequate and reasonable measures to ensure its data systems were protected against unauthorized
3 intrusions, failing to properly and adequately educate and train its employees, failing to put into
4 place reasonable or adequately computer systems and security practices to safeguard patients'
5 identifiable medical information including access restrictions and encryption, failing to have
6 adequate privacy policies and procedures in place that did not preserve the confidentiality of the
7 medical and personal identifying information of Plaintiff, the SubClass and the Class in their
8 possession, and failing to protect and preserve confidentiality of electronic medical information of
9 Plaintiff, the SubClass and the Class in their possession against disclosure and/or release, outweighs
10 the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous,
11 unethical, deceitful and offensive, and causes substantial injury to Plaintiff, the SubClass and the
12 Class.

13 134. Defendants have obtain money and property from Plaintiff, the SubClass and the
14 Class because of the payment of the services and products they received from Defendants. Plaintiff,
15 the SubClass and the Class have suffered an injury in fact by acquiring less in their transactions
16 with Defendants for the services and products they received from Defendants than they otherwise
17 would have if Defendants would had adequately protected the confidentiality of their medical and
18 personal identifying information.

19 135. Pursuant to the Business & Professions Code § 17203, Plaintiff, the SubClass and the
20 Class seek an order of this Court requiring Defendants awarding Plaintiff and the Class restitution
21 of monies wrongfully acquired by Defendants in the form of payments for services by means of
22 such unlawful, fraudulent and unfair business acts and practices, so as to restore any and all monies
23 to Plaintiff, the SubClass and the Class which were acquired and obtained by means of such
24 unlawful, fraudulent and unfair business acts and practices, which ill-gotten gains are still retained
25 by Defendants.

26 136. The aforementioned unlawful, fraudulent and unfair business acts or practices
27 conducted by Defendants have been committed in the past and continues to this day. Defendants
28 have failed to acknowledge the wrongful nature of their actions. Defendants have not corrected or

1 publicly issued comprehensive corrective notices to Plaintiff, the SubClass and the Class, and have
2 not corrected or enacted adequate privacy policies and procedures to protect and preserve
3 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
4 Class in their possession.

5 137. Because of Defendants' aforementioned conduct, Plaintiff, the SubClass and the
6 Class have no other adequate remedy of law in that absent injunctive relief from the Court and
7 Defendants are likely to continue to injure Plaintiff, the SubClass and the Class.

8 138. Pursuant to Business & Professions Code § 17203, Plaintiff, the SubClass and the
9 Class also seek an order of this Court for equitable and/or injunctive relief in the form of requiring
10 Defendants to correct its illegal conduct that is necessary and proper to prevent Defendants from
11 repeating their illegal and wrongful practices as alleged above and protect and preserve
12 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
13 Class in Defendants' possession that has already been accessed, viewed, exfiltrated and/or publicly
14 exposed by at least one unauthorized third party because by way of Defendants' illegal and
15 wrongful practices set forth above. Pursuant to Business & Professions Code § 17203, Plaintiff, the
16 SubClass and the Class further seek an order of this Court for equitable and/or injunctive relief in
17 the form of requiring Defendants to publicly issue comprehensive corrective notices.

18 139. Because this case is brought for the purposes of enforcing important rights affecting
19 the public interest, Plaintiff, the SubClass and the Class also seek the recovery of attorneys' fees
20 and costs in prosecuting this action against Defendants under Code of Civil Procedure § 1021.5 and
21 other applicable law.

22 **PRAYER FOR RELIEF**

23 WHEREFORE, Plaintiff respectfully request that the Court grant Plaintiff and the proposed
24 SubClass and Class the following relief against Defendants, and each of them:

25 **As for the First, Second and Third Causes of Action**

- 26 1. For nominal damages in the amount of one thousand dollar (\$1,000) per violation to Plaintiff
27 individually and to each member of the SubClass and the Class pursuant to Civil Code §
28 56.36(b)(1);

1 2. For actual damages according to proof per violation pursuant to Civil Code § 56.36(b)(2);

2 **As for the Fourth Cause of Action**

3 3. For damages according to proof to Plaintiff individually and to each member of the Class
4 pursuant to California Civil Code § Civil Code § 1798.84(b);

5 4. For injunctive relief pursuant to California Civil Code § Civil Code § 1798.84(e);

6 **As for the Fifth Cause of Action**

7 5. For an order awarding Plaintiff, the SubClass and the Class restitution of all monies
8 wrongfully acquired by Defendants by means of such unlawful, fraudulent and unfair
9 business acts and practices;

10 6. For injunctive relief in the form of an order instructing Defendants to prohibit the
11 unauthorized release of medical and personal identifying information of Plaintiff, the
12 SubClass and the Class, and to adequately maintain the confidentiality of the medical and
13 personal identifying information of Plaintiff and the Class;

14 7. For injunctive relief in the form of an order enjoining Defendants from disclosing the
15 medical and personal identifying information of Plaintiff, the SubClass and the Class
16 without the prior written authorization of each Plaintiff, the SubClass and the Class member;

17 **As to All Causes of Action**

18 8. That the Court issue an Order certifying this action be certified as a class action on behalf of
19 the proposed SubClass and Class, appointing Plaintiff as representative of the proposed
20 SubClass and Class, and appointing Plaintiff's attorneys, as counsel for members of the
21 proposed SubClass and Class;

22 9. For an award of attorneys' fees as authorized by statute, including, but not limited to, the
23 provisions of California Code of Civil Procedure § 1021.5, and as authorized under the
24 "common fund" doctrine, and as authorized by the "substantial benefit" doctrine;

25 10. For costs of the suit;

26 11. For prejudgment interest at the legal rate; and

27 12. Any such further relief as this Court deems necessary, just, and proper.
28

1 Dated: September 8, 2021

KEEGAN & BAKER LLP

2
3 By  _____

4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

Plaintiff, the SubClass and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

Dated: September 8, 2021

KEEGAN & BAKER LLP

By  _____

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

PROOF OF SERVICE

I, Stacy Johnson, declare that I am over the age of 18 years and am not a party to the case; I am employed in the County of San Diego, California; and my business address is 2292 Faraday Avenue, Suite 100, Carlsbad, California 92008. The mailing occurred in Wildomar, California.

I caused to be served the following document(s): **FIRST AMENDED CLASS ACTION COMPLAINT FOR DAMAGES, RESTITUTION, AND INJUNCTIVE RELIEF FOR VIOLATIONS OF: (1) THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CIVIL CODE §§ 56, ET SEQ.; (2) BREACH OF CALIFORNIA SECURITY NOTIFICATION LAWS, CALIFORNIA CIVIL CODE § 1798.82; AND (3) BUSINESS AND PROFESSIONS CODE §§ 17200, ET SEQ.** on the interested parties listed below:

Daniel T. Rockey, Esq.
daniel.rockey@bclplaw.com
BRYAN CAVE LLP
Three Embarcadero Center, 7th Floor
San Francisco, CA 94111
Tel: (415) 675-3400 / Fax: (415) 675-3434
Attorney for Defendant Neighborhood Healthcare

Craig J. Mariam, Esq.
cmariam@grsm.com
GORDON REES SCULLY MANSUKHANI, LLP
633 West Fifth Street, 52nd Floor
Los Angeles, CA 90071
Tel: (213) 270-7856 / Fax: (877) 306-0043
Attorney for Defendant Health Center Partners of Southern California

■ **BY ELECTRONIC SERVICE:** I transmitted the documents described above to One Legal for electronic service on Daniel T. Rockey, Esq. (Daniel.rockey@bclplaw.com); and Craig J. Mariam, Esq. (cmariam@grsm.com). In light of the COVID-19 pandemic in California and Governor Newsom’s Executive Order N-38-20, dated March 27, 2020, the requirements under Code of Civil Procedure section 1010.6 regarding agreement to electronic service have been suspended. Accordingly, all documents served in this matter will be done by electronic means consistent with other provisions of the Code of Civil Procedure.

■ (State) I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: September 8, 2021



Exhibit A



C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE



NAME

ADDRESS1

ADDRESS2

CSZ

COUNTRY



SEQ
CODE 2D
Ver 1

BREAK

To Enroll, Please Call:
1-833-416-0926
Or Visit:
<https://response.idx.us/hcp-netgain-incident>
Enrollment Code: <<XXXXXXXXXX>>

April 12, 2021

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by Netgain Technology, LLC (“Netgain”), the IT service provider for Health Center Partners of Southern California (“HCP”). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTHCENTER>>. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, we engaged our own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, our health center members and partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain’s cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

Once we learned that HCP data may have been involved in the incident, we worked with our cybersecurity experts to review the impacted files and identify the individuals whose information was contained in such files so that we may notify such individuals. Our investigation revealed that the impacted files contained your personal information. **Again, we are not aware of any misuse of your personal information as a result of this incident.** Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your information.

What Information Was Involved: The information involved varies depending on the individual but may include the following: <<VARPARAGRAPH>>.

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, we have reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and we are committed to assisting their investigation into the matter.

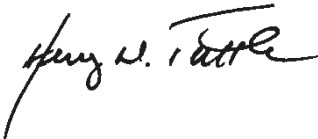
We are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include **xx** months of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What You Can Do: As we have stated, we are not aware of any misuse of your information as a result of this incident. However, we encourage you to follow the recommendations on the next page to help protect your information. We also encourage you to enroll in the complimentary services offered by going to <https://response.idx.us/hcp-netgain-incident> or calling 1-833-416-0926 and using the enrollment code provided above. Please note that the deadline to enroll is July 12, 2021.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-833-416-0926 between 6:00 a.m. and 6:00 p.m. Pacific Time.

The security of your information is a top priority for HCP, and we are committed to safeguarding your data and privacy.

Sincerely,

A handwritten signature in black ink, appearing to read "Henry W. Tuttle". The signature is written in a cursive style with a large initial "H".

Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
www.consumer.ftc.gov ,	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
and	1-888-743-0023	1-877-566-7226	1-401-274-4400
www.ftc.gov/idtheft			
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Exhibit B



To Enroll, Please Call:
(833) 903-3642
Or Visit:
<https://response.idx.us/nhc-netgain-incident>
Enrollment Code: <<ENROLLMENT>>

C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

April 8, 2021

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

The privacy and security of your personal information is very important to Neighborhood Healthcare. We are writing to make you aware of an issue brought to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud hosting and managed services provider. Neighborhood Healthcare used Netgain to host some Neighborhood Healthcare files.

What Happened

On November 24, 2020, Netgain became aware of a security incident that involved unauthorized access to portions of the Netgain environment and Netgain client environments and began taking steps to investigate this incident. But, on December 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain took additional measures to contain the threat and address the issue. Netgain’s technical teams worked closely with third-party experts to remove the threat in the impacted environments and confirm that client and internal systems are protected.

Neighborhood Healthcare learned of the ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to believe that the protected health information (“PHI”) of our patients had been impacted in the incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some information including, potentially, some files containing patient PHI may have been impacted in the incident. Netgain could not confirm, at that time, what records may have been impacted in the incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood Healthcare that Netgain believed were impacted by the attackers. Those files came from a Neighborhood Healthcare server accessible by the Netgain environment. Since that time, Neighborhood Healthcare has worked to review those records, to identify individuals impacted, conduct an investigation into the incident with the assistance outside experts, and to transmit this letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood Healthcare determined that the impacted files included some of your information.

What Information Was Involved

The information involved may have included some of the following: your name, date of birth, address, Social Security Number and information about the care that you received from Neighborhood Healthcare such as insurance coverage information, physician you saw, and treatment codes. Neighborhood Healthcare is offering credit monitoring services to you at no charge. Please see the **What You Can Do** section below for information about these services including how to enroll. Please also see the **Additional Important Information** section below for further precautionary measures you may wish to take. Netgain has received assurances that the data has not gone beyond the attacker, that the data was not and will not be misused, and that the data will not be disseminated or otherwise be made publicly available.

What We Are Doing

Please know that we take this incident and the security of your personal information very seriously. Ensuring the safety of our patients' data is of the utmost importance to us. Since we learned of this incident, we have been working with Netgain to seek assurances that they are taking appropriate steps to respond to this incident. We have also conducted an investigation of the incident with the help of outside experts, and we have transitioned to a new hosting provider (a transition that was already in process when this incident occurred).

In addition, we are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include <<12/24 months>> of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What Netgain Is Doing

Netgain took several steps to strengthen its environment following the incident, including international Geo-fencing for Azure-hosted environments, deploying additional log monitoring across all servers, and additional hardening of network security rules and protocols to restrict lateral movement across environments. Netgain stated that it paid a significant amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

What You Can Do

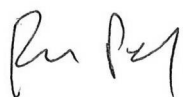
We recommend that you review the additional information enclosed. Additionally, we encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 903-3642 or going to <https://response.idx.us/nhc-netgain-incident> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 8, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

We very much regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, please call (833) 903-3642, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely



Rakesh Patel
CEO
Neighborhood Healthcare

Additional Important Information

1. Website and Enrollment. Go to <https://response.idx.us/nhc-netgain-incident> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 903-3642 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Generally. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing financial account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state's Attorney General.

5. The FTC. You can obtain information from Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

6. Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

7. Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788 equifax.com/personal/credit-report-services/ 800-525-6285	Experian Security Freeze P.O. Box 9554 Allen, TX 75013-9544 experian.com/freeze/center.html 888-397-3742	TransUnion (FVAD) P.O. Box 160 Woodlyn, PA 19094 transunion.com/credit-freeze 888-909-8872
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

More information can also be obtained by contacting the Federal Trade Commission listed above.

8. Protecting Medical Information: To date, we have no reason to believe that your PHI potentially involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following steps can help protect you from medical identity theft issues.

- Do not share health insurance cards with anyone apart from your care providers and other family members who are covered under the insurance plan or who help you with your medical care.
- Review the “explanation of benefits statements” that you receive from your health insurance company. If you see something amiss, follow up with your insurance company or the health care provider identified on the explanation of benefits to request further information.
- Ask your health insurance company for a report on all services they have paid for you for the current year. If you do not recognize an item in that list, speak with your insurance company to verify it.

9. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

Jane Doe, individually and on the behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff

(EXCEPT IN U.S. PLAINTIFF CASES)

'21CV1587 BEN RBB

(c) Attorneys (Firm Name, Address, and Telephone Number)

Patrick N. Keegan, Esq. Keegan & Baker, LLP 2292 Faraday Ave. Ste 100, Carlsbad, CA 92008

DEFENDANTS

Neighborhood Healthcare, Health Center Partners of Southern California, Netgain Technology, LLC and DOE

County of Residence of First Listed Defendant

(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

Daniel T. Rockey, Bryan Cave Leighton Paisner LLP 3 Embarcadero Center, 7th Fl. San Francisco, CA 94111

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff, 2 U.S. Government Defendant, 3 Federal Question (U.S. Government Not a Party), 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, PTF DEF, 1 1, 2 2, 3 3, 4 4, 5 5, 6 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: Nature of Suit Code Descriptions.

Table with columns: CONTRACT, REAL PROPERTY, CIVIL RIGHTS, TORTS, PRISONER PETITIONS, HABEAS CORPUS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES. Includes various legal categories like Personal Injury, Property Rights, and Tax Suits.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding, 2 Removed from State Court, 3 Remanded from Appellate Court, 4 Reinstated or Reopened, 5 Transferred from Another District, 6 Multidistrict Litigation - Transfer, 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

42 USC 233

Brief description of cause:

Plaintiff alleges violation of Confidentiality of Medical Information Act. Defendant removes under 42 USC 233(l)(2).

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DATE

September 8, 2021

SIGNATURE OF ATTORNEY OF RECORD

/s/ Daniel T. Rockey

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I. **(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

- II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 - United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 - Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 - Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

- III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

- IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).

- V. **Origin.** Place an "X" in one of the seven boxes.
 - Original Proceedings. (1) Cases which originate in the United States district courts.
 - Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
 - Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 - Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 - Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 - Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 - Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.

PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

- VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

- VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P. Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction. Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

- VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

EXHIBIT 1

SUPERIOR COURT OF CALIFORNIA
County of SAN DIEGO

Register of Actions Notice

Case Number:	37-2021-00023936-CU-BT-CTL	Filing Date:	06/01/2021
Case Title:	Doe vs Neighborhood Healthcare [EFILE]	Case Age:	99 days
Case Status:	Pending	Location:	Central
Case Category:	Civil - Unlimited	Judicial Officer:	Joel R. Wohlfeil
Case Type:	Business Tort	Department:	C-73

Future Events

Date	Time	Department	Event
11/05/2021	01:30 PM	C-73	Civil Case Management Conference - Complaint

Participants

Name	Role	Representation
Doe, Jane	Plaintiff	KEEGAN, PATRICK N
Health Center Partners of Southern California	Defendant	
Neighborhood Healthcare	Defendant	Rockey, Daniel T
Netgain Technology LLC	Defendant	

Representation

Name	Address	Phone Number
KEEGAN, PATRICK N	2292 Faraday Avenue Suite 100 Carlsbad CA 92008	
ROCKEY, DANIEL T	3 Embarcadero Center San Francisco CA 94111	(415) 675-3400

ROA#	Entry Date	Short/Long Entry	Filed By
1	06/01/2021	Complaint filed by Doe, Jane. Refers to: Neighborhood Healthcare; Health Center Partners of Southern California; Netgain Technology LLC	Doe, Jane (Plaintiff)
2	06/01/2021	Civil Case Cover Sheet filed by Doe, Jane. Refers to: Neighborhood Healthcare; Health Center Partners of Southern California; Netgain Technology LLC	Doe, Jane (Plaintiff)
3	06/01/2021	Original Summons filed by Doe, Jane. Refers to: Neighborhood Healthcare; Health Center Partners of Southern California; Netgain Technology LLC	Doe, Jane (Plaintiff)
4	06/02/2021	Summons issued.	
5	06/01/2021	Case assigned to Judicial Officer Wohlfeil, Joel.	
6	06/02/2021	Civil Case Management Conference scheduled for 11/05/2021 at 01:30:00 PM at Central in C-73 Joel R. Wohlfeil.	
7	06/02/2021	Civil Case Management Conference scheduled for 11/05/2021 at 01:30:00 PM at Central in C-73 Joel R. Wohlfeil.	
8	06/02/2021	Case initiation form printed.	
9	06/02/2021	Ex Parte scheduled for 06/08/2021 at 08:30:00 AM at Central in C-73 Joel R. Wohlfeil.	
10	06/02/2021	Civil Case Management Conference scheduled for 11/05/2021 at 01:30:00 PM at Central in C-73 Joel R. Wohlfeil was vacated.	
11	06/02/2021	Ex Parte Application - Other and Supporting Documents filed by Doe, Jane.	Doe, Jane (Plaintiff)
12	06/02/2021	Proposed Order submitted by Doe, Jane received but not filed on 06/02/2021.	Doe, Jane (Plaintiff)
13	06/08/2021	Minutes finalized for Ex Parte heard 06/08/2021 08:30:00 AM.	

14	06/08/2021	Order After Hearing (Order granting Pltf's ex parte application to appear by Pseudonym. Order is without prejudice.) filed by Doe, Jane.	Doe, Jane (Plaintiff)
15	06/16/2021	Proof of Service of Summons & Complaint - Unnamed Occupants filed by Doe, Jane.	Doe, Jane (Plaintiff)
16	08/09/2021	Notice and Acknowledgment of Receipt filed by Doe, Jane. Refers to: Health Center Partners of Southern California	Doe, Jane (Plaintiff)
17	08/16/2021	Stipulation - Other - Fee Due (Extending Time to Respond to Initial Complaint and Order) filed by Neighborhood Healthcare; Doe, Jane.	Neighborhood Healthcare (Defendant); Doe, Jane (Plaintiff)

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Telephone: (760) 929-9303
4 Facsimile: (760) 929-9260

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego
06/01/2021 at 04:40:18 PM
Clerk of the Superior Court
By Richard Day, Deputy Clerk

5 Attorneys for Plaintiff JANE DOE

6
7 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
8 **FOR THE COUNTY OF COUNTY OF SAN DIEGO**

9 JANE DOE, individually and on behalf of all
others similarly situated,

10 Plaintiff,

11 vs.

12 NEIGHBORHOOD HEALTHCARE; HEALTH
13 CENTER PARTNERS OF SOUTHERN
CALIFORNIA; NETGAIN TECHNOLOGY,
14 LLC; and DOE DEFENDANTS 1-100;

15 Defendants.
16

) Case No.: 37-2021-00023936-CU-BT-CTL
)

) **CLASS ACTION COMPLAINT FOR**
) **DAMAGES, RESTITUTION, AND**
) **INJUNCTIVE RELIEF FOR VIOLATIONS**
) **OF:**

-) (1) **THE CONFIDENTIALITY OF**
) **MEDICAL INFORMATION ACT,**
) **CIVIL CODE §§ 56, ET SEQ.;**
) (2) **BREACH OF CALIFORNIA**
) **SECURITY NOTIFICATION**
) **LAWS, CALIFORNIA CIVIL CODE**
) **§ 1798.82; AND**
) (3) **BUSINESS AND PROFESSIONS**
) **CODE §§ 17200, ET SEQ.**

) **JURY TRIAL DEMANDED**
)

17
18
19 Plaintiff Jane Doe (or “Plaintiff”), by and through her attorneys, bring this class action on
20 behalf of herself individually and all others similarly situated, against Defendants Neighborhood
21 Healthcare, Health Center Partners of Southern California, and Netgain Technology, LLC
22 (collectively referred to as “Defendants”), and alleges upon information and belief as follows:

23 **INTRODUCTION**

24 1. This class action arises from the negligent and failure of Defendants to properly
25 create, maintain, preserve, and/or store confidential, medical and personal identifying information
26 of Plaintiff¹ and all other persons similarly situated which allowed an unauthorized person to gain
27

28 ¹ California statutory law specifically allows a party to bring a lawsuit using a pseudonym in cases involving health care patients. Cal. Civ. Code § 3427.3 (West 2011). Specifically, section 3427.3

1 access to a computer database server of Defendants from October 22, 2020 to December 3, 2020,
2 causing unauthorized access, viewing, exfiltration, theft, and/or disclosure of unencrypted medical
3 and personal identifying information of Plaintiff and other persons similarly situated, to at least one
4 unauthorized person resulting in violations of the Confidentiality of Medical Information Act, Civil
5 Code §§ 56, *et seq.* (hereinafter referred to as the “Act”), the Security Notification Laws, Civil Code
6 § 1798.82, and the Business and Professions Code §§ 17200 *et seq.* Under the Act, Plaintiff, and
7 all other persons similarly situated, have the right to expect that the confidentiality of their medical
8 information in possession of Defendants and/or derived from Defendants to be reasonably
9 preserved and protected from unauthorized access, viewing, exfiltration, theft, and/or disclosure.

10 2. As alleged more fully below, failing to take adequate and reasonable measures to
11 ensure its data systems were protected against unauthorized intrusions, by failing to invest in cyber
12 security and data protection safeguards, failing to implement adequate and reasonable security
13 controls and user authorization and authentication processes, failing to limit the types of data
14 permitted to be transferred, failing to properly and adequately educate and train its employees, and
15 to put into place reasonable or adequate computer systems and security practices to safeguard
16 customers’ and patients’ medical and personal identifying information, Defendants negligently
17 created, maintained, preserved, and stored Plaintiff’s and the Class (defined *infra*) members’
18 medical and personal identifying information in possession of or derived from Defendants allowed
19 such information to be accessed and actually viewed by at least one unauthorized third party,
20 without Plaintiff’s and the Class members’ prior written authorization, which constitutes
21 unauthorized disclosure and/or release of their information in violation of Civil Code §§ 56.10(a)
22 and 56.101(a) of the Act. In fact, Defendant Health Center Partners of Southern California’s form

23
24
25 provides, “The court having jurisdiction over a civil proceeding under this title shall take all steps
26 ***reasonably necessary to safeguard the individual privacy and prevent harassment of a health care***
27 ***patient***, licensed health practitioner, or employee, client, or customer of a health care facility who is
28 a party or witness in the proceeding, including granting protective orders. ***Health care patients***,
licensed health practitioners, and employees, clients, and customers of the health care facility ***may***
use pseudonyms to protect their privacy.” Cal. Civ. Code § 3427.3 (emphasis added). Here, a
pseudonym has been used in place of the real name of Plaintiff because at all times relevant to this
action, Plaintiff is a health care patient under Civil Code § 56.05(k) and has individual privacy
concerns and a reasonable fear of harassment in light of the nature of the case.

1 letter, entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle, President &
2 Chief Executive Officer, Health Center Partners of Southern California, sent to Plaintiff and all
3 other persons similarly situated, informing them, in part, of “a recent data security incident
4 experienced by Netgain Technology, LLC (‘Netgain’), the IT service provider for Health Center
5 Partners of Southern California (‘HCP’)” and stating, in part, “HCP supports community health
6 centers in a variety of ways, including collaborative grant-funded programs and services for
7 Neighborhood Healthcare.... **What Happened:** Netgain recently informed HCP that it had
8 experienced a data security incident that involved systems containing HCP data.... According to
9 Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital
10 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
11 obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the
12 attacker in exchange for assurances that the attacker will delete all copies of this data and that it will
13 not publish, sell, or otherwise disclose the data.... The information involved varies depending on the
14 individual but may include the following: name, address, date of birth, diagnosis/treatment
15 information and treatment cost information. Once we learned that HCP data may have been
16 involved in the incident, we worked with our cybersecurity experts to review the impacted files and
17 identify the individuals whose information was contained in such files so that we may notify such
18 individuals. Our investigation revealed that the impacted files contained your personal information.”
19 An exemplar of Defendant Health Center Partners of Southern California’s “**Notice of Data**
20 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
21 as **Exhibit A.**

22 3. Additionally, Defendant Neighborhood Healthcare caused a form letter sent on its
23 behalf, entitled “**Notice of Data Breach,**” dated April 8, 2021, signed by Rakesh Patel, CEO,
24 Neighborhood Healthcare, stating, in part, “We are writing to make you aware of an issue brought
25 to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud
26 hosting and managed services provider. Neighborhood Healthcare used Netgain to host some
27 Neighborhood Healthcare files. **What Happened** On November 24, 2020, Netgain became aware
28 of a security incident that involved unauthorized access to portions of the Netgain environment and

1 Netgain client environments and began taking steps to investigate this incident. But, on December
2 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files
3 owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain
4 took additional measures to contain the threat and address the issue. Netgain’s technical teams
5 worked closely with third-party experts to remove the threat in the impacted environments and
6 confirm that client and internal systems are protected. Neighborhood Healthcare learned of the
7 ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to
8 believe that the protected health information (“PHI”) of our patients had been impacted in the
9 incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some
10 information including, potentially, some files containing patient PHI may have been impacted in the
11 incident. Netgain could not confirm, at that time, what records may have been impacted in the
12 incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood
13 Healthcare that Netgain believed were impacted by the attackers. Those files came from a
14 Neighborhood Healthcare server accessible by the Netgain environment. Since that time,
15 Neighborhood Healthcare has worked to review those records, to identify individuals impacted,
16 conduct an investigation into the incident with the assistance outside experts, and to transmit this
17 letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood
18 Healthcare determined that the impacted files included some of your information. **What**
19 **Information Was Involved** The information involved may have included some of the following:
20 your name, date of birth, address, Social Security Number and information about the care that you
21 received from Neighborhood Healthcare such as insurance coverage information, physician you
22 saw, and treatment codes.” An exemplar of Defendant Neighborhood Healthcare’s “**Notice of Data**
23 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
24 as **Exhibit B**.

25 4. Additionally, Defendant Netgain Technology, LLC stated in a blog post, entitled
26 “What we learned as a ransomware victim – so you don’t become one,” that “late last year, Netgain
27 was the victim of a criminal ransomware attack.... to become a victim of such an attack is both
28 humbling and galvanizing.... we identified additional opportunities to strengthn our security posture

1 in a continuous journey with an ongoing commitment to ensure this remains top-of-mind. As part
2 of our incident response, we have implemented a number of these identified enhancements to our
3 security posture and have continued to progress a multipronged approach. We've deployed new
4 tools, revised policies and enforcement procedures, and implemented an advanced around-the-clock
5 managed detections and response service for proactive threat monitoring.”

6 5. Because the individually identifiable medical information and other personal
7 identifying information of Plaintiff and the Class was subject to unauthorized access and viewing by
8 at least one unauthorized third party and in violation of the Act, Plaintiff, individually and on behalf
9 of all others similarly situated, seeks from Defendants nominal damages in the amount of one
10 thousand dollars (\$1,000) for each violation under Civil Code §56.36(b)(1) and actual damages,
11 according to proof, for each violation pursuant to Civil Code § 56.36(b)(2). Further, because
12 Plaintiff also alleges Defendants' conduct violates Business & Professions Code §§ 17200, *et seq.*,
13 Plaintiff, individually and on behalf of others similarly situated, seeks injunctive relief and
14 restitution from Defendants under Business and Professions Code § 17203.

15 6. This action, if successful, will enforce an important right affecting the public interest
16 and would confer a significant benefit, whether pecuniary or non-pecuniary, on a large class of
17 persons. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff
18 in relation to Plaintiff's stake in the matter, and therefore class certification is appropriate in this
19 matter.

20 **JURISDICTION AND VENUE**

21 7. This Court has jurisdiction over this action under California Code of Civil Procedure
22 § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class in the aggregate
23 exceeds the \$25,000 jurisdictional minimum of this Court. Further, the amount in controversy as to
24 Plaintiff individually does not exceed \$75,000.

25 8. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of
26 Civil Procedure §§ 395(a) and 395.5 because Defendant Neighborhood Healthcare is incorporated
27 in and does business in the State of California, and employs persons located in the County of San
28 Diego and in this judicial district. Defendants have obtained medical information of Plaintiff and

1 the Class in the transaction of business in the State of California and in this judicial district, which
2 has caused both obligations and liability of Defendants to arise in the State of California and in this
3 judicial district.

4 9. Further, this action does not qualify for federal jurisdiction under the Class Action
5 Fairness Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies
6 to this action because (1) more than two-thirds of the members of the proposed Class and SubClass
7 are citizens of the State of California, and (2) Defendants are citizens of the State of California.

8 **PARTIES**

9 **A. PLAINTIFF**

10 10. Plaintiff Jane Doe is and was at all times relevant to this action a resident of the State
11 of California and citizen of the State of California. At all times relevant to this action, Plaintiff
12 JANE DOE was a patient of, received medical treatment and diagnosis from, and provided her
13 personal information, including her name, address, date of birth, social security number, phone
14 number and email address to Defendant Neighborhood Healthcare. Additionally, Plaintiff received
15 a letter addressed to her, sent on Defendant Health Center Partners of Southern California’s behalf,
16 entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle, President & Chief
17 Executive Officer, Health Center Partners of Southern California, informing her, in part, of “a
18 recent data security incident experienced by Netgain Technology, LLC (‘Netgain’), the IT service
19 provider for Health Center Partners of Southern California (‘HCP’)” and stating, in part, “HCP
20 supports community health centers in a variety of ways, including collaborative grant-funded
21 programs and services for Neighborhood Healthcare.... **What Happened:** Netgain recently
22 informed HCP that it had experienced a data security incident that involved systems containing
23 HCP data.... According to Netgain, in late September 2020, an unauthorized third party gained
24 access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the
25 unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an
26 undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies
27 of this data and that it will not publish, sell, or otherwise disclose the data.... The information
28 involved varies depending on the individual but may include the following: name, address, date of

1 birth, diagnosis/treatment information and treatment cost information. Once we learned that HCP
2 data may have been involved in the incident, we worked with our cybersecurity experts to review
3 the impacted files and identify the individuals whose information was contained in such files so that
4 we may notify such individuals. Our investigation revealed that the impacted files contained your
5 personal information.” As a result, Plaintiff reasonably fears that disclosure and/or release of her
6 medical information created, maintained, preserved and/or stored on Defendants’ computer
7 networks could subject her to harassment or abuse.

8 **B. DEFENDANTS**

9 11. Defendant Neighborhood Healthcare (“NH”) is a California corporation, is registered
10 to do business and does business in the State of California (CA Corp. No. C0667935), with its
11 principal business office located at 1540 E. Valley Parkway, Escondido CA 92026, and with its
12 registered agent of service of process located at 150 La Terraza Blvd, Suite 201, Escondido CA
13 92025. On or about April 8, 2021, NH caused a form letter sent on its behalf, entitled “**Notice of**
14 **Data Breach,**” dated April 8, 2021, signed by Rakesh Patel, CEO, Neighborhood Healthcare, an
15 exemplar of which is attached hereto as **Exhibit B**, to be submitted to the Attorney General of the
16 State of California. At all times relevant to this action, NH was and is a provider of health care, a
17 contractor, and/or other authorized recipient of personal and confidential medical information, as
18 that term is defined and set forth in the Act, including the names, addresses, dates of birth,
19 diagnosis/treatment information and treatment cost information of Plaintiff and the SubClass
20 (defined *infra*), and is subject to the requirements and mandates of the Act, including but not limited
21 to Civil Code §§ 56.10, 56.101 and 56.36. At all times relevant to this action, NH was and is a
22 provider of health care and employed and employs persons located in the County of San Diego
23 and in this judicial district.

24 12. Defendant Health Center Partners of Southern California (“HCP”) is a business
25 entity doing business in the State of California, with its principal business office located at 3710
26 Ruffin Road, San Diego, CA 92123. On or about April 12, 2021, HCP caused a form letter sent on
27 its behalf, entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle,
28 President & Chief Executive Officer, Health Center Partners of Southern California, an exemplar of

1 which is attached hereto as **Exhibit A**, to be submitted to the Attorney General of the State of
2 California and to be mailed to Plaintiff and the Class. At all times relevant to this action, HCP was
3 and is a “business” within the meaning of Civil Code § 1798.140(c)(1), owns or licenses
4 computerized data which includes Plaintiff’s and the Class’ personal information, within the
5 meaning of Civil Code § 1798.82(h), collected Plaintiff’s and the Class’ personal information
6 within the meaning of Civil Code § 1798.81.5(d)(1)(A).

7 13. Defendant Netgain Technology, LLC (“NETGAIN”) is a business entity doing
8 business in the State of California, with its principal business office located at 5353 Mission Center
9 Road, Suite 202, San Diego, CA 92108. At all times relevant to this action, NETGAIN was and is
10 NH’s and HCP’s third-party vendor. On March 24, 2021, NETGAIN posted on its website a blog,
11 entitled “What we learned as a ransomware victim – so you don’t become one,” which stated, in
12 part, “In our case, late last year, Netgain was the victim of a criminal ransomware attack.... to
13 become a victim of such an attack is both humbling and galvanizing.... we identified additional
14 opportunities to strengthn our security posture in a continuous journey with an ongoing commitment
15 to ensure this remains top-of-mind. As part of our incident response, we have implemented a
16 number of these identified enhancements to our security posture and have continued to progress a
17 multipronged approach. We’ve deployed new tools, revised policies and enforcement procedures,
18 and implemented an advanced around-the-clock managed detections and response service for
19 proactive threat monitoring.”

20 **C. DOE DEFENDANTS**

21 14. The true names and capacities, whether individual, corporate, associate, or otherwise,
22 of Defendants sued herein as Doe Defendants 1 through 100, inclusive, are currently unknown to
23 Plaintiff, who therefore sue the Defendants by such fictitious names under the Code of Civil
24 Procedure § 474. Each of the Defendants designated herein as a Doe Defendant is legally
25 responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of
26 court and/or amend this complaint to reflect the true names and capacities of the Defendants
27 designated hereinafter as Doe Defendants 1 through 100 when such identities become known. Any
28

1 reference made to a named Defendant by specific name or otherwise, individually or plural, is also
2 reference to the actions or inactions of Doe Defendants 1 through 100, inclusive.

3 **D. AGENCY/AIDING AND ABETTING**

4 15. At all times herein mentioned, Defendants, and each of them, were an agent or joint
5 venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the
6 course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the
7 acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized
8 the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

9 16. Defendants, and each of them, aided and abetted, encouraged and rendered
10 substantial assistance to the other Defendants in breaching their obligations to Plaintiff and the
11 Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially
12 assist the commissions of these wrongful acts and other wrongdoings complained of, each of the
13 Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its
14 conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals,
15 and wrongdoing.

16 **FACTUAL ALLEGATIONS**

17 17. As a result, at all times relevant to this action, including the period from October 22,
18 2020 to December 3, 2020, HCP possessed Plaintiff's and the Class' medical information, in
19 electronic and physical form, in possession of or derived from Defendant regarding their medical
20 history, mental or physical condition, or treatment. Such medical information included or contained
21 an element of personal identifying information sufficient to allow identification of Plaintiff and the
22 Class, such as their names, date of birth, addresses, medical record numbers, insurance provider,
23 electronic mail addresses, telephone numbers, or social security numbers, or other information that,
24 alone or in combination with other publicly available information, reveals their identity. At all
25 times relevant to this action, including the period from October 22, 2020 to December 3, 2020, HCP
26 maintained and continues to maintain "medical information," within the meaning of Civil Code §
27 56.05(j), of Plaintiff and the Class, each of which are "patients" within the meaning of Civil Code §
28 56.05(k).

1 18. As a result, at all times relevant to this action, including the period from October 22,
2 2020 to December 3, 2020, NH possessed Plaintiff's and the SubClass' medical information, in
3 electronic and physical form, in possession of or derived from Defendant regarding their medical
4 history, mental or physical condition, or treatment. Such medical information included or contained
5 an element of personal identifying information sufficient to allow identification of Plaintiff and the
6 SubClass, such as their names, date of birth, addresses, medical record numbers, insurance provider,
7 electronic mail addresses, telephone numbers, or social security numbers, or other information that,
8 alone or in combination with other publicly available information, reveals their identity. At all
9 times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH
10 maintained and continues to maintain "medical information," within the meaning of Civil Code §
11 56.05(j), of Plaintiff and the SubClass, each of which are "patients" within the meaning of Civil
12 Code § 56.05(k). At all times relevant to this action, including the period from October 22, 2020 to
13 December 3, 2020, NH was and is a "provider of health care" within the meaning of Civil Code §
14 56.05(m). At all times relevant to this action, including the period from October 22, 2020 to
15 December 3, 2020, Plaintiff and SubClass members were patients, within the meaning of Civil Code
16 § 56.05(k).

17 19. As a result, at all times relevant to this action, including the period from October 22,
18 2020 to December 3, 2020, NETGAIN possessed Plaintiff's, the SubClass' and the Class' medical
19 information, in electronic and physical form, in possession of or derived from Defendant regarding
20 their medical history, mental or physical condition, or treatment. Such medical information
21 included or contained an element of personal identifying information sufficient to allow
22 identification of Plaintiff, the SubClass and the Class, such as their names, date of birth, addresses,
23 medical record numbers, insurance provider, electronic mail addresses, telephone numbers, or social
24 security numbers, or other information that, alone or in combination with other publicly available
25 information, reveals their identity. At all times relevant to this action, including the period from
26 October 22, 2020 to December 3, 2020, NETGAIN maintained and continues to maintain "medical
27 information," within the meaning of Civil Code § 56.05(j), of Plaintiff and the Class, each of which
28 are "patients" within the meaning of Civil Code § 56.05(k).

1 20. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, pursuant to Civil Code § 56.06(a), HCP, as a business that created, maintained,
3 preserved, and stored records of the care, products and services that Plaintiff and the Class members
4 received in the State of California from HCP’s over 16 member community health centers, 140
5 member practice sites, 857,757 patients served, and/or other providers of health care, health care
6 service plans, pharmaceutical companies, and contractors, as defined by the Act, is and was
7 organized for the purpose of maintaining medical information, within the meaning of Civil Code §
8 56.05(j), in order to make the information available to Plaintiff and the Class members or to a
9 provider of health care at the request of Plaintiff and the Class members or a provider of health care,
10 for purposes of allowing Plaintiff and the Class members to manage their information, or for the
11 diagnosis and treatment of Plaintiff and the Class members, is and was deemed to be a “provider of
12 health care,” within the meaning of Civil Code § 56.05(m).

13 21. Alternatively, at all times relevant to this action, including the period from October
14 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), HCP, as an entity that is a
15 medical group, independent practice association, pharmaceutical benefits manager, or a medical
16 service organization, and is not a health care service plan or provider of health care to Plaintiff and
17 the Class members, is and was a “contractor” under Civil Code § 56.05(d).

18 22. Alternatively, at all times relevant to this action, including the period from October
19 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, HCP is and was a recipient of
20 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
21 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
22 further disclosing that medical information except in accordance with a new authorization that
23 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
24 of this chapter or by law.

25 23. Alternatively, at all times relevant to this action, including the period from October
26 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, HCP is and was a recipient of
27 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
28 the Act, and was prohibited from further disclosing such medical information unless in accordance

1 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
2 permitted by other provisions of this chapter or by law.

3 24. Additionally, at all times relevant to this action, including prior to the period from
4 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), HCP is and was an entity
5 engaged in the business of furnishing administrative services to programs that provide payment for
6 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
7 or permitting its employees or agents to use or disclose Plaintiff's and the Class members' medical
8 information possessed in connection with performing administrative functions for a program, except
9 as reasonably necessary in connection with the administration or maintenance of the program, or as
10 required by law, or with an authorization.

11 25. As a provider of health care, a contractor, and/or other authorized recipient of
12 personal and confidential medical information, HCP is required by the Act to ensure that medical
13 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
14 patients' authorization, and to protect and preserve the confidentiality of the medical information
15 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

16 26. At all times relevant to this action, including the period from October 22, 2020 to
17 December 3, 2020, pursuant to Civil Code § 56.06(a), NH, as a business that created, maintained,
18 preserved, and stored records of the care, products and services that Plaintiff and the Class members
19 received in the State of California from NH and/or other providers of health care, health care service
20 plans, pharmaceutical companies, and contractors, as defined by the Act, is and was organized for
21 the purpose of maintaining medical information, within the meaning of Civil Code § 56.05(j), in
22 order to make the information available to Plaintiff and the Class members or to a provider of health
23 care at the request of Plaintiff and the Class members or a provider of health care, for purposes of
24 allowing Plaintiff and the Class members to manage their information, or for the diagnosis and
25 treatment of Plaintiff and the Class members, is and was deemed to be a "provider of health care,"
26 within the meaning of Civil Code § 56.05(m).

27 27. Alternatively, at all times relevant to this action, including the period from October
28 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), NH, as an entity that is a medical

1 group, independent practice association, pharmaceutical benefits manager, or a medical service
2 organization, and is not a health care service plan or provider of health care to Plaintiff and the
3 Class members, is and was a “contractor” under Civil Code § 56.05(d).

4 28. Alternatively, at all times relevant to this action, including the period from October
5 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NH is and was a recipient of
6 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
7 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
8 further disclosing that medical information except in accordance with a new authorization that
9 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
10 of this chapter or by law.

11 29. Alternatively, at all times relevant to this action, including the period from October
12 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NH is and was a recipient of
13 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
14 the Act, and was prohibited from further disclosing such medical information unless in accordance
15 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
16 permitted by other provisions of this chapter or by law.

17 30. Additionally, at all times relevant to this action, including prior to the period from
18 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), NH is and was an entity
19 engaged in the business of furnishing administrative services to programs that provide payment for
20 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
21 or permitting its employees or agents to use or disclose Plaintiff’s and the Class members’ medical
22 information possessed in connection with performing administrative functions for a program, except
23 as reasonably necessary in connection with the administration or maintenance of the program, or as
24 required by law, or with an authorization.

25 31. As a provider of health care, a contractor, and/or other authorized recipient of
26 personal and confidential medical information, NH is required by the Act to ensure that medical
27 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
28

1 patients' authorization, and to protect and preserve the confidentiality of the medical information
2 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

3 32. At all times relevant to this action, including the period from October 22, 2020 to
4 December 3, 2020, pursuant to Civil Code § 56.06(a), NETGAIN, as a business that created,
5 maintained, preserved, and stored records of the care, products and services that Plaintiff and the
6 Class members received in the State of California from NH and/or other providers of health care,
7 health care service plans, pharmaceutical companies, and contractors, as defined by the Act, is and
8 was organized for the purpose of maintaining medical information, within the meaning of Civil
9 Code § 56.05(j), in order to make the information available to Plaintiff and the Class members or to
10 a provider of health care at the request of Plaintiff and the Class members or a provider of health
11 care, for purposes of allowing Plaintiff and the Class members to manage their information, or for
12 the diagnosis and treatment of Plaintiff and the Class members, is and was deemed to be a "provider
13 of health care," within the meaning of Civil Code § 56.05(m).

14 33. Alternatively, at all times relevant to this action, including the period from October
15 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NETGAIN is and was a recipient of
16 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
17 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
18 further disclosing that medical information except in accordance with a new authorization that
19 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
20 of this chapter or by law.

21 34. Alternatively, at all times relevant to this action, including the period from October
22 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NETGAIN is and was a recipient
23 of medical information of Plaintiff and the Class members pursuant to an authorization as provided
24 by the Act, and was prohibited from further disclosing such medical information unless in
25 accordance with a new authorization that meets the requirements of Section 56.21, or as specifically
26 required or permitted by other provisions of this chapter or by law.

27 35. As a provider of health care and/or other authorized recipient of personal and
28 confidential medical information, NETGAIN is required by the Act to ensure that medical

1 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
2 patients' authorization, and to protect and preserve the confidentiality of the medical information
3 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

4 36. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, HCP created, maintained, preserved, and stored records of the care, services and
6 products, including the names, addresses, dates of birth, diagnosis/treatment information and
7 treatment cost information of Plaintiff and the Class (all of which constitutes medical information,
8 as that term is defined and set forth in the Act), that Plaintiff and other Class members received in
9 the State of California from NH and other HCP providers of health care on its computer server.

10 37. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, NH created, maintained, preserved, and stored records of the care, services and
12 products, including the names, addresses, dates of birth, diagnosis/treatment information and
13 treatment cost information of Plaintiff and the SubClass (all of which constitutes medical
14 information, as that term is defined and set forth in the Act), that Plaintiff and other SubClass
15 members received in the State of California from NH on its computer network.

16 38. As a result, on or before October 30, 2020, Defendants possessed Plaintiff's,
17 SubClass' and the Class' medical information, in electronic and physical form, in possession of or
18 derived from Defendants regarding their medical history, mental or physical condition, or treatment.
19 Such medical information included or contained an element of personal identifying information
20 sufficient to allow identification of Plaintiff, the SubClass and the Class, such as their names,
21 addresses, dates of birth, social security numbers, phone numbers and/or email addresses, or other
22 information that, alone or in combination with other publicly available information, reveals their
23 identity.

24 39. As providers of health care, contractors, and/or other recipients of medical
25 information, Defendants are required by the Act to ensure that medical information regarding a
26 patient is not disclosed or disseminated or released without their patients' authorization, and to
27 protect and preserve the confidentiality of the medical information regarding a patient, under Civil
28 Code §§ 56.10, 56.26, 56.36, and 56.101.

1 40. As providers of health care, contractors, and/or other recipients of medical
2 information, Defendants are required by the Act not to disclose medical information regarding a
3 patient without first obtaining an authorization under Civil Code §§ 56.10 and 56.26.

4 41. As providers of health care, contractors, and/or other recipients of medical
5 information, Defendants are required by the Act to create, maintain, preserve, and store medical
6 information in a manner that preserves the confidentiality of the information contained therein
7 under Civil Code § 56.101(a).

8 42. As providers of health care, contractors, and/or other recipients of medical
9 information, Defendants are required by the Act to protect and preserve confidentiality of electronic
10 medical information of Plaintiff and the Class in its possession under Civil Code § 56.101(b)(1)(A).

11 43. As providers of health care, contractors, and/or other recipients of medical
12 information, Defendants are required by the Act to take appropriate preventive actions to protect the
13 confidential information or records against release consistent with Defendants' obligations under
14 the Act, under Civil Code § 56.36(e)(2)(E), or other applicable state law, and the Health Insurance
15 Portability and Accountability Act of 1996 (Public Law 104-191) (HIPAA) and all HIPAA
16 Administrative Simplification Regulations in effect on January 1, 2012, contained in Parts 160, 162,
17 and 164 of Title 45 of the Code of Federal Regulations, and Part 2 of Title 42 of the Code of
18 Federal Regulations, including, but not limited to, all of the following:

- 19 i. Developing and implementing security policies and procedures.
- 20 ii. Designating a security official who is responsible for developing and implementing
21 its security policies and procedures, including educating and training the workforce.
- 22 iii. Encrypting the information or records, and protecting against the release or use of
23 the encryption key and passwords, or transmitting the information or records in a
24 manner designed to provide equal or greater protections against improper
25 disclosures.

26 44. At all times relevant to this action, including the period from October 22, 2020 to
27 December 3, 2020, HCP created, maintained, preserved, and stored Plaintiff's and the Class
28 members' medical information in an un-encrypted format.

1 45. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, NH created, maintained, preserved, and stored Plaintiff’s and the SubClass
3 members’ medical information in an un-encrypted format.

4 46. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, NH disclosed and/or delivered Plaintiff’s and the SubClass members’ medical
6 information to HCP and NETGAIN. At all times relevant to this action, NH did not obtain written
7 authorization from the Plaintiff and the SubClass prior to disclosing and/or delivering Plaintiff’s and
8 the SubClass members’ medical information to HCP and NETGAIN. Furthermore, NH’s disclosure
9 of and/or delivery of Plaintiff’s and the SubClass members’ medical information to HCP and
10 NETGAIN was not permissible without written authorization from the Plaintiff and the SubClass or
11 under any exemption under Civil Code § 56.10(c).

12 47. At all times relevant to this action, including the period from October 22, 2020 to
13 December 3, 2020, HCP created, maintained, preserved, stored, disclosed and/or delivered
14 Plaintiff’s and the Class members’ medical information to NETGAIN on its computer servers. At
15 all times relevant to this action, HCP did not obtain written authorization from the Plaintiff and the
16 Class prior to creating, maintaining, preserving, storing, disclosing and/or delivering Plaintiff’s and
17 the Class members’ medical information to NETGAIN on its computer servers. Furthermore,
18 NETGAIN’s disclosure of and/or delivery of Plaintiff’s and the Class members’ medical
19 information to NETGAIN on its computer servers was not permissible without written authorization
20 from the Plaintiff and the Class or under any exemption under Civil Code § 56.10(c).

21 48. By law, the HIPAA Privacy Rule applies only to covered entities, e.g. health care
22 providers. However, most health care providers do not carry out all of their health care activities
23 and functions by themselves. Instead, they often use the services of a variety of other persons or
24 businesses. The Privacy Rule allows covered providers to disclose protected health information
25 (PHI) to these “business associates” if the providers obtain assurances that the business associate
26 will use the information only for the purposes for which it was engaged by the covered entity, will
27 safeguard the information from misuse, and will help the covered entity comply with some of the
28 covered entity’s duties under the Privacy Rule. Covered entities may disclose PHI to an entity in its

1 role as a business associate only to help the covered entity carry out its health care functions – not
2 for the business associate’s independent use or purposes, except as needed for the proper
3 management and administration of the business associate. The Privacy Rule requires that a covered
4 entity obtain assurances from its business associate that the business associate will appropriately
5 safeguard the PHI it receives or creates on behalf of the covered entity. The satisfactory assurances
6 must be in writing, whether in the form of a contract or other agreement between the covered entity
7 and the business associate.

8 49. When hiring and monitoring a service provider or business associate such as
9 NETGAIN, HCP and NH knew or should have known that they had a duty to inquire about
10 potential service providers’ and business associates’ cybersecurity programs and how such
11 programs are maintained. HCP and NH knew or should have known that they had a duty to
12 compare potential service providers’ and business associates’ cybersecurity programs to the
13 industry standards adopted by other healthcare providers, and should evaluate potential service
14 providers’ track records in the industry by reviewing public information about data security
15 incidents and litigation. HCP and NH knew or should have known that they had a duty to also ask
16 potential service providers and business associates about whether they have experienced any
17 cybersecurity incidents and how such incidents were handled, as well as whether the potential
18 service provider has an insurance policy in place that would cover losses caused by cybersecurity
19 breaches (including losses caused by internal and external threats). HCP and NH knew or should
20 have known that they had a duty to review service provider and business associates contracts to
21 ensure that the contracts require the service providers to comply, on an ongoing basis, with
22 cybersecurity and information security standards (and avoid contract provisions that limit service
23 providers’ responsibility for cybersecurity and information technology breaches). Finally, HCP and
24 NH knew or should have known that they had a duty to pay particular attention to contract terms
25 relating to confidentiality, the use and sharing of information, notice by the vendor of cybersecurity
26 risk assessments and audit reports, cybersecurity breaches and records retention and destruction.

27 50. Alternatively, Plaintiff alleges on information and belief that HCP’s and NH’s
28 disclosure of and/or delivery of Plaintiff’s, the Class’ and the SubClass’ medical information to

1 NETGAIN was either without a business associate agreement or pursuant to a business associate
2 agreement that was not permissible under the Privacy Rule or any exemption under Civil Code §
3 56.10(c), and/or because HCP and NH negligently failed to obtain reasonable assurances and
4 negligently failed to monitor and conduct assessments of NETGAIN to verify that NETGAIN
5 would comply with HIPAA privacy regulations and to follow guidelines and policies to maintain
6 the privacy, confidentiality, including by encryption, and otherwise reasonably protect Plaintiff's
7 and the Class' medical information from disclosure and/or release to at least one unauthorized third
8 party "user" prior to and after HCP's and NH's disclosure of and/or delivery of Plaintiff's and the
9 Class members' medical information to NETGAIN.

10 51. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, at least one "unauthorized third party gained access to Netgain's digital
12 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
13 obtained certain files" containing including Plaintiff's, the SubClass' and the Class' medical
14 information (i.e., their names, addresses, dates of birth, diagnosis/treatment information and
15 treatment cost information) that was located on a NETGAIN server in an un-encrypted format, as
16 represented in HCP's "**Notice of Data Breach**" form letter submitted to the Attorney General of the
17 State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**.

18 52. Defendants had the resources necessary to protect and preserve confidentiality of
19 electronic medical information of Plaintiff, the SubClass and the Class in their possession, but
20 neglected to adequately implement data security measures as required by HIPPA and the Act,
21 despite their obligation to do so.

22 53. Additionally, the risk of vulnerabilities in its computer and data systems of being
23 exploited by an unauthorized third party trying to steal Plaintiff's, the SubClass' and the Class'
24 electronic personally identifying and medical information was foreseeable and/or known to
25 Defendants. The California Data Breach Report 2012-2015, issued in February 2016 by Attorney
26 General, Kamala D. Harris, reported, "Malware and hacking presents the greatest threat, both in the
27 number of breaches and the number of records breached" and "Social Security numbers and
28 medical information – was breached than other data types." Moreover, as Attorney General further

1 reported, just because “[e]xternal adversaries cause most data breaches, [] this does not mean that
2 organizations are solely victims; they are also stewards of the data they collect and maintain. People
3 entrust businesses and other organizations with their data on the understanding that the
4 organizations have a both an ethical and a legal obligation to protect it from unauthorized access.
5 Neglecting to secure systems and data opens a gateway for attackers, who take advantage of
6 uncontrolled vulnerabilities.” Regarding encryption, Attorney General instructed in California Data
7 Breach Report 2012-2015, “As we have said in the past, breaches of this type are preventable.
8 Affordable solutions are widely available: strong full-disk encryption on portable devices and
9 desktop computers when not in use.[] Even small businesses that lack full time information security
10 and IT staff can do this. They owe it to their patients, customers, and employees to do it now.”

11 54. More recently the HIPAA Journal posted on November 1, 2018 warned, “Healthcare
12 organization[s] need to ensure that their systems are well protected against cyberattacks, which
13 means investing in technologies to secure the network perimeter, detect intrusions, and block
14 malware and phishing threats.”

15 55. Further, it also was foreseeable and/or known to Defendants that negligently
16 creating, maintaining, preserving, and/or storing Plaintiff’s, the SubClass’ and the Class’ medical
17 and personal identifying information, in electronic form, onto Defendants’ computer networks in a
18 manner that did not preserve the confidentiality of the information could have a devastating effect
19 on them. As reported in the California Data Breach Report 2012-2015, “There are real costs to
20 individuals. Victims of a data breach are more likely to experience fraud than the general public,
21 according to Javelin Strategy & Research. In 2014, 67 percent of breach victims in the U.S. were
22 also victims of fraud, compared to just 25 percent of all consumers.”

23 56. To be successful, phishing relies on a series of affirmative acts by a company and its
24 employees such as clicking a link, downloading a file, or providing sensitive information. Once
25 criminals gained access to the email accounts of a company and its employees, the email servers
26 communicated—that is, disclosed—the contents of those accounts to the criminals. “Phishing
27 scams are one of the most common ways hackers gain access to sensitive or confidential
28 information. Phishing involves sending fraudulent emails that appear to be from a reputable

1 company, with the goal of deceiving recipients into either clicking on a malicious link or
2 downloading an infected attachment, usually to steal financial or confidential information.”
3 (<https://www.varonis.com/blog/data-breach-statistics/>). As posted on April 21, 2020, the FBI had
4 issued a fresh warning [Alert Number MI-000122-MW] following an increase in COVID-19
5 phishing scams targeting healthcare providers.

6 57. At all times relevant to this action, including the period from October 22, 2020 to
7 December 3, 2020, Defendants negligently created, maintained, preserved, and/or stored Plaintiff’s,
8 the SubClass’ and the Class’ medical information, including Plaintiff’s, the SubClass’ and the
9 Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
10 information, in electronic form, onto Defendants’ computer networks in a manner that did not
11 preserve the confidentiality of the information, and negligently failed to protect and preserve
12 confidentiality of electronic medical information of Plaintiff, the SubClass and the Class in their
13 possession, as required by HIPPA and the Act, and specifically, under Civil Code §§ 56.10(a),
14 56.26(a), 56.36(e)(2)(E), 56.101(a), and 56.101(b)(1)(A), and according to their written
15 representations to Plaintiff and the Class.

16 58. Had Defendants taken such appropriate preventive actions, fix the deficiencies in
17 their data security systems and adopted security measures as required by HIPPA and the Act from
18 October 22, 2020 to December 3, 2020, Defendants could have prevented Plaintiff’s and the Class’
19 electronic medical information within Defendants’ computer networks from being accessed and
20 actually viewed by unauthorized third parties.

21 59. At all times relevant to this action, including the period of from October 22, 2020 to
22 December 3, 2020, NH, by disclosing and/or delivering Plaintiff’s and the SubClass’ personal
23 identifying and medical information to HCP, allowed Plaintiff’s and the SubClass’ personal
24 identifying and medical information to be accessed and actually viewed by at least one unauthorized
25 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
26 Code § 56.10(a).

27 60. At all times relevant to this action, including the period of from October 22, 2020 to
28 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic

1 medical information of Plaintiff and the SubClass on NETGAIN’s computer server, allowed
2 Plaintiff’s and the SubClass’ medical and personal identifying information to be accessed and
3 actually viewed by at least one unauthorized third party, without first obtaining an authorization,
4 constituting a disclosure in violation of Civil Code § 56.10(a).

5 61. At all times relevant to this action, including the period from October 22, 2020 to
6 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
7 medical information of Plaintiff and the Class on NETGAIN’s computer server, allowed Plaintiff’s
8 and the Class’ medical and personal identifying information to be accessed and actually viewed by
9 at least one unauthorized third party, without first obtaining an authorization, constituting a
10 disclosure in violation of Civil Code § 56.10(a).

11 62. At all times relevant to this action, including the period from October 22, 2020 to
12 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
13 medical information of Plaintiff and the Class on NETGAIN’s computer server, allowed Plaintiff’s
14 and the Class’ medical and personal identifying information to be accessed and actually viewed by
15 at least one unauthorized third party, without first obtaining an authorization, constituting a
16 disclosure in violation of Civil Code § 56.26(a).

17 63. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, NH, by disclosing and/or delivering Plaintiff’s and the SubClass members’
19 medical and personal identifying information to HCP, allowed Plaintiff’s and the SubClass’ medical
20 and personal identifying information to be accessed and actually viewed by at least one
21 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

22 64. At all times relevant to this action, including the period from October 22, 2020 to
23 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic
24 medical information of Plaintiff and the SubClass on NETGAIN’s computer server, allowed
25 Plaintiff’s and the SubClass’ medical and personal identifying information to be accessed and
26 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
27 Code § 56.101(a).

28

1 65. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
3 medical information of Plaintiff and the Class on NETGAIN’s computer server, allowed Plaintiff’s
4 and the Class’ medical and personal identifying information to be accessed and actually viewed by
5 at least one unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

6 66. At all times relevant to this action, including the period from October 22, 2020 to
7 December 3, 2020, NH, by disclosing and/or delivering Plaintiff’s and the SubClass members’
8 medical and personal identifying information to HCP, allowed Plaintiff’s and the SubClass’ medical
9 and personal identifying information to be accessed and actually viewed by at least one
10 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

11 67. At all times relevant to this action, including the period from October 22, 2020 to
12 December 3, 2020, NH’s negligent failure to protect and preserve confidentiality of electronic
13 medical information of Plaintiff and the SubClass, on NETGAIN’s computer server, allowed
14 Plaintiff’s and the SubClass’ medical and personal identifying information to be accessed and
15 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
16 Code § 56.101(b)(1)(A).

17 68. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, HCP’s negligent failure to protect and preserve confidentiality of electronic
19 medical information of Plaintiff and the Class, on NETGAIN’s computer server, allowed Plaintiff’s
20 and the Class’ medical and personal identifying information to be accessed and actually viewed by
21 at least one unauthorized third party, constituting a release in violation of Civil Code §
22 56.101(b)(1)(A).

23 69. On or about April 12, 2021, HCP caused a form letter, entitled “**Notice of Data**
24 **Breach,**” dated April 12, 2021, signed by Henry Tuttle, President & Chief Executive Officer,
25 Health Center Partners of Southern California, to be mailed to Plaintiff and the Class, informing
26 them, in part, of “a recent data security incident experienced by Netgain Technology, LLC
27 (‘Netgain’), the IT service provider for Health Center Partners of Southern California (‘HCP’)” and
28 stating, in part, “HCP supports community health centers in a variety of ways, including

1 collaborative grant-funded programs and services for Neighborhood Healthcare.... **What**
2 **Happened:** Netgain recently informed HCP that it had experienced a data security incident that
3 involved systems containing HCP data.... According to Netgain, in late September 2020, an
4 unauthorized third party gained access to Netgain’s digital environment, and between October 22,
5 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data.
6 Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the
7 attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the
8 data.... The information involved varies depending on the individual but may include the following:
9 name, address, date of birth, diagnosis/treatment information and treatment cost information. Once
10 we learned that HCP data may have been involved in the incident, we worked with our
11 cybersecurity experts to review the impacted files and identify the individuals whose information
12 was contained in such files so that we may notify such individuals. Our investigation revealed that
13 the impacted files contained your personal information.” An exemplar of HCP’s “**Notice of Data**
14 **Breach**” form letter submitted to the Attorney General of the State of California and mailed to
15 Plaintiff and the Class is attached hereto as **Exhibit A**. Plaintiff received in the mail a HCP “**Notice**
16 **of Data Breach**” form letter, addressed to her, which alerted Plaintiff that her medical and personal
17 identifying information, along with other Class members, was improperly accessed by at least one
18 unauthorized third party. As a result, Plaintiff fears that disclosure and/or release of her medical
19 and personal identifying information created, maintained, preserved, and/or stored on Defendants’
20 computer networks could subject her to harassment or abuse. Moreover, although thereafter, on
21 May 4, 2021, Plaintiff wrote both HCP and NH separately requesting further information about this
22 security incident, neither HCP nor NH provided a substantive response to her requests.

23 70. HCP’s “**Notice of Data Breach**” form letter submitted to the Attorney General of
24 the State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**, further
25 states, “**What We Are Doing:** [] We are providing you with steps that you can take to help protect
26 your personal information, and as an added precaution, we are offering you complimentary identity
27 protection services through IDX, a leader in risk mitigation and response.”
28

1 71. HCP’s “**Notice of Data Breach**” form letter concludes by making the following
2 hollow gesture, “The security of your information is a top priority for HCP, and we are committed
3 to safeguarding your data and privacy.” Other than offering “steps that you can take to help protect
4 your personal information” and “complimentary identity protection services through IDX” “as an
5 added precaution,” HCP’s “**Notice of Data Breach**” form letter does nothing to further protect
6 Plaintiff and the Class from future incidents of identity theft despite the severity of the unauthorized
7 access, viewing, exfiltration, theft, disclosure and/or release of their electronic medical and personal
8 information caused by Defendants’ violations of their duty to implement and maintain reasonable
9 security procedures and practices.

10 72. To date, other than offering “steps that you can take to help protect your personal
11 information” and “complimentary identity protection services through IDX” “as an added
12 precaution,” HCP has not offered any monetary compensation for the unauthorized disclosure
13 and/or release of Plaintiff’s and the Class’ electronic medical information under the Act. In effect,
14 HCP is shirking its responsibility for the harm it has caused, while shifting the burdens and costs of
15 its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

16 73. To date, NH has not offered any compensation for the unauthorized disclosure and/or
17 release of Plaintiff’s and SubClass’ electronic medical information under the Act. In effect, NH is
18 shirking its responsibility for the harm it has caused, while shifting the burdens and costs of its
19 wrongful conduct onto its patients, i.e. Plaintiff and the SubClass.

20 74. To date, NETGAIN has not offered any monetary compensation for the unauthorized
21 disclosure and/or release of Plaintiff’s and the Class’ electronic medical information under the Act.
22 In effect, NETGAIN is shirking its responsibility for the harm it has caused, while shifting the
23 burdens and costs of its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

24 75. Based upon the information posted on the U.S. Department of Health and Human
25 Services’ official website, HCP reported on “04/09/2021” a “Hacking/IT Incident” involving
26 “Network Server” affecting “293,516” persons, which involved a “Business Associate,” to the U.S.
27 Department of Health & Human Services’ Office for Civil Rights.

28

1 76. Based upon the information posted on the U.S. Department of Health and Human
2 Services' official website, NH reported on "04/14/2021" a "Hacking/IT Incident" involving
3 "Network Server" affecting "45,200" persons, which involved a "Business Associate," to the U.S.
4 Department of Health & Human Services' Office for Civil Rights.

5 77. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA
6 covered entities to provide notification following a breach of unsecured protected health
7 information. Following a breach of unsecured protected health information, covered entities must
8 provide notification of the breach to affected individuals. Covered entities must *only* provide the
9 required notifications if the breach involved unsecured protected health information. Unsecured
10 protected health information is protected health information (PHI) that has not been rendered
11 unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or
12 methodology specified by the Secretary of the U.S. Department of Health and Human Services in
13 guidance. Under approved guidance of the U.S. Department of Health and Human Services, PHI is
14 rendered unusable, unreadable, or indecipherable to unauthorized individuals if (1) electronic PHI
15 has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process
16 to transform data into a form in which there is a low probability of assigning meaning without use
17 of a confidential process or key" (45 CFR 164.304 definition of encryption) and (2) such
18 confidential process or key that might enable decryption has not been breached. By reporting this
19 incident to the U.S. Department of Health and Human Services, HCP and NH each has separately
20 determined and is affirming that Plaintiff's, the Class' and the SubClass' electronic PHI was either
21 not encrypted at all, or if it was encrypted, the encryption has been breached by the unauthorized
22 third party. Further, because Plaintiff's, the Class' and the SubClass' identifiable medical
23 information contained in NETGAIN's computer server was not rendered unusable, unreadable, or
24 indecipherable, the unauthorized third party or parties who "obtained" and downloaded Plaintiff's
25 and the Class' identifiable medical information was able to and did actually view Plaintiff's, the
26 Class' and the SubClass' electronic medical information contained in and "obtained" and
27 downloaded from NETGAIN's computer server. As a result, HCP and NH each has separately
28 determined and have affirmed that Plaintiff's, the Class' and the SubClass' identifiable medical

1 information contained in NETGAIN’s computer server was unencrypted and thus, the unauthorized
 2 third party or parties who “obtained” and downloaded Plaintiff’s, the Class’ and the SubClass’
 3 identifiable medical information was able to and did actually view Plaintiff’s, the Class’ and the
 4 SubClass’ electronic medical information contained in and “obtained” and downloaded from
 5 NETGAIN’s computer server. Therefore, HCP, NH and NETGAIN was negligent for failing to
 6 encrypt or adequately encrypt Plaintiff’s, the Class’ and the SubClass’ electronic medical
 7 information contained in NETGAIN’s computer server.

8 78. As a result, Defendants were negligent for failing to encrypt or adequately encrypt
 9 Plaintiff’s, the Class’ and the SubClass’ electronic medical information on their computer networks.
 10 Further, because Plaintiff’s, the Class’ and the SubClass’ identifiable medical information on
 11 Defendants’ computer networks was not rendered unusable, unreadable, or indecipherable, the
 12 unauthorized third party or parties who accessed Plaintiff’s, the Class’ and the SubClass’
 13 identifiable medical information was able to and did view Plaintiff’s, the Class’ and the SubClass’
 14 electronic medical information contained within NETGAIN’s computer server.

CLASS ACTION ALLEGATIONS

15
 16 79. Plaintiff brings this action on behalf of herself individually and on behalf of all
 17 others similarly situated. The putative class and subclass that Plaintiff seeks to represent is defined
 18 as follows:

19 Class: All persons to whom Health Center Partners of Southern California sent a
 20 notification letter of a data security incident that has occurred between October
 21 22, 2020 to December 3, 2020, an exemplar of which is attached hereto as
Exhibit A.

22 SubClass: All persons to whom Neighborhood Healthcare sent a notification
 23 letter of a data security incident that has occurred between November 24, 2020 to
 24 December 3, 2020, an exemplar of which is attached hereto as **Exhibit B.**

25 The officers, directors, employees, and agents of Defendants and any “affiliate,” “principal” or
 26 “subsidiary” of Defendants, as defined in the Corporations Code §§ 150, 175, and 189, respectively,
 27 are excluded from the Class and the SubClass. Plaintiff reserves the right under California Rule of
 28 Court 3.765 to amend or modify the Class definition with greater particularity or further division

1 into subclasses or limitation to particular issues as warranted, and as additional facts are discovery
2 by Plaintiff during her future investigations.

3 80. This action is properly maintainable as a class action. The members of the Class and
4 the SubClass are so numerous that joinder of all members is impracticable, if not completely
5 impossible. While the exact number of the Class is unknown to Plaintiff at this time, HCP filed a
6 report with the U.S. Department of Health & Human Services' Office for Civil Rights, on or about
7 December 28, 2020, that this incident affected 293,516 persons. The disposition of the claims of
8 the members of Class through this class action will benefit both the parties and this Court. In
9 addition, the Class and the SubClass is readily identifiable from information and records in the
10 possession of Defendants and their agents, and the Class and the SubClass is defined in objective
11 terms that make the eventual identification of the Class and the SubClass members possible and/or
12 sufficient to allow members of the Class and the SubClass identify themselves as having a right to
13 recover.

14 81. There is a well-defined community of interest among the members of the Class and
15 the SubClass because common questions of law and fact predominate, Plaintiff's claims are typical
16 of the members of the class, and Plaintiff can fairly and adequately represent the interests of the
17 Class.

18 82. Common questions of law and fact exist as to all members of the Class and the
19 SubClass and predominate over any questions affecting solely individual members of the Class and
20 the SubClass. Among the questions of law and fact common to the Class that predominate over
21 questions which may affect individual Class members, including the following:

- 22 a) Whether Defendants possessed Plaintiff's, the SubClass' and the Class' medical and
23 personal identifying information from October 22, 2020 to December 3, 2020;
24 b) Whether Defendants created, maintained, preserved and/or stored Plaintiff's, the
25 SubClass' and the Class' medical and personal identifying information, in electronic
26 form, onto Defendants' computer networks from October 22, 2020 to December 3,
27 2020;

- 1 c) Whether Defendants implemented and maintained reasonable security procedures
2 and practices to protect Plaintiff's, the SubClass' and the Class' medical and
3 personal identifying information, in electronic form, within Defendants' computer
4 networks from October 22, 2020 to December 3, 2020;
- 5 d) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
6 information, in electronic form, within Defendants' computer networks from October
7 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
8 exposed by an unauthorized third party;
- 9 e) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
10 information, in electronic form, within Defendants' computer networks from October
11 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
12 exposed by an unauthorized third party without the prior written authorization of
13 Plaintiff, the SubClass and the Class, as required by Civil Code §§ 56.10 and 56.26;
- 14 f) Whether Defendants' creation, maintenance, preservation and/or storage of
15 Plaintiff's, the SubClass' and the Class' medical and personal identifying
16 information, in electronic form, within Defendants' computer networks, accessed,
17 viewed, exfiltrated and/or publicly exposed by an unauthorized third party was
18 permissible without written authorization from Plaintiff, the SubClass and the Class
19 or under any exemption under Civil Code § 56.10(c);
- 20 g) Whether Defendants' creation, maintenance, preservation and/or storage of
21 Plaintiff's, the SubClass' and the Class' medical and personal identifying
22 information, in electronic form, within Defendants' computer networks, accessed,
23 viewed, exfiltrated and/or publicly exposed by an unauthorized third party
24 constitutes a release in violation of Civil Code §56.101;
- 25 h) Whether the timing of HCP's notice that Plaintiff's and the Class' medical and
26 personal identifying information, in electronic form, was accessed, viewed,
27 exfiltrated and/or publicly exposed by an unauthorized third party, was given in the
28 most expedient time possible and without reasonable delay;

1 i) Whether Defendants' conduct constitute unlawful, fraudulent or unfair practices in
2 violation of Business and Professions Code §§ 17200, *et seq.*; and

3 j) Whether Plaintiff, the SubClass and the Class are entitled to actual, nominal or
4 statutory damages, injunctive relief and/or restitution.

5 83. Plaintiff's claims are typical of those of the other SubClass and Class members
6 because Plaintiff, like every other SubClass and Class member, were exposed to virtually identical
7 conduct and now suffer from the same violations of the law as other SubClass and Class members.

8 84. Plaintiff will fairly and adequately protect the interests of the SubClass and the
9 Class. Moreover, Plaintiff has no interest that is contrary to or in conflict with those of the
10 SubClass and the Class, she seeks to represent. In addition, Plaintiff has retained competent counsel
11 experienced in class action litigation to further ensure such protection and intend to prosecute this
12 action vigorously.

13 85. The nature of this action and the nature of laws available to Plaintiff and the other
14 SubClass and Class members make the use of the class action format a particularly efficient and
15 appropriate procedure to afford relief to Plaintiff and the other SubClass and Class members for the
16 claims alleged and the disposition of whose claims in a class action will provide substantial benefits
17 to both the parties and the Court because:

18 a) If each of the SubClass and the Class members were required to file an individual
19 lawsuit, the Defendants would necessarily gain an unconscionable advantage since
20 they would be able to exploit and overwhelm the limited resources of each individual
21 member of the SubClass and Class with its vastly superior financial and legal
22 resources;

23 b) The costs of individual suits could unreasonably consume the amounts that would be
24 recovered;

25 c) Proof of a common business practice or factual pattern which Plaintiff experienced is
26 representative of that experienced by the SubClass and the Class and will establish
27 the right of each of the members to recover on the causes of action alleged;

28

- 1 d) Individual actions would create a risk of inconsistent results and would be
- 2 unnecessary and duplicative of this litigation; and
- 3 e) The disposition of the claims of the members of the SubClass and the Class through
- 4 this class action will produce salutary by-products, including a therapeutic effect
- 5 upon those who indulge in fraudulent practices, and aid to legitimate business
- 6 enterprises by curtailing illegitimate competition.

7 86. The prosecution of separate actions by individual members of the SubClass and the
8 Class would create a risk of inconsistent or varying adjudications with respect to individual
9 members of the SubClass and the Class, which would establish incompatible standards of conduct
10 for the Defendants in the State of California and would lead to repetitious trials of the numerous
11 common questions of fact and law in the State of California. Plaintiff knows of no difficulty that
12 will be encountered in the management of this litigation that would preclude its maintenance as a
13 class action. As a result, a class action is superior to other available methods for the fair and
14 efficient adjudication of this controversy.

15 87. Notice to the members of the SubClass and the Class may be made by e-mail or first-
16 class mail addressed to all persons who have been individually identified by Defendants and who
17 have been given notice of the data breach.

18 88. Plaintiff, the SubClass and the Class have suffered irreparable harm and damages
19 because of Defendants' wrongful conduct as alleged herein. Absent certification, Plaintiff, the
20 SubClass and the Class will continue to be damaged and to suffer by the unauthorized disclosure
21 and/or release of their medical and personal identifying information, thereby allowing these
22 violations of law to proceed without remedy.

23 89. Moreover, Plaintiff's, the SubClass' and the Class' individual damages are
24 insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendants'
25 violations of law inflicting substantial damages in the aggregate would go unremedied. In addition,
26 Defendants have acted or refused to act on grounds generally applicable to Plaintiff, the SubClass
27 and the Class, thereby making appropriate final injunctive relief with respect to, the Class as a
28 whole.

FIRST CAUSE OF ACTION
Violations of the Confidentiality of Medical Information Act
California Civil Code §§ 56, et seq.
(On Behalf of Plaintiff and the SubClass Against NH)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

90. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if fully stated herein.

91. At all times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH is considered a “provider of health care,” within the meaning of Civil Code § 56.05(m), and maintained and continues to maintain “medical information” within the meaning of Civil Code § 56.05(j), of Plaintiff and the SubClass.

92. Plaintiff and the SubClass are “patients” of NH within the meaning of Civil Code § 56.05(k) and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure and/or release of their medical information could subject them to harassment or abuse.

93. At all times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH negligently created, maintained, preserved, and/or stored Plaintiff’s and the SubClass’ medical information, including Plaintiff’s and the SubClass’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in electronic form, onto Defendants’ computer networks in a manner that did not preserve the confidentiality of the information, and negligently failed to protect and preserve confidentiality of electronic medical information of Plaintiff and the SubClass in its possession, as required by the Act, and specifically, under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and 56.36(e)(2)(E), and according to their written representations to Plaintiff and the SubClass.

94. Due to NH’s disclosure and/or delivery Plaintiff’s and the SubClass members’ medical and personal identifying information to HCP without written authorization from Plaintiff and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff’s and the SubClass’ medical information, including Plaintiff’s and the SubClass’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be accessed and actually viewed by at least one unauthorized third party, without first obtaining an

1 authorization, constituting a disclosure in violation of Civil Code §§ 56.10, 56.13, 56.245, and
2 56.26(a).

3 95. Due to NH's negligent creation, maintenance, preservation and/or storage of
4 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server, NH
5 allowed Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass'
6 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
7 electronic form, to be accessed and actually viewed by at least one unauthorized third party, without
8 first obtaining an authorization, constituting a disclosure in violation of Civil Code §§ 56.10, 56.13,
9 56.245, and 56.26(a).

10 96. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass members'
11 medical and personal identifying information to HCP without written authorization from Plaintiff
12 and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff's and
13 the SubClass' medical information, including Plaintiff's and the SubClass' names, addresses, dates
14 of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be
15 accessed and actually viewed by at least one unauthorized third party, constituting a release in
16 violation of Civil Code § 56.101(a).

17 97. Due to NH's negligent creation, maintenance, preservation and/or storage of
18 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server,
19 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
20 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
21 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
22 constituting a release in violation of Civil Code § 56.101(a).

23 98. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass' medical
24 information and personal identifying information to HCP without written authorization from
25 Plaintiff and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed
26 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
27 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
28

1 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
2 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

3 99. Due to NH’s negligent creation, maintenance, preservation and/or storage of
4 Plaintiff’s and the SubClass members’ medical information on NETGAIN’s computer server, NH
5 allowed Plaintiff’s and the SubClass’ medical information, including Plaintiff’s and the SubClass’
6 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
7 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
8 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

9 100. As a result of NH’s above-described conduct in violation of the Act, Plaintiff and the
10 SubClass have suffered damages from the unauthorized disclosure and/or release of their medical
11 and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

12 101. As a result of NHs’ above-described conduct in violation of the Act, Plaintiff and the
13 SubClass seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
14 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
15 Code § 56.36(b)(2).

16 **SECOND CAUSE OF ACTION**
17 **Violations of the Confidentiality of Medical Information Act**
18 **California Civil Code §§ 56, et seq.**
19 **(On Behalf of Plaintiff and the Class Against HCP)**

20 102. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
21 fully stated herein.

22 103. At all times relevant to this action, including the period from October 22, 2020 to
23 December 3, 2020, HCP is considered a “provider of health care” within the meaning of Civil Code
24 § 56.05(m), a “contractor” under Civil Code § 56.05(d), and/or “engaged in the business of
25 furnishing administrative services to programs that provide payment for health care services” under
26 Civil Code § 56.26(a), and maintained and continues to maintain “medical information” within the
27 meaning of Civil Code § 56.05(j), of Plaintiff and the Class.
28

1 104. Plaintiff and the Class are “patients” within the meaning of Civil Code § 56.05(k)
2 and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure
3 and/or release of their medical information could subject them to harassment or abuse.

4 105. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, HCP negligently created, maintained, preserved, and/or stored Plaintiff’s and the
6 Class’ medical information, including Plaintiff’s and the Class’ names, addresses, dates of birth,
7 diagnosis/treatment information and treatment cost information, in electronic form, onto
8 NETGAIN’s computer server in a manner that did not preserve the confidentiality of the
9 information, and negligently failed to protect and preserve confidentiality of electronic medical
10 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
11 under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
12 56.36(e)(2)(E).

13 106. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
14 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
15 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
16 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
17 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
18 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
19 Code §§ 56.10, 56.13, 56.245, and 56.26(a).

20 107. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
21 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
22 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
23 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
24 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
25 third party, constituting a release in violation of Civil Code § 56.101(a).

26 108. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
27 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
28 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s

1 and the Class' names, addresses, dates of birth, diagnosis/treatment information and treatment cost
2 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
3 third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

4 109. As a result of HCP's above-described conduct in violation of the Act, Plaintiff and
5 the Class have suffered damages from the unauthorized disclosure and/or release of their medical
6 and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

7 110. As a result of HCP's above-described conduct in violation of the Act, Plaintiff and
8 the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
9 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
10 Code § 56.36(b)(2).

11 **THIRD CAUSE OF ACTION**
12 **Violations of the Confidentiality of Medical Information Act**
13 **California Civil Code §§ 56, et seq.**
14 **(On Behalf of Plaintiff and the Class Against NETGAIN)**

15 111. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
16 fully stated herein.

17 112. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, NETGAIN is considered a "provider of health care" within the meaning of Civil
19 Code § 56.05(m), and maintained and continues to maintain "medical information" within the
20 meaning of Civil Code § 56.05(j), of Plaintiff and the Class.

21 113. Plaintiff and the Class are "patients" within the meaning of Civil Code § 56.05(k)
22 and are "Endanger" within the meaning of Civil Code § 56.05(e) because they fear that disclosure
23 and/or release of their medical information could subject them to harassment or abuse.

24 114. At all times relevant to this action, including the period from October 22, 2020 to
25 December 3, 2020, NETGAIN negligently created, maintained, preserved, and/or stored Plaintiff's
26 and the Class' medical information, including Plaintiff's and the Class' names, addresses, dates of
27 birth, diagnosis/treatment information and treatment cost information, in electronic form, onto
28 NETGAIN's computer server in a manner that did not preserve the confidentiality of the
information, and negligently failed to protect and preserve confidentiality of electronic medical

1 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
2 under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
3 56.36(e)(2)(E).

4 115. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
5 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
6 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
7 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
8 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
9 unauthorized third party, without first obtaining an authorization, constituting a disclosure in
10 violation of Civil Code §§ 56.10, 56.13, 56.245, and 56.26(a).

11 116. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
12 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
13 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
14 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
15 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
16 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

17 117. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
18 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
19 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
20 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
21 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
22 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

23 118. As a result of NETGAIN's above-described conduct in violation of the Act, Plaintiff
24 and the Class have suffered damages from the unauthorized disclosure and/or release of their
25 medical and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

26 119. As a result of NETGAIN's above-described conduct in violation of the Act, Plaintiff
27 and the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
28

1 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
2 Code § 56.36(b)(2).

3 **FOURTH CAUSE OF ACTION**
4 **Breach of California Security Notification Laws**
5 **California Civil Code § 1798.82**
6 **(On Behalf of Plaintiff and the Class Against HCP)**

7 120. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
8 fully stated herein.

9 121. Pursuant to Civil Code § 1798.82(a), “A person or business that conducts business in
10 California, and that owns or licenses computerized data that includes personal information, shall
11 disclose a breach of the security of the system following discovery or notification of the breach in
12 the security of the data to a resident of California (1) whose unencrypted personal information was,
13 or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted
14 personal information was, or is reasonably believed to have been, acquired by an unauthorized
15 person and the encryption key or security credential was, or is reasonably believed to have been,
16 acquired by an unauthorized person and the person or business that owns or licenses the encrypted
17 information has a reasonable belief that the encryption key or security credential could render that
18 personal information readable or usable. The disclosure shall be made in the most expedient time
19 possible and without unreasonable delay, consistent with the legitimate needs of law enforcement,
20 as provided in subdivision (c), or any measures necessary to determine the scope of the breach and
21 restore the reasonable integrity of the data system.” Prior to passages of such statute, the California
22 State Assembly cited an incident where authorities knew of the breach in security for 21 days
23 “before state workers were told” as an example of “late notice.”

24 122. Civil Code § 1798.82 further provides, “(h) For purposes of this section, ‘personal
25 information’ means an individual’s first name or first initial and last name in combination with any
26 one or more of the following data elements, when either the name or the data elements are not
27 encrypted: (1) Social security number. (2) Driver’s license number or California Identification Card
28 number. (3) Account number, credit or debit card number, in combination with any required
security code, access code, or password that would permit access to an individual's financial

1 account. (4) Medical information. (5) Health insurance information. (i) (2) For purposes of this
2 section, ‘medical information’ means any information regarding an individual’s medical history,
3 mental or physical condition, or medical treatment or diagnosis by a health care professional. (3)
4 For purposes of this section, ‘health insurance information’ means an individual’s health insurance
5 policy number or subscriber identification number, any unique identifier used by a health insurer to
6 identify the individual, or any information in an individual’s application and claims history,
7 including any appeals records.”

8 123. HCP conducts business in California and owns or licenses computerized data which
9 includes the personal information, within the meaning of Civil Code § 1798.82(h), of Plaintiff and
10 the Class.

11 124. Based upon NH’s “**Notice of Data Breach**” form letter, HCP was aware that
12 Plaintiff’s and the Class’ unencrypted personal information on NETGAIN’s computer server was,
13 or is reasonably believed to have been, acquired by an unauthorized person no later than December
14 3, 2020, but did not begin to mail notification letters to Plaintiff and the Class until April 12, 2021.
15 Thus, HCP waited at least 131 days before *beginning* to inform Plaintiff and the Class of this
16 incident and the subsequent threat to Plaintiff’s and the Class’ personal information. As a result,
17 HCP did not disclose to Plaintiff and the Class that their personal information was, or was
18 reasonably believed to have been, acquired by an unauthorized person, in the most expedient time
19 possible and without reasonable delay in violation of Civil Code § 1798.82(a). Given the example
20 of the Legislature finding that a delay of 21 days to be “late notice” under the statute, HCP’s delay
21 of 131 days before *beginning* to inform Plaintiff and the Class that their personal information was,
22 or was reasonably believed to have been, acquired by an unauthorized person by mailing HCP’s
23 form letter to Plaintiff and the Class is presumptively unreasonable notice in violation of Civil Code
24 § 1798.82(a).

25 125. Plaintiff and the Class have been injured by fact that HCP did not disclose their
26 personal information was, or was reasonably believed to have been, acquired by an unauthorized
27 person in the most expedient time possible and without reasonable delay in violation of Civil Code
28 § 1798.82(a). HCP’s delays in informing required by Civil Code § 1798.82(a) and providing all of

1 the information required by Civil Code § 1798.82(d) to Plaintiff and the Class that their personal
2 information was, or was reasonably believed to have been, acquired by an unauthorized person,
3 have prevented Plaintiff and the Class from taking steps to protect their personal information from
4 unauthorized use and/or identify theft.

5 126. Plaintiff and the Class seek recovery of their damages pursuant to Civil Code §
6 1798.84(b) and injunctive relief pursuant to Civil Code § 1798.84(e).

7 **FIFTH CAUSE OF ACTION**
8 **Unlawful and Unfair Business Acts and Practices in Violation of**
9 **California Business & Professions Code §17200, *et seq.***
10 **(On Behalf of Plaintiff, the SubClass and the Class Against All Defendants)**

11 127. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
12 fully stated herein.

13 128. The acts, misrepresentations, omissions, practices, and non-disclosures of
14 Defendants as alleged herein constituted unlawful and unfair business acts and practices within the
15 meaning of California Business & Professions Code §§ 17200, *et seq.*

16 129. By the aforementioned business acts or practices, Defendants have engaged in
17 “unlawful” business acts and practices in violation of the aforementioned statutes, including Civil
18 Code §§ 56.10(a), 56.26(a), 56.36(e)(2)(E), 56.101(a), 56.101(b)(1)(A), 1798.82(a) and 1798.82(d).
19 Plaintiff reserves the right to allege other violations of law committed by Defendants which
20 constitute unlawful acts or practices within the meaning of California Business & Professions Code
21 §§ 17200, *et seq.*

22 130. By the aforementioned business acts or practices, Defendants have also engaged in
23 “unfair” business acts or practices in that the harm caused by Defendants’ failure to maintain
24 adequate information security procedures and practices, including but not limited to, failing to take
25 adequate and reasonable measures to ensure its data systems were protected against unauthorized
26 intrusions, failing to properly and adequately educate and train its employees, failing to put into
27 place reasonable or adequately computer systems and security practices to safeguard patients’
28 identifiable medical information including access restrictions and encryption, failing to have
adequate privacy policies and procedures in place that did not preserve the confidentiality of the

1 medical and personal identifying information of Plaintiff, the SubClass and the Class in their
2 possession, and failing to protect and preserve confidentiality of electronic medical information of
3 Plaintiff, the SubClass and the Class in their possession against disclosure and/or release, outweighs
4 the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous,
5 unethical, deceitful and offensive, and causes substantial injury to Plaintiff, the SubClass and the
6 Class.

7 131. Defendants have obtain money and property from Plaintiff, the SubClass and the
8 Class because of the payment of the services and products they received from Defendants. Plaintiff,
9 the SubClass and the Class have suffered an injury in fact by acquiring less in their transactions
10 with Defendants for the services and products they received from Defendants than they otherwise
11 would have if Defendants would had adequately protected the confidentiality of their medical and
12 personal identifying information.

13 132. Pursuant to the Business & Professions Code § 17203, Plaintiff, the SubClass and the
14 Class seek an order of this Court requiring Defendants awarding Plaintiff and the Class restitution
15 of monies wrongfully acquired by Defendants in the form of payments for services by means of
16 such unlawful, fraudulent and unfair business acts and practices, so as to restore any and all monies
17 to Plaintiff, the SubClass and the Class which were acquired and obtained by means of such
18 unlawful, fraudulent and unfair business acts and practices, which ill-gotten gains are still retained
19 by Defendants.

20 133. The aforementioned unlawful, fraudulent and unfair business acts or practices
21 conducted by Defendants have been committed in the past and continues to this day. Defendants
22 have failed to acknowledge the wrongful nature of their actions. Defendants have not corrected or
23 publicly issued comprehensive corrective notices to Plaintiff, the SubClass and the Class, and have
24 not corrected or enacted adequate privacy policies and procedures to protect and preserve
25 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
26 Class in their possession.

27
28

1 134. Because of Defendants' aforementioned conduct, Plaintiff, the SubClass and the
2 Class have no other adequate remedy of law in that absent injunctive relief from the Court and
3 Defendants are likely to continue to injure Plaintiff, the SubClass and the Class.

4 135. Pursuant to Business & Professions Code § 17203, Plaintiff, the SubClass and the
5 Class also seek an order of this Court for equitable and/or injunctive relief in the form of requiring
6 Defendants to correct its illegal conduct that is necessary and proper to prevent Defendants from
7 repeating their illegal and wrongful practices as alleged above and protect and preserve
8 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
9 Class in Defendants' possession that has already been accessed, viewed, exfiltrated and/or publicly
10 exposed by at least one unauthorized third party because by way of Defendants' illegal and
11 wrongful practices set forth above. Pursuant to Business & Professions Code § 17203, Plaintiff, the
12 SubClass and the Class further seek an order of this Court for equitable and/or injunctive relief in
13 the form of requiring Defendants to publicly issue comprehensive corrective notices.

14 136. Because this case is brought for the purposes of enforcing important rights affecting
15 the public interest, Plaintiff, the SubClass and the Class also seek the recovery of attorneys' fees
16 and costs in prosecuting this action against Defendants under Code of Civil Procedure § 1021.5 and
17 other applicable law.

18 **PRAYER FOR RELIEF**

19 WHEREFORE, Plaintiff respectfully request that the Court grant Plaintiff and the proposed
20 SubClass and Class the following relief against Defendants, and each of them:

21 **As for the First, Second and Third Causes of Action**

- 22 1. For nominal damages in the amount of one thousand dollar (\$1,000) per violation to Plaintiff
23 individually and to each member of the SubClass and the Class pursuant to Civil Code §
24 56.36(b)(1);
25 2. For actual damages according to proof per violation pursuant to Civil Code § 56.36(b)(2);

26 **As for the Fourth Cause of Action**

- 27 3. For damages according to proof to Plaintiff individually and to each member of the Class
28 pursuant to California Civil Code § Civil Code § 1798.84(b);

1 4. For injunctive relief pursuant to California Civil Code § Civil Code § 1798.84(e);

2 **As for the Fifth Cause of Action**

3 5. For an order awarding Plaintiff, the SubClass and the Class restitution of all monies
4 wrongfully acquired by Defendants by means of such unlawful, fraudulent and unfair
5 business acts and practices;

6 6. For injunctive relief in the form of an order instructing Defendants to prohibit the
7 unauthorized release of medical and personal identifying information of Plaintiff, the
8 SubClass and the Class, and to adequately maintain the confidentiality of the medical and
9 personal identifying information of Plaintiff and the Class;

10 7. For injunctive relief in the form of an order enjoining Defendants from disclosing the
11 medical and personal identifying information of Plaintiff, the SubClass and the Class
12 without the prior written authorization of each Plaintiff, the SubClass and the Class member;

13 **As to All Causes of Action**

14 8. That the Court issue an Order certifying this action be certified as a class action on behalf of
15 the proposed SubClass and Class, appointing Plaintiff as representative of the proposed
16 SubClass and Class, and appointing Plaintiff's attorneys, as counsel for members of the
17 proposed SubClass and Class;

18 9. For an award of attorneys' fees as authorized by statute, including, but not limited to, the
19 provisions of California Code of Civil Procedure § 1021.5, and as authorized under the
20 "common fund" doctrine, and as authorized by the "substantial benefit" doctrine;

21 10. For costs of the suit;

22 11. For prejudgment interest at the legal rate; and

23 12. Any such further relief as this Court deems necessary, just, and proper.

24 Dated: June 1, 2021

KEEGAN & BAKER LLP

25 By: 
26 Patrick N. Keegan, Esq.
27 Attorney for Plaintiff
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

Plaintiff, the SubClass and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

Dated: June 1, 2021

KEEGAN & BAKER LLP

By: 
Patrick N. Keegan, Esq.
Attorney for Plaintiff

Exhibit A



HEALTH CENTER PARTNERS
of Southern California

C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE



NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

SEQ
CODE 2D
Ver 1

BREAK

To Enroll, Please Call:
1-833-416-0926
Or Visit:
<https://response.idx.us/hcp-netgain-incident>
Enrollment Code: <<XXXXXXXXXX>>

April 12, 2021

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by Netgain Technology, LLC (“Netgain”), the IT service provider for Health Center Partners of Southern California (“HCP”). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTHCENTER>>. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, we engaged our own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, our health center members and partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain’s cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

Once we learned that HCP data may have been involved in the incident, we worked with our cybersecurity experts to review the impacted files and identify the individuals whose information was contained in such files so that we may notify such individuals. Our investigation revealed that the impacted files contained your personal information. **Again, we are not aware of any misuse of your personal information as a result of this incident.** Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your information.

What Information Was Involved: The information involved varies depending on the individual but may include the following: <<VARPARAGRAPH>>.

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, we have reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and we are committed to assisting their investigation into the matter.

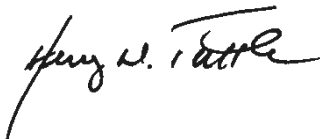
We are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include **xx** months of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What You Can Do: As we have stated, we are not aware of any misuse of your information as a result of this incident. However, we encourage you to follow the recommendations on the next page to help protect your information. We also encourage you to enroll in the complimentary services offered by going to <https://response.idx.us/hcp-netgain-incident> or calling 1-833-416-0926 and using the enrollment code provided above. Please note that the deadline to enroll is July 12, 2021.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-833-416-0926 between 6:00 a.m. and 6:00 p.m. Pacific Time.

The security of your information is a top priority for HCP, and we are committed to safeguarding your data and privacy.

Sincerely,

A handwritten signature in black ink, appearing to read "Henry W. Tuttle". The signature is written in a cursive style with a large, sweeping initial "H".

Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
www.consumer.ftc.gov ,	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
and	1-888-743-0023	1-877-566-7226	1-401-274-4400
www.ftc.gov/idtheft			
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Exhibit B



To Enroll, Please Call:
(833) 903-3642
Or Visit:
<https://response.idx.us/nhc-netgain-incident>
Enrollment Code: <<ENROLLMENT>>

C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

April 8, 2021

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

The privacy and security of your personal information is very important to Neighborhood Healthcare. We are writing to make you aware of an issue brought to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud hosting and managed services provider. Neighborhood Healthcare used Netgain to host some Neighborhood Healthcare files.

What Happened

On November 24, 2020, Netgain became aware of a security incident that involved unauthorized access to portions of the Netgain environment and Netgain client environments and began taking steps to investigate this incident. But, on December 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain took additional measures to contain the threat and address the issue. Netgain’s technical teams worked closely with third-party experts to remove the threat in the impacted environments and confirm that client and internal systems are protected.

Neighborhood Healthcare learned of the ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to believe that the protected health information (“PHI”) of our patients had been impacted in the incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some information including, potentially, some files containing patient PHI may have been impacted in the incident. Netgain could not confirm, at that time, what records may have been impacted in the incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood Healthcare that Netgain believed were impacted by the attackers. Those files came from a Neighborhood Healthcare server accessible by the Netgain environment. Since that time, Neighborhood Healthcare has worked to review those records, to identify individuals impacted, conduct an investigation into the incident with the assistance outside experts, and to transmit this letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood Healthcare determined that the impacted files included some of your information.

What Information Was Involved

The information involved may have included some of the following: your name, date of birth, address, Social Security Number and information about the care that you received from Neighborhood Healthcare such as insurance coverage information, physician you saw, and treatment codes. Neighborhood Healthcare is offering credit monitoring services to you at no charge. Please see the **What You Can Do** section below for information about these services including how to enroll. Please also see the **Additional Important Information** section below for further precautionary measures you may wish to take. Netgain has received assurances that the data has not gone beyond the attacker, that the data was not and will not be misused, and that the data will not be disseminated or otherwise be made publicly available.

What We Are Doing

Please know that we take this incident and the security of your personal information very seriously. Ensuring the safety of our patients' data is of the utmost importance to us. Since we learned of this incident, we have been working with Netgain to seek assurances that they are taking appropriate steps to respond to this incident. We have also conducted an investigation of the incident with the help of outside experts, and we have transitioned to a new hosting provider (a transition that was already in process when this incident occurred).

In addition, we are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include <<12/24 months>> of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What Netgain Is Doing

Netgain took several steps to strengthen its environment following the incident, including international Geo-fencing for Azure-hosted environments, deploying additional log monitoring across all servers, and additional hardening of network security rules and protocols to restrict lateral movement across environments. Netgain stated that it paid a significant amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

What You Can Do

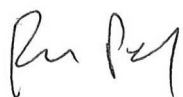
We recommend that you review the additional information enclosed. Additionally, we encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 903-3642 or going to <https://response.idx.us/nhc-netgain-incident> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 8, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

We very much regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, please call (833) 903-3642, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely



Rakesh Patel
CEO
Neighborhood Healthcare

Additional Important Information

1. Website and Enrollment. Go to <https://response.idx.us/nhc-netgain-incident> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 903-3642 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Generally. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing financial account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state's Attorney General.

5. The FTC. You can obtain information from Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

6. Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

7. Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788 equifax.com/personal/credit-report-services/ 800-525-6285	Experian Security Freeze P.O. Box 9554 Allen, TX 75013-9544 experian.com/freeze/center.html 888-397-3742	TransUnion (FVAD) P.O. Box 160 Woodlyn, PA 19094 transunion.com/credit-freeze 888-909-8872
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

More information can also be obtained by contacting the Federal Trade Commission listed above.

8. Protecting Medical Information: To date, we have no reason to believe that your PHI potentially involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following steps can help protect you from medical identity theft issues.

- Do not share health insurance cards with anyone apart from your care providers and other family members who are covered under the insurance plan or who help you with your medical care.
- Review the “explanation of benefits statements” that you receive from your health insurance company. If you see something amiss, follow up with your insurance company or the health care provider identified on the explanation of benefits to request further information.
- Ask your health insurance company for a report on all services they have paid for you for the current year. If you do not recognize an item in that list, speak with your insurance company to verify it.

9. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Tel: (760) 929-9303
4 Fax: (760) 929-9260

ELECTRONICALLY RECEIVED
Superior Court of California,
County of San Diego
06/02/2021 at 02:51:43 PM
Clerk of the Superior Court
By Kristin Sorianosos, Deputy Clerk

5 Attorney for Plaintiff
6 JANE DOE
7

8 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
9 **FOR THE COUNTY OF SAN DIEGO**

10 JANE DOE, individually and on behalf of all others
11 similarly situated,

12 Plaintiff,

13 vs.

14 NEIGHBORHOOD HEALTHCARE; HEALTH
CENTERS PARTNERS OF SOUTHERN
15 CALIFORNIA; NETGAIN TECHNOLOGY, LLC;
and DOE DEFENDANTS 1-100;

16 Defendants.
17

Case No. 37-2021-00023936-CU-BT-CTL

CLASS ACTION

Assigned to: Hon. Joel R. Wohlfeil, Dept. C-73

**[PROPOSED] ORDER GRANTING
PLAINTIFF'S EX PARTE APPLICATION TO
APPEAR BY PSEUDONYM**

Date: June 8, 2021

Time: 8:30 a.m.

Place: Department C-73

IMAGED FILE

18 Plaintiff Jane Doe's application for an order allowing Plaintiff to appear by pseudonym in this matter,
19 came *ex parte* for hearing on June 8, 2021, at 8:30 a.m. in Department C-73 before the Honorable Joel R.
20 Wohlfeil, and the Court, having reviewed Plaintiff Jane Doe's application and for good cause appearing
21 therefore, hereby orders as follows:

22 **IT IS HEREBY ORDERED THAT:**

23 Plaintiff Jane Doe alleges she was a patient within the meaning of Civil Code § 56.05(k). As such,
24 she is authorized by Civil Code § 3427.3 to use a pseudonym in this action to protect her privacy.
25

26 Dated: _____

27 _____
Hon. Joel R. Wohlfeil
Judge of the Superior Court
28

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar number, and address): Patrick Keegan, 167698 Keegan & Baker, LLP 2292 Faraday Avenue, Suite 100 Carlsbad, CA 92008 TELEPHONE NO.: (760)929-9303 Ext 100 ATTORNEY FOR (Name): Plaintiff	FOR COURT USE ONLY ELECTRONICALLY FILED Superior Court of California, County of San Diego 06/16/2021 at 11:34:00 AM Clerk of the Superior Court By E- Filing, Deputy Clerk
SUPERIOR COURT OF CALIFORNIA, COUNTY OF Superior Court of California, San Diego County 330 W. Broadway San Diego, CA 92101-3409	CASE NUMBER: 37-2021-00023936-CU-BT-CTL
PLAINTIFF/PETITIONER: JANE DOE, et al DEFENDANT/RESPONDENT: Neighborhood Healthcare. et al	Ref. No. or File No.: 5187-Netgain
PROOF OF SERVICE OF SUMMONS	

BY FAX

1. At the time of service I was a citizen of the United States, at least 18 years of age and not a party to this action.
2. I served copies of: Summons, Civil Case Cover Sheet, Class Action Complaint, Notice of Case Assignment and Case Management Conference, Alternative Dispute Resolution (ADR) Information, Stipulation to Use Alternative Dispute Resolution (ADR), Plaintiff's Ex Parte Application for an Order for Plaintiff to Appear by Pseudonym, Minute Order, Order Granting Plaintiff's Ex Parte Application to Appear by Pseudonym,
3. a. Party served: Neighborhood Healthcare

 b. Person Served: Sallie Barnett - Person Authorized to Accept Service of Process
4. Address where the party was served: 150 La Terraza Blvd, Ste. 201
 Escondido, CA 92025
5. I served the party
 b. **by substituted service.** On (date): 06/11/2021 at (time): 2:07PM I left the documents listed in item 2 with or in the presence of: Michelle Olmeda - Person In Charge Of Office
 (1) (business) a person at least 18 years of age apparently in charge at the office or usual place of business of the person to be served. I informed him or her of the general nature of the papers.
 (4) A declaration of mailing is attached.
6. The "Notice to the Person Served" (on the summons) was completed as follows:
 d. on behalf of:
 Neighborhood Healthcare

 under: CCP 416.10 (corporation)
7. **Person who served papers**
 a. Name: Tom Reinhardt
 b. Address: One Legal - P-000618-Sonoma
 1400 North McDowell Blvd, Ste 300
 Petaluma, CA 94954
 c. Telephone number: 415-491-0606
 d. The fee for service was: \$ 197.50
 e. I am:
 (3) registered California process server.
 (i) Employee or independent contractor.
 (ii) Registration No. P121764
 (iii) County San Diego
8. I declare under penalty of perjury under the laws of the United States of America and the State of California that the foregoing is true and correct.

Date: 06/15/2021

Tom Reinhardt

(NAME OF PERSON WHO SERVED PAPERS)



(SIGNATURE)

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name and Address): Patrick Keegan, 167698 Keegan & Baker, LLP 2292 Faraday Avenue, Suite 100 Carlsbad, CA 92008		TELEPHONE NO.: (760)929-9303 Ext 100	FOR COURT USE ONLY
ATTORNEY FOR (Name): Plaintiff		Ref. No. or File No. 5187-Netgain	
Insert name of court, judicial district or branch court, if any: Central - Civil 330 W. Broadway San Diego, CA 92101-3409			
PLAINTIFF: JANE DOE, et al			
DEFENDANT: Neighborhood Healthcare, et al			
PROOF OF SERVICE BY MAIL			CASE NUMBER: 37-2021-00023936-CU-BT-CTL

BY FAX

I am a citizen of the United States, over the age of 18 and not a party to the within action. My business address is 1400 N. McDowell Blvd, Petaluma, CA 94954.

On 06/16/2021, after substituted service under section CCP 415.20(a) or 415.20(b) or FRCP 4(e)(2)(B) or FRCP 4(h)(1)(B) was made (if applicable), I mailed copies of the:

Summons, Civil Case Cover Sheet, Class Action Complaint, Notice of Case Assignment and Case Management Conference, Alternative Dispute Resolution (ADR) Information, Stipulation to Use Alternative Dispute Resolution (ADR), Plaintiff's Ex Parte Application for an Order for Plaintiff to Appear by Pseudonym, Minute Order, Order Granting Plaintiff's Ex Parte Application to Appear by Pseudonym,

to the person to be served at the place where the copies were left by placing a true copy thereof enclosed in a sealed envelope, with First Class postage thereon fully prepaid, in the United States Mail at Petaluma, California, addressed as follows:

Neighborhood Healthcare

Sallie Barnett

150 La Terraza Blvd, Ste. 201

Escondido, CA 92025

I am readily familiar with the firm's practice for collection and processing of documents for mailing. Under that practice, it would be deposited within the United States Postal Service, on that same day, with postage thereon fully prepaid, in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one (1) day after date of deposit for mailing in affidavit.

Fee for Service: \$ 197.50

I declare under penalty of perjury under the laws of the United States of America and the State of California that the foregoing is true and correct and that this declaration was executed on 06/16/2021 at Petaluma, California.

One Legal - P-000618-Sonoma
 1400 North McDowell Blvd, Ste 300
 Petaluma, CA 94954



Travis Carpenter

OL# 16442441

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego
08/16/2021 at 04:57:00 PM
Clerk of the Superior Court
By Richard Day, Deputy Clerk

1 **BRYAN CAVE LLP**
2 DANIEL T. ROCKEY (SBN 178604)
3 Three Embarcadero Center, 7th Floor
4 San Francisco, CA 94111
5 Email: daniel.rockey@BCLPLaw.com
6 Telephone: (415) 675-3400
7 Facsimile: (415) 675-3434
8 Attorneys for Defendant
9 NEIGHBORHOOD HEALTHCARE

10 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
11 **COUNTY OF SAN DIEGO**

12 JANE DOE, individually and on behalf of all
13 others similarly situated,

14 Plaintiff,

15 vs.

16 NEIGHBORHOOD HEALTHCARE; HEALTH
17 CENTER PARTNERS OF SOUTHERN
18 CALIFORNIA; NETGAIN TECHNOLOGY,
19 LLC; and DOE DEFENDANTS 1-100,

20 Defendants.

Case No. 37-2021-00023936-CU-BT-CTL

**STIPULATION EXTENDING TIME
TO RESPOND TO INITIAL
COMPLAINT; [~~PROPOSED~~]
ORDER**

Complaint Filed: June 8, 2021
Trial Date: None Set

21 Plaintiff Jane Doe (“Plaintiff”) and Defendant Neighborhood Healthcare (“Defendant”)
22 (collectively “the Parties”), by and through their counsel of record, hereby stipulate and agree as
23 follows:

24 WHEREAS, Plaintiff filed her Complaint in this action on June 8, 2021 naming three
25 defendants: Neighborhood Healthcare (“Neighborhood”), Health Center Partners of Southern
26 California (“HCP”), and Netgain Technology, LLC (“Netgain”) in connection with a ransomware
27 attack occurring in December 2020.

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

WHEREAS, on July 20, 2021, counsel for Plaintiff and counsel for defendant Neighborhood Healthcare (“Neighborhood”) met and conferred regarding Neighborhood’s intent to demur to the Complaint and certain other related issues. At that meet and confer, Neighborhood indicated that it would consider voluntarily producing to Plaintiff certain documents relevant to Plaintiff’s allegations in the interest of facilitating an amendment to the Complaint. At that time, Plaintiff agreed to a 15 day extension of the time for Neighborhood to respond to the complaint and proposed that once Plaintiff had effected service on the remaining defendants, the parties should agree upon a further extension of time to align the dates for all defendants to respond to the complaint. Neighborhood agreed to this proposal.

WHEREAS, on August 11, 2021, Neighborhood voluntarily produced to Plaintiff’s counsel certain agreements relevant to the allegations of the Complaint and inquired whether Plaintiff had effected service on the remaining defendants.

WHEREAS, Plaintiff’s counsel responded the next day, confirming receipt of the documents and indicating that based upon thereon, he intended to file an amended complaint, and additionally indicated that he had received an Acknowledgment of Receipt of Service of Summons and Complaint from HCP, dated August 9, 2021, and proposed that the parties enter into a stipulation seeking court approval to extend the deadline for Neighborhood to respond to the Complaint up to and including September 8, 2021, corresponding to the date for HCP’s response to the Complaint.

WHEREAS, Neighborhood accepted Plaintiff’s counsel’s proposal.

WHEREAS, a further extension of time for Defendant to respond to the Complaint will allow for coordination of responses to the Complaint, will allow time for Plaintiff to file an amended complaint, and will allow additional time for the Parties to discuss potential resolution.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

WHEREAS, the proposed stipulation will not alter the date of any event or any deadline already fixed by Court order.

WHEREAS, the parties have not previously sought any extensions of time from the Court, NOW, THEREFORE, the Parties hereby agree and stipulation that Defendants' response deadline to the Complaint should be continued to September 8, 2021.

IT IS THEREFORE STIPULATED AND AGREED THAT:


1. Neighborhood's deadline to respond to the Complaint shall be extended to September 8, 2021.

2. The Parties further agree that if Plaintiff files an amended complaint, Defendant's deadline to respond shall be extended accordingly.

IT IS SO STIPULATED.

Dated: August 16, 2021

Patrick N. Keegan
KEEGAN & BAKER, LLP

By: 
Patrick N. Keegan

Attorneys for Plaintiff
Jane Doe

Dated: August 16, 2021

Daniel T. Rockey
BRYAN CAVE LEIGHTON PAISNER LLP

By: _____
Daniel T. Rockey

Attorneys for Defendant
Neighborhood Healthcare

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

~~PROPOSED~~ ORDER

Pursuant to the foregoing Stipulation of the parties, and good cause appearing therefor, IT IS SO ORDERED that Defendant Neighborhood Healthcare shall have until September 8, 2021 to respond to Plaintiff's initial complaint.



Dated: 8/17/21

Judge Joel R. Wohlfeil

Judge of the Superior Court of California
County of San Diego

BRYAN CAVE LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

PROOF OF SERVICE

I am employed in the aforesaid County, State of California; I am over the age of eighteen years and not a party to the within entitled action; my business address is: Three Embarcadero Center, 7th Floor, San Francisco, CA 94111.

On August 16, 2021, I caused to be served on the interested parties in said action the within:

**STIPULATION EXTENDING TIME TO RESPOND TO INITIAL COMPLAINT;
[PROPOSED] ORDER**

Patrick Keegan
Keegan & Baker
2292 Faraday Avenue, Suite 100
Carlsbad, CA 92008
Tel: (760)929-9303 ext 100

BY U.S. MAIL -- I am “readily familiar” with the firm’s practice of collection and processing correspondence for mailing. Under that practice it would be deposited with U.S. Postal Service on that same day with postage thereon fully prepaid at San Francisco, California in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit.

BY E-MAIL – I caused a true copy of the foregoing document(s) to be served by electronic email transmission at the time shown on each transmission, to each interested party at the email address shown above. Each transmission was reported as complete and without error.

BY OVERNIGHT DELIVERY -- Depositing the above document(s) in a box or other facility regularly maintained by FedEx in an envelope or package designated by FedEx with delivery fees paid or provided for.

(BY File & Serve XPress) -- I caused a true copy of the foregoing documents to be served by File & Serve XPress to each interested party at the email address shown above. Each transmission was reported as complete and without error.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed on August 16, 2021, at San Francisco, California.



Bridgette Warren

BRYAN CAVE LEIGHTON PAISNER LLP
THREE EMBARCADERO CENTER, 7TH FLOOR
SAN FRANCISCO, CA 94111-4070

**SUPERIOR COURT OF CALIFORNIA,
COUNTY OF SAN DIEGO
CENTRAL**

MINUTE ORDER

DATE: 06/08/2021

TIME: 08:30:00 AM

DEPT: C-73

JUDICIAL OFFICER PRESIDING: Joel R. Wohlfeil

CLERK: Jessica Pascual, Andrea Taylor

REPORTER/ERM: Not Requested

BAILIFF/COURT ATTENDANT:

CASE NO: **37-2021-00023936-CU-BT-CTL** CASE INIT.DATE: 06/01/2021

CASE TITLE: **Doe vs Neighborhood Healthcare [EFILE]**

CASE CATEGORY: Civil - Unlimited CASE TYPE: Business Tort

EVENT TYPE: Ex Parte

APPEARANCES

PATRICK N KEEGAN, counsel, present for Plaintiff(s) telephonically.

Counsel is before the court on Plaintiff's ex parte application for an order for Plaintiff to Appear by Pseudonym.

The Court, having read the moving papers, and having heard comments from counsel, grants the Ex Parte.

The Court signs the proposed order as modified.

Joel R. Wohlfeil

Judge Joel R. Wohlfeil

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Tel: (760) 929-9303
4 Fax: (760) 929-9260

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego
06/02/2021 at 02:51:00 PM
Clerk of the Superior Court
By Kristin Sorianosos, Deputy Clerk

5 Attorney for Plaintiff
6 JANE DOE

7 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
8 **FOR THE COUNTY OF SAN DIEGO**

9 JANE DOE, individually and on behalf of all others
similarly situated,

10 Plaintiff,

11 vs.

12 NEIGHBORHOOD HEALTHCARE; HEALTH
13 CENTERS PARTNERS OF SOUTHERN
CALIFORNIA; NETGAIN TECHNOLOGY, LLC;
14 and DOE DEFENDANTS 1-100;

15 Defendants.

Case No. 37-2021-00023936-CU-BT-CTL

CLASS ACTION

Assigned to: Hon. Joel R. Wohlfeil, Dept. C-73

**PLAINTIFF’S EX PARTE APPLICATION
FOR AN ORDER FOR PLAINTIFF TO
APPEAR BY PSEUDONYM; MEMORANDUM
OF POINTS AND AUTHORITIES;
DECLARATION OF PATRICK N. KEEGAN**

Date: June 8, 2021

Time: 8:30 a.m.

Place: Department C-73

16 IMAGED FILE

17 PLEASE TAKE NOTICE that pursuant to California Rules of Court, Rules 3.1200, *et seq.* and the
18 Court’s June 2, 2021 telephonic request, that on June 8, 2021, at 8:30 a.m. in the courtroom of Honorable
19 Joel R. Wohlfeil, in Department C-73 of the San Diego Superior Court, 330 West Broadway, San Diego,
20 California 92101, counsel for Plaintiff Jane Doe will appear *ex parte* (via CourtCall or Microsoft Teams)
21 for an Order allowing Plaintiff to appear by pseudonym in this matter, pursuant to Cal. Civ. Code § 3427.3
22 (West 2011).

23 This *ex parte* application is based upon section 3427.3 and good cause shown, and is supported by
24 the memorandum of points and authorities, the declaration of Patrick N. Keegan, the files and records in this
25 action, and such oral argument as the Court may consider in deciding this application.

26 Dated: June 2, 2021

KEEGAN & BAKER, LLP

s/ Patrick N. Keegan

Patrick N. Keegan, Esq.

Attorney for Plaintiff JANE DOE

1 **MEMORANDUM OF POINTS AND AUTHORITIES**

2 Plaintiff Jane Doe (or “Plaintiff”), individually and on behalf of others similarly situated, respectfully
3 submits this memorandum of points and authorities in support of her *ex parte* application for an order
4 allowing her to proceed by pseudonym in place of the real name of Plaintiff, pursuant to Cal. Civ. Code §
5 3427.3 (West 2011) (specifically allowing health care patients to bring a lawsuit using a pseudonym)
6 because at all times relevant to this action, Plaintiff is a health care patient under Civil Code § 56.05(k) and
7 has individual privacy concerns and a reasonable fear of harassment in light of the nature of the case.

8 **I. INTRODUCTION**

9 As alleged in Plaintiff’s Class Action Complaint for Damages, Restitution, and Injunctive Relief for
10 Violations of: (1) the Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*; (2) Breach of
11 California Security Notification Laws, California Civil Code § 1798.82; and (3) Business and Professions
12 Code §§ 17200, *et seq.*, filed on June 1, 2021 (“Complaint”), this class action arises from Defendants’
13 negligent failure to properly create, maintain, preserve, and/or store confidential, medical and person
14 identifying information that allowed an unauthorized person to gain access to a computer database server
15 of Defendants from October 22, 2020 to December 3, 2020, causing the disclosure and/or release of
16 unencrypted medical and personal information of Plaintiff and other persons similarly situated, to an
17 unauthorized person resulting in violations of the Confidentiality of Medical Information Act, Civil Code
18 §§ 56, *et seq.* (See, e.g., Complaint, at ¶1).

19 California statutory law specifically allows a party to bring a lawsuit using a pseudonym in cases
20 involving health care patients. Cal. Civ. Code § 3427.3 (West 2011). The Complaint at page 1, in footnote
21 1, cites and sets forth section 3427.3 in its entirety, and then further alleges, “Here, a pseudonym has been
22 used in place of the real name of Plaintiff because at all times relevant to this action, Plaintiff is a health care
23 patient under Civil Code § 56.05(k) and has individual privacy concerns and a reasonable fear of harassment
24 in light of the nature of the case.” (Complaint, at ¶1 n.1). The Complaint further alleges that the Notice of
25 Data Breach letter that Plaintiff received states that “in late September 2020, an unauthorized third party
26 gained access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the
27 unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an
28 undisclosed amount to the attacker.... The [Plaintiff’s] information involved ... may include the following:

1 name, address, date of birth, diagnosis/treatment information and treatment cost information.” (Complaint,
 2 at ¶2). Additionally, the Complaint also alleges that Plaintiff “fears that disclosure and/or release of her
 3 medical information created, maintained, preserved, and/or stored on Defendants’ computer networks could
 4 subject her to harassment or abuse.” (Complaint, at ¶¶10 and 69).

5 Further, Plaintiff is *not* proceeding *anonymous* in this action. Prior to filing the Complaint, Plaintiff
 6 sent separate letters to Defendant Neighborhood Healthcare (“NH”) and Defendant Health Center Partners
 7 of Southern California (“HCP”) disclosing the true name of Plaintiff Jane Doe and requesting further
 8 information about this security incident. (Complaint, at ¶69; and Keegan Decl., ¶3). Therefore, the
 9 Defendants are not prejudice by Plaintiff proceeding pseudonymously in this action.

10 As demonstrated below, section 3427.3 specifically allows a party to bring a lawsuit using a
 11 pseudonym in cases involving health care patients. Even before the enactment of section 3427.3, California
 12 courts have allowed plaintiffs to proceed pseudonymously in countless published state court decisions. Even
 13 before the enactment of section 3427.3, California courts have also held that the California Code of Civil
 14 Procedure does not prohibit pseudonymous litigation. Accordingly, good cause exists for the granting of
 15 Plaintiff’s *ex parte* application.

16 **II. ARGUMENT**

17 California statutory law specifically allows a party to bring a lawsuit using a pseudonym in cases
 18 involving health care patients. Cal. Civ. Code § 3427.3 (West 2011). Specifically, section 3427.3 provides,

19 The court having jurisdiction over a civil proceeding under this title ***shall take all steps***
 20 ***reasonably necessary to safeguard the individual privacy*** and prevent harassment ***of a***
 21 ***health care patient***, licensed health practitioner, or employee, client, or customer of a health
 22 ***care facility who is a party or witness in the proceeding, including granting protective orders.***
Health care patients, licensed health practitioners, and employees, clients, and customers
 of the health care facility ***may use pseudonyms to protect their privacy.***

23 Cal. Civ. Code § 3427.3 (emphasis added). Here, the Complaint alleges that at all times relevant to this
 24 action, Plaintiff is and was a health care patient.¹ (Complaint, at ¶1 n.1). The Complaint further alleges that
 25 the Notice of Data Breach letter that Plaintiff received states that “in late September 2020, an unauthorized
 26 third party gained access to Netgain’s digital environment, and between October 22, 2020 to December 3,

27
 28 ¹ As alleged in the Complaint, Plaintiff is a “natural person ... who received health care services from
 a provider of health care” within the meaning of Civil Code § 56.05(k). Complaint, at ¶10.

2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker.... The [Plaintiff's] information involved ... may include the following: name, address, date of birth, diagnosis/treatment information and treatment cost information.” (Complaint, at ¶2). Additionally, Plaintiff also alleges in the Complaint that she “fears that disclosure and/or release of her medical information created, maintained, preserved, and/or stored on Defendants’ computer networks could subject her to harassment or abuse.” (Complaint, at ¶¶10 and 69). Thus, under section 3427.3, Plaintiff may proceed in this case using the pseudonym “Jane Doe” in conformity with the laws of the State of California.

Further, Plaintiff, as a health care patient, may use a pseudonym in the Complaint and in this litigation to protect her privacy under section 3427.3, and there is no additional requirement under section 3427.3 that Plaintiff must also *show* a risk of “harassment, injury, ridicule, or embarrassment” in order to proceed pseudonymously.

Moreover, Plaintiff is *not* proceeding *anonymous* in this action. (Keegan Decl., ¶3). Defendants Neighborhood Healthcare (“NH”) and Defendant Health Center Partners of Southern California (“HCP”) have known all along the true identity of Plaintiff, as pre-filing communications between the parties identify Plaintiff’s true identity. (Complaint, at ¶69; and Keegan Decl., ¶3). Therefore, the Defendants are not prejudice by Plaintiff proceeding pseudonymously in this action. Moreover, what Plaintiff seeks to avoid by proceeding pseudonymously in this action is additional harassment or abuse, i.e. in addition to the harassment or abuse suffered and caused by the disclosure and/or release of her medical information created, maintained, preserved, and/or stored on Defendants’ computer networks, that she fears she could be subjected to if her name is disclosed in public facing documents filed with this Court in this action. Clearly, the Legislature recognized this “need to safeguard the individual privacy and prevent harassment of a health care patient” when enacting Civil Code § 3427.3.

1. Prior to the Enactment of Civil Code § 3427.3, California Courts Have Allowed Plaintiffs to Proceed Pseudonymously in Countless Published State Court Decisions

Even before the enactment of section 3427.3, California courts have allowed plaintiffs to proceed pseudonymously in countless published state court decisions. For example, *prior to the enactment of section 3427.3*, California courts have allowed plaintiffs to proceed with pseudonyms in a variety of cases *not*

1 *involving health care patients*. For example, *prior to the enactment of section 3427.3*, in *Doe v. Saenz*
2 (2006) 140 Cal.App.4th 960, 977–979, three convicted felons were permitted to pursue legal actions under
3 fictitious names challenging a decision by the Department of Social Services to classify their offenses as
4 nonexemptible, thereby precluding them from working in licensed community care facilities. In *Hooper v.*
5 *Deukmejian* (1981) 122 Cal.App.3d 987, 993, an individual convicted on a plea of maintaining a place for
6 selling or using marijuana was permitted to sue under a fictitious name *on behalf of himself and all others*
7 *similarly situated* (in a class action) to determine whether they were entitled to the benefits and protections
8 of marijuana reform legislation. In *Doe v. Superior Court (Luster)* (2011) 194 Cal.App.4th 750, the Court
9 of Appeal held that in an action brought under a fictitious name, it was appropriate for plaintiff to verify her
10 discovery responses using the fictitious name: “Any other rule would render the ability to use a fictitious
11 name in the litigation meaningless.” *Id.*, at 754. In *Starbucks Corp. v. Superior Court* (2008) 168
12 Cal.App.4th 1436, the Court of Appeal noted that the use of “Doe plaintiffs” to protect legitimate privacy
13 rights “The judicial use of ‘Doe plaintiffs’ to protect legitimate privacy rights has gained wide currency,
14 particularly given the rapidity and ubiquity of disclosures over the World Wide Web.” *Id.*, at 1452.

15 Additionally, *prior to the enactment of section 3427.3*, California courts have allowed plaintiffs to
16 proceed with a pseudonym in a variety of cases *involving health care patients*. *Jane Doe 8015 v. Superior*
17 *Court* (2007) 148 Cal.App.4th 489, 491-492, a patient was allowed to bring an action against a laboratory
18 using a pseudonym after it was determined that one of the laboratory’s phlebotomists had reused needles,
19 resulting in the plaintiff’s contraction of HIV.

20 California courts have also recognized that the U.S. Supreme Court has also implicitly endorsed the
21 use of pseudonyms to protect a health care patient’s privacy. *See, e.g., Doe v. Lincoln Unified School Dist.*,
22 188 Cal.App.4th at 766-767 (citing *Roe v. Wade* (1973) 410 U.S. 113, 93 S.Ct. 705, 35 L.Ed.2d 147
23 [abortion]; *Doe v. Bolton* (1973) 410 U.S. 179, 93 S.Ct. 739, 35 L.Ed.2d 201 [abortion]; and *Poe v. Ullman*
24 (1961) 367 U.S. 497, 81 S.Ct. 1752, 6 L.Ed.2d 989 [birth control].)

25 **2. Prior to the Enactment of Civil Code § 3427.3, California Courts Have Long Held That**
26 **the California Code of Civil Procedure Does Not Prohibit Pseudonymous Litigation**

27 California courts have also held that the California Code of Civil Procedure does not prohibit
28 pseudonymous litigation. *See, Doe v. Lincoln Unified School Dist.* (2010) 188 Cal.App.4th 758, 765-767;

1 and *Doe v. Superior Court (Luster)* (2011) 194 Cal.App.4th 750, 754 (holding that in an action brought
2 under a fictitious name, it was appropriate for plaintiff to verify her discovery responses using the fictitious
3 name). In *Doe v. Lincoln Unified School Dist.*, a teacher who had been placed on sick leave, sued under a
4 fictitious name to protect her privacy. She used “Jane Doe” as the plaintiff’s name on her complaint to
5 protect her privacy. *Id.*, at 762. The school district defendant argued on appeal that the teacher had no
6 standing to sue because Jane Doe was not the real party in interest and that a party must sue in his or her own
7 real name because of Code of Civil Procedure § 367. *Id.*, at 765. The *Doe v. Lincoln Unified School Dist.*
8 court rejected defendant’s argument, and held that Code of Civil Procedure § 367 does not require that a
9 party sue in his or her own name, citing “countless published state court decisions where one or more of the
10 parties have used fictitious names.” *Id.*, at 766. Code of Civil Procedure § 367 states that, “Every action
11 must be prosecuted in the name of the real party in interest, except as otherwise provided by statute.” Cal.
12 Code Civ. Pro. § 367. Specifically, the *Doe v. Lincoln Unified School Dist.* court held Code of Civil
13 Procedure § 367 to mean that a lawsuit must be brought on behalf of a person having legal standing to
14 commence the action, and “[t]he question for purposes of standing is not the name used by the party suing
15 but whether the party suing is the party possessing the right sued upon.” *Id.*, at 765-767 (holding using a
16 fictitious name does not deprive a plaintiff of standing or preclude it from being the real party in interest).

17 Furthermore, *Doe v. Superior Court (Luster)* (2011) 194 Cal.App.4th 750 is instructive. The *Doe*
18 *v. Superior Court (Luster)* court rejected the defendant’s argument that the Doe plaintiff’s true name must
19 be supplied on the verifications under Code of Civil Procedure § 2015.5, which allows declarations under
20 penalty of perjury when “subscribed” by the party or witness, *id.* at 754, and held that, “for purposes of this
21 litigation, plaintiff’s verification of the petition using the name Jane Doe is appropriate. Any other rule
22 would render the ability to use a fictitious name in the litigation meaningless.” *Id.*, at 754.

23 **III. CONCLUSION**

24 For the foregoing reasons, Plaintiff respectfully requests that the Court allow Plaintiff to proceed in
25 this matter by pseudonym.

26 Dated: June 2, 2021

KEEGAN & BAKER, LLP
s/ Patrick N. Keegan
Patrick N. Keegan, Esq.
Attorney for Plaintiff JANE DOE

DECLARATION OF PATRICK N. KEEGAN

I, Patrick N. Keegan, declare as follows:

1. I am an attorney licensed to practice before all of the courts of the State of California. I am a partner of the law firm of Keegan & Baker, LLP, counsel of record for Plaintiff Jane Doe (or “Plaintiff”).

2. I submit this declaration pursuant to California Rules of Court, Rules 3.1200, *et seq.* in support of Plaintiff’s Ex Parte Application for an Order allowing Plaintiff to appear by pseudonym in this matter, pursuant to Cal. Civ. Code § 3427.3 (West 2011). On June 2, 2021, I received a call from the Court’s clerk for the Department requesting this *Ex Parte* Application be made.

3. Prior to filing Plaintiff’s Class Action Complaint for Damages, Restitution, and Injunctive Relief for Violations of: (1) the Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*; (2) Breach of California Security Notification Laws, California Civil Code § 1798.82; and (3) Business and Professions Code §§ 17200, *et seq.*, on June 1, 2021 (“Complaint”), I, on behalf of Plaintiff, sent separate letters to Defendant Neighborhood Healthcare (“NH”) and Defendant Health Center Partners of Southern California (“HCP”) disclosing the true name of Plaintiff Jane Doe and requesting further information about this security incident. Therefore, Plaintiff is *not* proceeding *anonymous* in this action, and the Defendants are not prejudice by Plaintiff proceeding pseudonymously in this action.

4. The Complaint was filed on Tuesday, June 1, 2021, thereafter I received a call from the Court’s clerk for the Department requesting this *Ex Parte* Application on Wednesday, June 2, 2021, and no defendant has been served or has yet appeared in this litigation and, for reasons specified herein, no opposition is anticipated and Plaintiff should not be required to inform defendants prior to the hearing on this matter.

I declare under penalty of perjury pursuant to the laws of the State of California that the foregoing is true and correct. Executed this 2nd day of June, 2021, in Carlsbad, California.

s/ Patrick N. Keegan
Patrick N. Keegan

FILED
Clerk of the Superior Court

JUN 08 2021

By: A. TAYLOR

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Tel: (760) 929-9303
4 Fax: (760) 929-9260

5 Attorney for Plaintiff
JANE DOE
6
7

8 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
9 **FOR THE COUNTY OF SAN DIEGO**

10 JANE DOE, individually and on behalf of all others
similarly situated,

11 Plaintiff,

12 vs.

13 NEIGHBORHOOD HEALTHCARE; HEALTH
14 CENTERS PARTNERS OF SOUTHERN
15 CALIFORNIA; NETGAIN TECHNOLOGY, LLC;
and DOE DEFENDANTS 1-100;

16 Defendants.
17

Case No. 37-2021-00023936-CU-BT-CTL

CLASS ACTION

Assigned to: Hon. Joel R. Wohlfeil, Dept. C-73

**[PROPOSED] ORDER GRANTING
PLAINTIFF'S EX PARTE APPLICATION TO
APPEAR BY PSEUDONYM**

Date: June 8, 2021

Time: 8:30 a.m.

Place: Department C-73

IMAGED FILE

18 Plaintiff Jane Doe's application for an order allowing Plaintiff to appear by pseudonym in this matter,
19 came *ex parte* for hearing on June 8, 2021, at 8:30 a.m. in Department C-73 before the Honorable Joel R.
20 Wohlfeil, and the Court, having reviewed Plaintiff Jane Doe's application and for good cause appearing
21 therefore, hereby orders as follows:

22 IT IS HEREBY ORDERED THAT:

23 Plaintiff Jane Doe alleges she was a patient within the meaning of Civil Code § 56.05(k). As such,
24 she is authorized by Civil Code § 3427.3 to use a pseudonym in this action to protect her privacy.

25 *order is w/o prejudice to an application to vacate this*
26 *order. 6-8-21*
Dated: _____

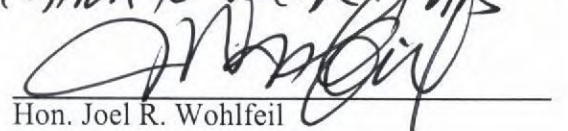
27 
Hon. Joel R. Wohlfeil
28 Judge of the Superior Court

EXHIBIT 2

1. ISSUE DATE: (MM/DD/YYYY) 8/29/2019
2a. FTCA DEEMING NOTICE NO.: 1-F00000167-19-01
2b. Supersedes: []
3. COVERAGE PERIOD: From: 1/1/2020 Through: 12/31/2020
4. NOTICE TYPE: Renewal
5. ENTITY NAME AND ADDRESS: NEIGHBORHOOD HEALTHCARE 425 N DATE ST ESCONDIDO, CA 92025
6. ENTITY TYPE: Grantee
7. EXECUTIVE DIRECTOR: Rakesh Patel
8a. GRANTEE ORGANIZATION: NEIGHBORHOOD HEALTHCARE
8b. GRANT NUMBER: H80CS00285

DEPARTMENT OF HEALTH AND HUMAN SERVICES
HEALTH RESOURCES AND SERVICES ADMINISTRATION



NOTICE OF DEEMING ACTION
FEDERAL TORT CLAIMS ACT AUTHORIZATION:
Federally Supported Health Centers Assistance Act(FSHCAA), as amended,
Sections 224(g)-(n) of the Public Health Service (PHS) Act, 42 U.S.C. § 233(g)-(n)

9. THIS ACTION IS BASED ON THE INFORMATION SUBMITTED TO, AND AS APPROVED BY HRSA, AS REQUIRED UNDER 42 U.S.C. § 233(h) FOR THE ABOVE TITLED ENTITY AND IS SUBJECT TO THE TERMS AND CONDITIONS INCORPORATED EITHER DIRECTLY OR BY REFERENCE IN THE FOLLOWING:

- a. The authorizing program legislation cited above.
- b. The program regulation cited above, and,
- c. HRSA's FTCA-related policies and procedures.

In the event there are conflicting or otherwise inconsistent policies applicable to the program, the above order of precedence shall prevail.

10. Remarks:

The check box [x] in the supersedes field indicates that this notice supersedes any and all active NDAs and rescinds any and all future NDAs issued prior to this notice.

Electronically signed by Tonya Bowers, Deputy Associate Administrator for Primary Health Care on: 8/29/2019 6:44:48 PM

A printer version document only. The document may contain some accessibility challenges for the screen reader users. To access same information, a fully 508 compliant accessible HTML version is available on the HRSA Electronic Handbooks in the FTCA Folder. If you need more information, please contact the BPHC Helpline at 877-974-BPHC (2742); Weekdays from 8:30 AM to 5:30 PM ET.

FTCA DEEMING NOTICE NO.:
1-F00000167-19-01

GRANT NUMBER:
H80CS00285



NEIGHBORHOOD HEALTHCARE
425 N DATE ST
ESCONDIDO, CA92025

Dear Rakesh Patel:

The Health Resources and Services Administration (HRSA), in accordance with the Federally Supported Health Centers Assistance Act (FSHCAA), as amended, sections 224(g)-(n) of the Public Health Service (PHS) Act, 42 U.S.C. §§ 233(g)-(n), deems NEIGHBORHOOD HEALTHCARE to be an employee of the PHS, for the purposes of section 224, effective 1/1/2020 through 12/31/2020.

Section 224(a) of the PHS Act provides liability protection under the Federal Tort Claims Act (FTCA), 28 U.S.C. §§ 1346(b), 2672, or by alternative benefits provided by the United States where the availability of such benefits precludes a remedy under the FTCA, for damage for personal injury, including death, resulting from the performance of medical, surgical, dental, or related functions by PHS employees while acting within the scope of such employment. This protection is exclusive of any other civil action or proceeding. Coverage extends to deemed entities and their (1) officers; (2) governing board members; (3) full- and part-time employees; and (4) contractors who are licensed or certified individual health care practitioners providing full-time services (i.e., on average at least 32½ hours per week for the entity for the period of the contract), or, if providing an average of less than 32½ hours per week of such service, are licensed or certified providers in the fields of family practice, general internal medicine, general pediatrics, or obstetrics/gynecology. Volunteers are neither employees nor contractors and therefore are not eligible for FTCA coverage under FSHCAA.

This Notice of Deeming Action (NDA) is also confirmation of medical malpractice coverage for both NEIGHBORHOOD HEALTHCARE and its covered individuals as described above. This NDA, along with documentation confirming employment or contractor status with the deemed entity, may be used to show liability coverage for damage for personal injury, including death, resulting from the performance of medical, surgical, dental, or related functions by PHS employees while acting within the scope of such employment.

In addition, FTCA coverage is comparable to an "occurrence" policy without a monetary cap. Therefore, any coverage limits that may be mandated by other organizations are met.

This action is based on the information provided in your FTCA deeming application, as required under 42 U.S.C. § 233(h), with regard to your entity's: (1) implementation of appropriate policies and procedures to reduce the risk of malpractice and litigation; (2) review and verification of professional credentials and privileges, references, claims history, fitness, professional review organization findings, and licensure status of health professionals; (3) cooperation with the Department of Justice (DOJ) in the defense of claims and actions to prevent claims in the future; and (4) cooperation with DOJ in providing information related to previous malpractice claims history.

Deemed health centers must continue to receive funding under Section 330 of the PHS Act, 42 U.S.C. § 254b, in order to maintain coverage as a deemed PHS employee. If the deemed entity loses its Section 330 funding, such coverage will end immediately upon termination of the grant. In addition to the relevant statutory and regulatory requirements, every deemed health center is expected to follow HRSA's FTCA-related policies and procedures, which may be found online at <http://www.bphc.hrsa.gov>.

For further information regarding FTCA, please contact the Health Center Program Support (Formally the BPHC Helpline) at 877-464-4772, option 1, or using the [BPHC Contact Form](#).

A printer version document only. The document may contain some accessibility challenges for the screen reader users. To access same information, a fully 508 compliant accessible HTML version is available on the HRSA Electronic Handbooks in the FTCA Folder. If you need more information, please contact the BPHC Helpline at 877-974-BPHC (2742); Weekdays from 8:30 AM to 5:30 PM ET.

EXHIBIT 3



August 18, 2021

Daniel T. Rockey
Partner
Direct: +1 415 268 1986
Fax: +1 415 430 4386
daniel.rockey@bclplaw.com

BRYAN CAVE LEIGHTON PAISNER LLP
Three Embarcadero Center
7th Floor
San Francisco CA 94111 4070
T: +1 415 675 3400
F: +1 415 675 3434
bclplaw.com

By United States Mail and Email

U.S. Department of Health and Human Services
Office of the General Counsel
General Law Division
Claims and Employment Law Branch
330 "C" Street, SW
Attention: CLAIMS
Switzer Building, Suite 2600
Washington, D.C. 20201
FAX No. 202-619-2922
HHS-FTCA-Claims@hhs.gov

**Re: Federal Torts Claims Act - Notice of Suit by Deemed Entity pursuant to 42 USC 233(l)
and 28 C.F.R. § 15.2**

To Whom it May Concern:

I am an attorney with the law firm of Bryan Cave Leighton Paisner, LLP and counsel to Neighborhood Healthcare ("Neighborhood Healthcare"), a non-profit public benefit corporation and community health center that provides medical, dental, and behavioral health services to underserved communities in and around Escondido, California, where it is located. Neighborhood Healthcare is a federal grant recipient (Grant No. H80CS00285) and a "deemed entity" pursuant to 42 USC §233(g). See Exh. 1 HRSA Deeming Notice.

I am writing to provide notice pursuant to 42 USC 233(l), 28 C.F.R. § 15.2, and Health and Human Services Administration policy¹ that a complaint has been filed against Neighborhood Healthcare in San Diego Superior Court, captioned *Jane Doe v. Neighborhood Healthcare, et al.*, Case No. 37-2021-00023936-CU-BT-CTL. See Complaint attached as Exhibit 2. The complaint alleges that Neighborhood Healthcare violated the California Confidentiality of Medical Information Act ("CMIA") by sharing plaintiff Jane Doe's medical records without proper authorization (Ca. Civ. Code §56.10) and/or failing to maintain patient medical records in such a way as to ensure their confidentiality (Ca. Civ. Code § 56.101).

The Federally Supported Health Centers Assistance Act of 1992 (and as amended in 1995) (the "FSHCAA"), 42 U.S.C. § 233(g) *et seq.*, authorizes the Secretary of Health and Human Services to extend to certain federally funded health centers and their officers, directors, and employees the same protection that § 233(a) affords to Public Health Service ("PHS") employees. Under the Emergency Health Personnel Act of 1970, Pub. L. No. 91-623, § 4, 84 Stat. 1868, 1870-71 (1970), codified at 42 U.S.C. § 233, Public Health Service personnel are immunized from any civil action or proceeding arising out of the performance of medical, surgical, dental or related functions within the scope of their

¹ See <https://bphc.hrsa.gov/ftca/claimsfilings/healthcenterclaims.html> for complaint notice guidance.

Randy S. Grossman
 August 18, 2021
 Page 2



employment. 42 U.S.C. § 233(a). To facilitate the legislative objective of ensuring the availability of medical services in underserved areas, 42 U.S.C. § 233(a) shields PHS personnel from liability arising out of their medical and related duties by making the remedy for damages against the United States under the Federal Tort Claims Act the exclusive remedy for such actions. *Id.*

The protection offered to federally funded health centers by the FSHCAA grants “absolute immunity . . . for actions arising out of the performance of medical or related functions within the scope of . . . employment by barring all actions against them for such conduct.” *Hui v. Castaneda*, 559 U.S. 799, 806 (2010). Once a community health center is determined by the Health Resources and Services Administration (“HRSA”) to be a “deemed entity” pursuant to § 233(g), the FTCA is the exclusive remedy for damages resulting from the performance of medical, dental or “related functions.” 42 U.S.C. § 233(a). When the Secretary determines that a health center is a deemed entity for a given annual period, that “determination shall be final and binding upon the Secretary and the Attorney General and other parties to any civil action or proceeding.” 42 USC §233(g)(1)(F).

Upon the filing of a state court complaint, a deemed entity is directed to provide notice of the complaint to the appropriate federal agency -- in this case, the Health and Human Services Administration – which is itself directed to promptly provide notice to the United States Attorney for the district embracing the place where the action is brought, as well as the Branch Director of the Torts Branch, Civil Division, Department of Justice.² Because the *Doe* complaint filed against Neighborhood Healthcare was brought in San Diego County, the district embracing the filing location is the Southern District of California. Although the obligation to notify the United States Attorney falls upon HHS, for convenience and efficiency, we are copying the Acting U.S. Attorney for the Southern District of California, Randy S. Grossman, with this notice.³

Upon notification that a state court action is pending against a deemed entity, the Attorney General has a mandatory duty to appear in that court within 15 days of notice of the lawsuit to report whether the “Secretary has determined under subsections (g) and (h) of [Section 233], that such entity, officer, governing board member, employee, or contractor of the entity is deemed to be an employee of the Public Health Service for purposes of this section with respect to the actions or omissions that are the subject of such civil action or proceeding.” 42 USC § 233(l)(1).

Importantly, the immunity provided under § 233(a) is not limited to claims of medical malpractice, but encompasses liability arising out of “related functions”— *i.e.*, functions related to the performance of medical, surgical, or dental functions. 42 U.S.C. § 233(a); *Teresa T. v. Ragaglia* (D. Conn. 2001) 154 F.Supp.2d 290, 299-300 (immunity provided by Section 233(a) “is not limited to claims for medical malpractice” and extends to functions related to the provision of medical care); *Cuoco v. Moritsugu* (2d Cir. 2000) 222 F.3d 99, 108 (“Cuoco asserts that § 233(a) provides immunity only from medical malpractice claims. But there is nothing in the language of § 233(a) to support that conclusion.”); *Z.B. ex rel. Next Friend v. Ammonoosuc Community Health Services, Inc.* (D. Me., June 13, 2004, No. CIV. 03-540 (NH)) 2004 WL 1571988, at *3, *report and recommendation adopted sub nom. Z.B. ex rel. Kilmer v. Ammonoosuc Community Health Services, Inc.* (D. Me., Aug. 31, 2004, No. CIV. 04-34-P-S) 2004 WL 1925538 (holding that alleged failure to report domestic abuse in connection with home health visits subject to §233(a) immunity as such “negligence is ‘related to’ the provision of medical services because the duty to report arises out of the employees’ status as medical professionals.”); *Pinzon v. Mendocino Coast Clinics Inc.* (N.D. Cal., Aug. 20, 2015, No. 14-CV-05504-JST) 2015 WL 4967257, at *3 (holding that

² 28 C.F.R. § 15.2.

³ This notice is being simultaneously transmitted to Randy S. Grossman, Acting United States Attorney, U.S. Attorney’s Office Southern District of California, Federal Office Building, 889 Front Street, Room 6293, San Diego, California 92101-0720.

Randy S. Grossman
 August 18, 2021
 Page 3



plaintiff's claims for violation of the Americans with Disabilities Act, the Civil Rights Act of 1964, and the Health Insurance Portability and Accountability Act of 1996 were covered by §233(a) immunity because the remedy against the United States provided thereby is 'exclusive of any other civil action or proceeding by reason of the same subject-matter' against the employee.'). "Related functions" includes administrative or operational activities which relate to the provision of medical, dental, or surgical healthcare. *See, e.g., C. K. v. United States* (S.D. Cal., Nov. 12, 2020, No. 19-CV-2492 TWR (RBB)) 2020 WL 6684921, at *6 ("administrative or operational duties could qualify as related functions where they were connected to the provision of medical care.').

Maintaining medical records for patients receiving health care, and ensuring the confidentiality of such records, is a core administrative and operational function of providing healthcare and is thus a "medical ... or related function" within the meaning of 42 U.S.C. § 233(a). Indeed, maintaining the confidentiality of health records is a legally required function of providing health care under both state and federal law. For example, the California Confidentiality of Medical Information Act ("CMIA") requires health care providers to maintain patient health records and to provide a copy of such health records to the patient upon request. Civ. Code, § 56.07. The CMIA prohibits providers of healthcare from disclosing medical information without patient authorization, except for certain specified purposes, which includes diagnosis, treatment, and payment. Civ. Code § 56.10. The CMIA further provides that "[e]very provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Civ. Code, § 56.101. Similarly, the Health Insurance Portability and Accountability Act of 1996 also requires that healthcare providers maintain patient health records and disclose such records only with patient authorization (45 C.F.R. § 164.502) or "for treatment, payment, or health care operations" (45 C.F.R. § 164.506), and requires maintenance of administrative, physical, and technical safeguards for electronic patient health records to guard against unauthorized access or disclosure (45 C.F.R. § 164.302 *et seq.*). In fact, the statute which governs the federal health center program and which renders a health center eligible for §233(a) immunity, requires the center to have, among other things, "an ongoing quality improvement system that includes clinical services and management, and that maintains the confidentiality of patient records." 42 U.S.C. § 254b(b)(1)-(2), (k)(3)(C).

In *Mele v. Hill Health Center* (D. Conn., Jan. 8, 2008, No. 3:06CV455SRU) 2008 WL 160226, the District Court held that allegations the defendant improperly disclosed the plaintiff's medical records in violation of medical confidentiality laws fell within the "related functions" covered by §233(a). *Id.* at *2-4. The court explained:

Those claims concern the medical functions of providing treatment and the related function of ensuring the privacy of patient medical information. Thus, the claims are covered by section 233(a).

Id. Other courts have similarly assessed that §233(a) immunity applies to alleged breaches of patient confidentiality. For example, in *Kezer v. Penobscot Community Health Center*, 15-cv-225-JAW, 2019 BL 141566 at *6 (D. Me. Mar. 21, 2019), the court held that a claimed breach of patient confidentiality falls within the scope of § 233(a) immunity, as "the Plaintiffs' claim arose when the Defendants, who are all medical providers, fa[iled] to comply with their ongoing professional duty to keep Ms. Kezer's medical records confidential while performing health care services." In so holding, the court noted that under applicable state law, a breach of confidentiality fell within the rubric of professional medical negligence. *Id.* Notably, Judge Robinson of the US District Court for the Southern District of California, the district in which the complaint against Neighborhood Healthcare was brought, cited *Kezer* approvingly in rejecting the Department of Justice's argument that § 233(a) did not embrace a health center employee's alleged failure to report suspected abuse. *C. K.,* (S.D. Cal., Nov. 12, 2020, No. 19-CV-2492 TWR (RBB)) 2020 WL

Randy S. Grossman
August 18, 2021
Page 4



6684921, at *6 (“As in *Kezer*, applicable state law supports a medical malpractice claim,....”). *See also, Logan v. St. Charles Health Council, Inc.* (W.D. Va., May 1, 2006, No. 1:06CV00039) 2006 WL 1149214, at *1–3 (holding that FTCA embraces claims for breach of privacy statute, but finding that §233(a) did not apply because plaintiff sued based on employer/employee relationship, rather than patient/medical professional relationship); *Roberson v. Greater Hudson Valley Family Health Center, Inc.* (S.D.N.Y., June 12, 2018, No. 17-CV-7325 (NSR)) 2018 WL 2976024, at *1 (claim alleging that employee of defendant inappropriately accessed plaintiff’s medical records and disclosed information to people she knew must be dismissed for failure to file administrative claim as required by FTCA); *See also Brignac v. United States*, 239 F.Supp.3d 1367, 1377-78 (N.D. Ga. 2017) (applying § 233(a) where patient brought a negligent supervision claim against the health center alleging he was sexually assaulted by a doctor during treatment); *La Casa de Buena Salud v. United States*, No. CIV 07-238 JB/RHS, 2008 WL 2323495, at *20 (D.N.M. Mar. 21 2008) (applying § 233(a) to a negligent hiring claim brought by the estate of a deceased patient, as hiring was a “related function”).

Here, Plaintiff Doe, a patient of Neighborhood Healthcare, alleges that Neighborhood failed to ensure the confidentiality of her patient records, as required by Civil Code § 56.10 and § 56.101 of the CMIA. As the above courts have recognized, the maintenance of current, accurate, and accessible medical records is a “related function” to the provision of medical care, and ensuring the confidentiality of such records is a legally required function of healthcare providers under both the CMIA and HIPAA. The courts have further held that the alleged failure of a healthcare provider to maintain the confidentiality of medical records in violation of §56.10 of the CMIA constitutes a claim for professional negligence under California law. *See, e.g., Francies v. Kapla* (2005) 127 Cal.App.4th 1381, 1386, fn. 11, *as modified* (Apr. 8, 2005) (holding that claim for unauthorized disclosure of medical records in violation of CMIA is subject to cap on noneconomic damages under Medical Injury Compensation Reform Act); Civ. Code, § 3333.2 (MICRA applies to “any action for injury against a health care provider based on professional negligence.”). It is thus clear that the claims of Jane Doe asserted against Neighborhood Healthcare here fit squarely within the immunity provided by §233(a).

In view of the foregoing, Neighborhood Healthcare hereby requests that the United States promptly appear in *Doe v. Neighborhood Healthcare et al.*, and assume the defense of the matter. Please note that because not all parties have been served with the complaint, the plaintiff and Neighborhood Healthcare have stipulated to an extension of time to respond to the complaint up to and including September 8, 2021.

Randy S. Grossman
August 18, 2021
Page 5



If you wish to discuss the foregoing or have any questions concerning the lawsuit, please do not hesitate to reach out to me. I can provide any information that would be helpful understanding the allegations and the incident upon which they are premised, and am ready and willing to facilitate all necessary cooperation in the defense of the above-referenced claims.

Very truly yours,

Daniel T. Rockey

Partner

DTR
Enclosures

Cc: Randy S. Grossman, Acting United States Attorney for the Southern District of California
(Randy.Grossman@usdoj.gov)

EXHIBIT 1

1. ISSUE DATE: (MM/DD/YYYY) 8/29/2019
2a. FTCA DEEMING NOTICE NO.: 1-F00000167-19-01
2b. Supersedes: []
3. COVERAGE PERIOD: From: 1/1/2020 Through: 12/31/2020
4. NOTICE TYPE: Renewal
5. ENTITY NAME AND ADDRESS: NEIGHBORHOOD HEALTHCARE 425 N DATE ST ESCONDIDO, CA 92025
6. ENTITY TYPE: Grantee
7. EXECUTIVE DIRECTOR: Rakesh Patel
8a. GRANTEE ORGANIZATION: NEIGHBORHOOD HEALTHCARE
8b. GRANT NUMBER: H80CS00285

DEPARTMENT OF HEALTH AND HUMAN SERVICES
HEALTH RESOURCES AND SERVICES ADMINISTRATION



NOTICE OF DEEMING ACTION
FEDERAL TORT CLAIMS ACT AUTHORIZATION:
Federally Supported Health Centers Assistance Act(FSHCAA), as amended,
Sections 224(g)-(n) of the Public Health Service (PHS) Act, 42 U.S.C. § 233(g)-(n)

9. THIS ACTION IS BASED ON THE INFORMATION SUBMITTED TO, AND AS APPROVED BY HRSA, AS REQUIRED UNDER 42 U.S.C. § 233(h) FOR THE ABOVE TITLED ENTITY AND IS SUBJECT TO THE TERMS AND CONDITIONS INCORPORATED EITHER DIRECTLY OR BY REFERENCE IN THE FOLLOWING:

- a. The authorizing program legislation cited above.
- b. The program regulation cited above, and,
- c. HRSA's FTCA-related policies and procedures.

In the event there are conflicting or otherwise inconsistent policies applicable to the program, the above order of precedence shall prevail.

10. Remarks:

The check box [x] in the supersedes field indicates that this notice supersedes any and all active NDAs and rescinds any and all future NDAs issued prior to this notice.

Electronically signed by Tonya Bowers, Deputy Associate Administrator for Primary Health Care on: 8/29/2019 6:44:48 PM

A printer version document only. The document may contain some accessibility challenges for the screen reader users. To access same information, a fully 508 compliant accessible HTML version is available on the HRSA Electronic Handbooks in the FTCA Folder. If you need more information, please contact the BPHC Helpline at 877-974-BPHC (2742); Weekdays from 8:30 AM to 5:30 PM ET.

FTCA DEEMING NOTICE NO.:
1-F00000167-19-01

GRANT NUMBER:
H80CS00285



NEIGHBORHOOD HEALTHCARE
425 N DATE ST
ESCONDIDO, CA92025

Dear Rakesh Patel:

The Health Resources and Services Administration (HRSA), in accordance with the Federally Supported Health Centers Assistance Act (FSHCAA), as amended, sections 224(g)-(n) of the Public Health Service (PHS) Act, 42 U.S.C. §§ 233(g)-(n), deems NEIGHBORHOOD HEALTHCARE to be an employee of the PHS, for the purposes of section 224, effective 1/1/2020 through 12/31/2020.

Section 224(a) of the PHS Act provides liability protection under the Federal Tort Claims Act (FTCA), 28 U.S.C. §§ 1346(b), 2672, or by alternative benefits provided by the United States where the availability of such benefits precludes a remedy under the FTCA, for damage for personal injury, including death, resulting from the performance of medical, surgical, dental, or related functions by PHS employees while acting within the scope of such employment. This protection is exclusive of any other civil action or proceeding. Coverage extends to deemed entities and their (1) officers; (2) governing board members; (3) full- and part-time employees; and (4) contractors who are licensed or certified individual health care practitioners providing full-time services (i.e., on average at least 32½ hours per week for the entity for the period of the contract), or, if providing an average of less than 32½ hours per week of such service, are licensed or certified providers in the fields of family practice, general internal medicine, general pediatrics, or obstetrics/gynecology. Volunteers are neither employees nor contractors and therefore are not eligible for FTCA coverage under FSHCAA.

This Notice of Deeming Action (NDA) is also confirmation of medical malpractice coverage for both NEIGHBORHOOD HEALTHCARE and its covered individuals as described above. This NDA, along with documentation confirming employment or contractor status with the deemed entity, may be used to show liability coverage for damage for personal injury, including death, resulting from the performance of medical, surgical, dental, or related functions by PHS employees while acting within the scope of such employment.

In addition, FTCA coverage is comparable to an "occurrence" policy without a monetary cap. Therefore, any coverage limits that may be mandated by other organizations are met.

This action is based on the information provided in your FTCA deeming application, as required under 42 U.S.C. § 233(h), with regard to your entity's: (1) implementation of appropriate policies and procedures to reduce the risk of malpractice and litigation; (2) review and verification of professional credentials and privileges, references, claims history, fitness, professional review organization findings, and licensure status of health professionals; (3) cooperation with the Department of Justice (DOJ) in the defense of claims and actions to prevent claims in the future; and (4) cooperation with DOJ in providing information related to previous malpractice claims history.

Deemed health centers must continue to receive funding under Section 330 of the PHS Act, 42 U.S.C. § 254b, in order to maintain coverage as a deemed PHS employee. If the deemed entity loses its Section 330 funding, such coverage will end immediately upon termination of the grant. In addition to the relevant statutory and regulatory requirements, every deemed health center is expected to follow HRSA's FTCA-related policies and procedures, which may be found online at <http://www.bphc.hrsa.gov>.

For further information regarding FTCA, please contact the Health Center Program Support (Formally the BPHC Helpline) at 877-464-4772, option 1, or using the [BPHC Contact Form](#).

A printer version document only. The document may contain some accessibility challenges for the screen reader users. To access same information, a fully 508 compliant accessible HTML version is available on the HRSA Electronic Handbooks in the FTCA Folder. If you need more information, please contact the BPHC Helpline at 877-974-BPHC (2742); Weekdays from 8:30 AM to 5:30 PM ET.

EXHIBIT 2

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Telephone: (760) 929-9303
4 Facsimile: (760) 929-9260

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego
06/01/2021 at 04:40:18 PM
Clerk of the Superior Court
By Richard Day, Deputy Clerk

5 Attorneys for Plaintiff JANE DOE

6
7 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
8 **FOR THE COUNTY OF COUNTY OF SAN DIEGO**

9 JANE DOE, individually and on behalf of all
others similarly situated,

10 Plaintiff,

11 vs.

12 NEIGHBORHOOD HEALTHCARE; HEALTH
13 CENTER PARTNERS OF SOUTHERN
CALIFORNIA; NETGAIN TECHNOLOGY,
14 LLC; and DOE DEFENDANTS 1-100;

15 Defendants.
16

) Case No.: 37-2021-00023936-CU-BT-CTL

) **CLASS ACTION COMPLAINT FOR**
) **DAMAGES, RESTITUTION, AND**
) **INJUNCTIVE RELIEF FOR VIOLATIONS**
) **OF:**

-) (1) **THE CONFIDENTIALITY OF**
) **MEDICAL INFORMATION ACT,**
) **CIVIL CODE §§ 56, ET SEQ.;**
) (2) **BREACH OF CALIFORNIA**
) **SECURITY NOTIFICATION**
) **LAWS, CALIFORNIA CIVIL CODE**
) **§ 1798.82; AND**
) (3) **BUSINESS AND PROFESSIONS**
) **CODE §§ 17200, ET SEQ.**

) **JURY TRIAL DEMANDED**
)

17
18
19 Plaintiff Jane Doe (or “Plaintiff”), by and through her attorneys, bring this class action on
20 behalf of herself individually and all others similarly situated, against Defendants Neighborhood
21 Healthcare, Health Center Partners of Southern California, and Netgain Technology, LLC
22 (collectively referred to as “Defendants”), and alleges upon information and belief as follows:

23 **INTRODUCTION**

24 1. This class action arises from the negligent and failure of Defendants to properly
25 create, maintain, preserve, and/or store confidential, medical and personal identifying information
26 of Plaintiff¹ and all other persons similarly situated which allowed an unauthorized person to gain
27

28 ¹ California statutory law specifically allows a party to bring a lawsuit using a pseudonym in cases involving health care patients. Cal. Civ. Code § 3427.3 (West 2011). Specifically, section 3427.3

1 access to a computer database server of Defendants from October 22, 2020 to December 3, 2020,
2 causing unauthorized access, viewing, exfiltration, theft, and/or disclosure of unencrypted medical
3 and personal identifying information of Plaintiff and other persons similarly situated, to at least one
4 unauthorized person resulting in violations of the Confidentiality of Medical Information Act, Civil
5 Code §§ 56, *et seq.* (hereinafter referred to as the “Act”), the Security Notification Laws, Civil Code
6 § 1798.82, and the Business and Professions Code §§ 17200 *et seq.* Under the Act, Plaintiff, and
7 all other persons similarly situated, have the right to expect that the confidentiality of their medical
8 information in possession of Defendants and/or derived from Defendants to be reasonably
9 preserved and protected from unauthorized access, viewing, exfiltration, theft, and/or disclosure.

10 2. As alleged more fully below, failing to take adequate and reasonable measures to
11 ensure its data systems were protected against unauthorized intrusions, by failing to invest in cyber
12 security and data protection safeguards, failing to implement adequate and reasonable security
13 controls and user authorization and authentication processes, failing to limit the types of data
14 permitted to be transferred, failing to properly and adequately educate and train its employees, and
15 to put into place reasonable or adequate computer systems and security practices to safeguard
16 customers’ and patients’ medical and personal identifying information, Defendants negligently
17 created, maintained, preserved, and stored Plaintiff’s and the Class (defined *infra*) members’
18 medical and personal identifying information in possession of or derived from Defendants allowed
19 such information to be accessed and actually viewed by at least one unauthorized third party,
20 without Plaintiff’s and the Class members’ prior written authorization, which constitutes
21 unauthorized disclosure and/or release of their information in violation of Civil Code §§ 56.10(a)
22 and 56.101(a) of the Act. In fact, Defendant Health Center Partners of Southern California’s form

23
24
25 provides, “The court having jurisdiction over a civil proceeding under this title shall take all steps
26 ***reasonably necessary to safeguard the individual privacy and prevent harassment of a health care***
27 ***patient***, licensed health practitioner, or employee, client, or customer of a health care facility who is
28 a party or witness in the proceeding, including granting protective orders. ***Health care patients***,
licensed health practitioners, and employees, clients, and customers of the health care facility ***may***
use pseudonyms to protect their privacy.” Cal. Civ. Code § 3427.3 (emphasis added). Here, a
pseudonym has been used in place of the real name of Plaintiff because at all times relevant to this
action, Plaintiff is a health care patient under Civil Code § 56.05(k) and has individual privacy
concerns and a reasonable fear of harassment in light of the nature of the case.

1 letter, entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle, President &
2 Chief Executive Officer, Health Center Partners of Southern California, sent to Plaintiff and all
3 other persons similarly situated, informing them, in part, of “a recent data security incident
4 experienced by Netgain Technology, LLC (‘Netgain’), the IT service provider for Health Center
5 Partners of Southern California (‘HCP’)” and stating, in part, “HCP supports community health
6 centers in a variety of ways, including collaborative grant-funded programs and services for
7 Neighborhood Healthcare.... **What Happened:** Netgain recently informed HCP that it had
8 experienced a data security incident that involved systems containing HCP data.... According to
9 Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital
10 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
11 obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the
12 attacker in exchange for assurances that the attacker will delete all copies of this data and that it will
13 not publish, sell, or otherwise disclose the data.... The information involved varies depending on the
14 individual but may include the following: name, address, date of birth, diagnosis/treatment
15 information and treatment cost information. Once we learned that HCP data may have been
16 involved in the incident, we worked with our cybersecurity experts to review the impacted files and
17 identify the individuals whose information was contained in such files so that we may notify such
18 individuals. Our investigation revealed that the impacted files contained your personal information.”
19 An exemplar of Defendant Health Center Partners of Southern California’s “**Notice of Data**
20 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
21 as **Exhibit A.**

22 3. Additionally, Defendant Neighborhood Healthcare caused a form letter sent on its
23 behalf, entitled “**Notice of Data Breach,**” dated April 8, 2021, signed by Rakesh Patel, CEO,
24 Neighborhood Healthcare, stating, in part, “We are writing to make you aware of an issue brought
25 to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud
26 hosting and managed services provider. Neighborhood Healthcare used Netgain to host some
27 Neighborhood Healthcare files. **What Happened** On November 24, 2020, Netgain became aware
28 of a security incident that involved unauthorized access to portions of the Netgain environment and

1 Netgain client environments and began taking steps to investigate this incident. But, on December
2 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files
3 owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain
4 took additional measures to contain the threat and address the issue. Netgain’s technical teams
5 worked closely with third-party experts to remove the threat in the impacted environments and
6 confirm that client and internal systems are protected. Neighborhood Healthcare learned of the
7 ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to
8 believe that the protected health information (“PHI”) of our patients had been impacted in the
9 incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some
10 information including, potentially, some files containing patient PHI may have been impacted in the
11 incident. Netgain could not confirm, at that time, what records may have been impacted in the
12 incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood
13 Healthcare that Netgain believed were impacted by the attackers. Those files came from a
14 Neighborhood Healthcare server accessible by the Netgain environment. Since that time,
15 Neighborhood Healthcare has worked to review those records, to identify individuals impacted,
16 conduct an investigation into the incident with the assistance outside experts, and to transmit this
17 letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood
18 Healthcare determined that the impacted files included some of your information. **What**
19 **Information Was Involved** The information involved may have included some of the following:
20 your name, date of birth, address, Social Security Number and information about the care that you
21 received from Neighborhood Healthcare such as insurance coverage information, physician you
22 saw, and treatment codes.” An exemplar of Defendant Neighborhood Healthcare’s “**Notice of Data**
23 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
24 as **Exhibit B**.

25 4. Additionally, Defendant Netgain Technology, LLC stated in a blog post, entitled
26 “What we learned as a ransomware victim – so you don’t become one,” that “late last year, Netgain
27 was the victim of a criminal ransomware attack.... to become a victim of such an attack is both
28 humbling and galvanizing.... we identified additional opportunities to strengthn our security posture

1 in a continuous journey with an ongoing commitment to ensure this remains top-of-mind. As part
2 of our incident response, we have implemented a number of these identified enhancements to our
3 security posture and have continued to progress a multipronged approach. We've deployed new
4 tools, revised policies and enforcement procedures, and implemented an advanced around-the-clock
5 managed detections and response service for proactive threat monitoring.”

6 5. Because the individually identifiable medical information and other personal
7 identifying information of Plaintiff and the Class was subject to unauthorized access and viewing by
8 at least one unauthorized third party and in violation of the Act, Plaintiff, individually and on behalf
9 of all others similarly situated, seeks from Defendants nominal damages in the amount of one
10 thousand dollars (\$1,000) for each violation under Civil Code §56.36(b)(1) and actual damages,
11 according to proof, for each violation pursuant to Civil Code § 56.36(b)(2). Further, because
12 Plaintiff also alleges Defendants' conduct violates Business & Professions Code §§ 17200, *et seq.*,
13 Plaintiff, individually and on behalf of others similarly situated, seeks injunctive relief and
14 restitution from Defendants under Business and Professions Code § 17203.

15 6. This action, if successful, will enforce an important right affecting the public interest
16 and would confer a significant benefit, whether pecuniary or non-pecuniary, on a large class of
17 persons. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff
18 in relation to Plaintiff's stake in the matter, and therefore class certification is appropriate in this
19 matter.

20 **JURISDICTION AND VENUE**

21 7. This Court has jurisdiction over this action under California Code of Civil Procedure
22 § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class in the aggregate
23 exceeds the \$25,000 jurisdictional minimum of this Court. Further, the amount in controversy as to
24 Plaintiff individually does not exceed \$75,000.

25 8. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of
26 Civil Procedure §§ 395(a) and 395.5 because Defendant Neighborhood Healthcare is incorporated
27 in and does business in the State of California, and employs persons located in the County of San
28 Diego and in this judicial district. Defendants have obtained medical information of Plaintiff and

1 the Class in the transaction of business in the State of California and in this judicial district, which
2 has caused both obligations and liability of Defendants to arise in the State of California and in this
3 judicial district.

4 9. Further, this action does not qualify for federal jurisdiction under the Class Action
5 Fairness Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies
6 to this action because (1) more than two-thirds of the members of the proposed Class and SubClass
7 are citizens of the State of California, and (2) Defendants are citizens of the State of California.

8 **PARTIES**

9 **A. PLAINTIFF**

10 10. Plaintiff Jane Doe is and was at all times relevant to this action a resident of the State
11 of California and citizen of the State of California. At all times relevant to this action, Plaintiff
12 JANE DOE was a patient of, received medical treatment and diagnosis from, and provided her
13 personal information, including her name, address, date of birth, social security number, phone
14 number and email address to Defendant Neighborhood Healthcare. Additionally, Plaintiff received
15 a letter addressed to her, sent on Defendant Health Center Partners of Southern California’s behalf,
16 entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle, President & Chief
17 Executive Officer, Health Center Partners of Southern California, informing her, in part, of “a
18 recent data security incident experienced by Netgain Technology, LLC (‘Netgain’), the IT service
19 provider for Health Center Partners of Southern California (‘HCP’)” and stating, in part, “HCP
20 supports community health centers in a variety of ways, including collaborative grant-funded
21 programs and services for Neighborhood Healthcare.... **What Happened:** Netgain recently
22 informed HCP that it had experienced a data security incident that involved systems containing
23 HCP data.... According to Netgain, in late September 2020, an unauthorized third party gained
24 access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the
25 unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an
26 undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies
27 of this data and that it will not publish, sell, or otherwise disclose the data.... The information
28 involved varies depending on the individual but may include the following: name, address, date of

1 birth, diagnosis/treatment information and treatment cost information. Once we learned that HCP
2 data may have been involved in the incident, we worked with our cybersecurity experts to review
3 the impacted files and identify the individuals whose information was contained in such files so that
4 we may notify such individuals. Our investigation revealed that the impacted files contained your
5 personal information.” As a result, Plaintiff reasonably fears that disclosure and/or release of her
6 medical information created, maintained, preserved and/or stored on Defendants’ computer
7 networks could subject her to harassment or abuse.

8 **B. DEFENDANTS**

9 11. Defendant Neighborhood Healthcare (“NH”) is a California corporation, is registered
10 to do business and does business in the State of California (CA Corp. No. C0667935), with its
11 principal business office located at 1540 E. Valley Parkway, Escondido CA 92026, and with its
12 registered agent of service of process located at 150 La Terraza Blvd, Suite 201, Escondido CA
13 92025. On or about April 8, 2021, NH caused a form letter sent on its behalf, entitled “**Notice of**
14 **Data Breach,**” dated April 8, 2021, signed by Rakesh Patel, CEO, Neighborhood Healthcare, an
15 exemplar of which is attached hereto as **Exhibit B**, to be submitted to the Attorney General of the
16 State of California. At all times relevant to this action, NH was and is a provider of health care, a
17 contractor, and/or other authorized recipient of personal and confidential medical information, as
18 that term is defined and set forth in the Act, including the names, addresses, dates of birth,
19 diagnosis/treatment information and treatment cost information of Plaintiff and the SubClass
20 (defined *infra*), and is subject to the requirements and mandates of the Act, including but not limited
21 to Civil Code §§ 56.10, 56.101 and 56.36. At all times relevant to this action, NH was and is a
22 provider of health care and employed and employs persons located in the County of San Diego
23 and in this judicial district.

24 12. Defendant Health Center Partners of Southern California (“HCP”) is a business
25 entity doing business in the State of California, with its principal business office located at 3710
26 Ruffin Road, San Diego, CA 92123. On or about April 12, 2021, HCP caused a form letter sent on
27 its behalf, entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle,
28 President & Chief Executive Officer, Health Center Partners of Southern California, an exemplar of

1 which is attached hereto as **Exhibit A**, to be submitted to the Attorney General of the State of
2 California and to be mailed to Plaintiff and the Class. At all times relevant to this action, HCP was
3 and is a “business” within the meaning of Civil Code § 1798.140(c)(1), owns or licenses
4 computerized data which includes Plaintiff’s and the Class’ personal information, within the
5 meaning of Civil Code § 1798.82(h), collected Plaintiff’s and the Class’ personal information
6 within the meaning of Civil Code § 1798.81.5(d)(1)(A).

7 13. Defendant Netgain Technology, LLC (“NETGAIN”) is a business entity doing
8 business in the State of California, with its principal business office located at 5353 Mission Center
9 Road, Suite 202, San Diego, CA 92108. At all times relevant to this action, NETGAIN was and is
10 NH’s and HCP’s third-party vendor. On March 24, 2021, NETGAIN posted on its website a blog,
11 entitled “What we learned as a ransomware victim – so you don’t become one,” which stated, in
12 part, “In our case, late last year, Netgain was the victim of a criminal ransomware attack.... to
13 become a victim of such an attack is both humbling and galvanizing.... we identified additional
14 opportunities to strengthn our security posture in a continuous journey with an ongoing commitment
15 to ensure this remains top-of-mind. As part of our incident response, we have implemented a
16 number of these identified enhancements to our security posture and have continued to progress a
17 multipronged approach. We’ve deployed new tools, revised policies and enforcement procedures,
18 and implemented an advanced around-the-clock managed detections and response service for
19 proactive threat monitoring.”

20 **C. DOE DEFENDANTS**

21 14. The true names and capacities, whether individual, corporate, associate, or otherwise,
22 of Defendants sued herein as Doe Defendants 1 through 100, inclusive, are currently unknown to
23 Plaintiff, who therefore sue the Defendants by such fictitious names under the Code of Civil
24 Procedure § 474. Each of the Defendants designated herein as a Doe Defendant is legally
25 responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of
26 court and/or amend this complaint to reflect the true names and capacities of the Defendants
27 designated hereinafter as Doe Defendants 1 through 100 when such identities become known. Any
28

1 reference made to a named Defendant by specific name or otherwise, individually or plural, is also
2 reference to the actions or inactions of Doe Defendants 1 through 100, inclusive.

3 **D. AGENCY/AIDING AND ABETTING**

4 15. At all times herein mentioned, Defendants, and each of them, were an agent or joint
5 venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the
6 course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the
7 acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized
8 the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

9 16. Defendants, and each of them, aided and abetted, encouraged and rendered
10 substantial assistance to the other Defendants in breaching their obligations to Plaintiff and the
11 Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially
12 assist the commissions of these wrongful acts and other wrongdoings complained of, each of the
13 Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its
14 conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals,
15 and wrongdoing.

16 **FACTUAL ALLEGATIONS**

17 17. As a result, at all times relevant to this action, including the period from October 22,
18 2020 to December 3, 2020, HCP possessed Plaintiff's and the Class' medical information, in
19 electronic and physical form, in possession of or derived from Defendant regarding their medical
20 history, mental or physical condition, or treatment. Such medical information included or contained
21 an element of personal identifying information sufficient to allow identification of Plaintiff and the
22 Class, such as their names, date of birth, addresses, medical record numbers, insurance provider,
23 electronic mail addresses, telephone numbers, or social security numbers, or other information that,
24 alone or in combination with other publicly available information, reveals their identity. At all
25 times relevant to this action, including the period from October 22, 2020 to December 3, 2020, HCP
26 maintained and continues to maintain "medical information," within the meaning of Civil Code §
27 56.05(j), of Plaintiff and the Class, each of which are "patients" within the meaning of Civil Code §
28 56.05(k).

1 18. As a result, at all times relevant to this action, including the period from October 22,
2 2020 to December 3, 2020, NH possessed Plaintiff’s and the SubClass’ medical information, in
3 electronic and physical form, in possession of or derived from Defendant regarding their medical
4 history, mental or physical condition, or treatment. Such medical information included or contained
5 an element of personal identifying information sufficient to allow identification of Plaintiff and the
6 SubClass, such as their names, date of birth, addresses, medical record numbers, insurance provider,
7 electronic mail addresses, telephone numbers, or social security numbers, or other information that,
8 alone or in combination with other publicly available information, reveals their identity. At all
9 times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH
10 maintained and continues to maintain “medical information,” within the meaning of Civil Code §
11 56.05(j), of Plaintiff and the SubClass, each of which are “patients” within the meaning of Civil
12 Code § 56.05(k). At all times relevant to this action, including the period from October 22, 2020 to
13 December 3, 2020, NH was and is a “provider of health care” within the meaning of Civil Code §
14 56.05(m). At all times relevant to this action, including the period from October 22, 2020 to
15 December 3, 2020, Plaintiff and SubClass members were patients, within the meaning of Civil Code
16 § 56.05(k).

17 19. As a result, at all times relevant to this action, including the period from October 22,
18 2020 to December 3, 2020, NETGAIN possessed Plaintiff’s, the SubClass’ and the Class’ medical
19 information, in electronic and physical form, in possession of or derived from Defendant regarding
20 their medical history, mental or physical condition, or treatment. Such medical information
21 included or contained an element of personal identifying information sufficient to allow
22 identification of Plaintiff, the SubClass and the Class, such as their names, date of birth, addresses,
23 medical record numbers, insurance provider, electronic mail addresses, telephone numbers, or social
24 security numbers, or other information that, alone or in combination with other publicly available
25 information, reveals their identity. At all times relevant to this action, including the period from
26 October 22, 2020 to December 3, 2020, NETGAIN maintained and continues to maintain “medical
27 information,” within the meaning of Civil Code § 56.05(j), of Plaintiff and the Class, each of which
28 are “patients” within the meaning of Civil Code § 56.05(k).

1 20. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, pursuant to Civil Code § 56.06(a), HCP, as a business that created, maintained,
3 preserved, and stored records of the care, products and services that Plaintiff and the Class members
4 received in the State of California from HCP’s over 16 member community health centers, 140
5 member practice sites, 857,757 patients served, and/or other providers of health care, health care
6 service plans, pharmaceutical companies, and contractors, as defined by the Act, is and was
7 organized for the purpose of maintaining medical information, within the meaning of Civil Code §
8 56.05(j), in order to make the information available to Plaintiff and the Class members or to a
9 provider of health care at the request of Plaintiff and the Class members or a provider of health care,
10 for purposes of allowing Plaintiff and the Class members to manage their information, or for the
11 diagnosis and treatment of Plaintiff and the Class members, is and was deemed to be a “provider of
12 health care,” within the meaning of Civil Code § 56.05(m).

13 21. Alternatively, at all times relevant to this action, including the period from October
14 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), HCP, as an entity that is a
15 medical group, independent practice association, pharmaceutical benefits manager, or a medical
16 service organization, and is not a health care service plan or provider of health care to Plaintiff and
17 the Class members, is and was a “contractor” under Civil Code § 56.05(d).

18 22. Alternatively, at all times relevant to this action, including the period from October
19 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, HCP is and was a recipient of
20 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
21 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
22 further disclosing that medical information except in accordance with a new authorization that
23 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
24 of this chapter or by law.

25 23. Alternatively, at all times relevant to this action, including the period from October
26 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, HCP is and was a recipient of
27 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
28 the Act, and was prohibited from further disclosing such medical information unless in accordance

1 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
2 permitted by other provisions of this chapter or by law.

3 24. Additionally, at all times relevant to this action, including prior to the period from
4 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), HCP is and was an entity
5 engaged in the business of furnishing administrative services to programs that provide payment for
6 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
7 or permitting its employees or agents to use or disclose Plaintiff's and the Class members' medical
8 information possessed in connection with performing administrative functions for a program, except
9 as reasonably necessary in connection with the administration or maintenance of the program, or as
10 required by law, or with an authorization.

11 25. As a provider of health care, a contractor, and/or other authorized recipient of
12 personal and confidential medical information, HCP is required by the Act to ensure that medical
13 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
14 patients' authorization, and to protect and preserve the confidentiality of the medical information
15 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

16 26. At all times relevant to this action, including the period from October 22, 2020 to
17 December 3, 2020, pursuant to Civil Code § 56.06(a), NH, as a business that created, maintained,
18 preserved, and stored records of the care, products and services that Plaintiff and the Class members
19 received in the State of California from NH and/or other providers of health care, health care service
20 plans, pharmaceutical companies, and contractors, as defined by the Act, is and was organized for
21 the purpose of maintaining medical information, within the meaning of Civil Code § 56.05(j), in
22 order to make the information available to Plaintiff and the Class members or to a provider of health
23 care at the request of Plaintiff and the Class members or a provider of health care, for purposes of
24 allowing Plaintiff and the Class members to manage their information, or for the diagnosis and
25 treatment of Plaintiff and the Class members, is and was deemed to be a "provider of health care,"
26 within the meaning of Civil Code § 56.05(m).

27 27. Alternatively, at all times relevant to this action, including the period from October
28 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), NH, as an entity that is a medical

1 group, independent practice association, pharmaceutical benefits manager, or a medical service
2 organization, and is not a health care service plan or provider of health care to Plaintiff and the
3 Class members, is and was a “contractor” under Civil Code § 56.05(d).

4 28. Alternatively, at all times relevant to this action, including the period from October
5 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NH is and was a recipient of
6 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
7 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
8 further disclosing that medical information except in accordance with a new authorization that
9 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
10 of this chapter or by law.

11 29. Alternatively, at all times relevant to this action, including the period from October
12 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NH is and was a recipient of
13 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
14 the Act, and was prohibited from further disclosing such medical information unless in accordance
15 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
16 permitted by other provisions of this chapter or by law.

17 30. Additionally, at all times relevant to this action, including prior to the period from
18 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), NH is and was an entity
19 engaged in the business of furnishing administrative services to programs that provide payment for
20 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
21 or permitting its employees or agents to use or disclose Plaintiff’s and the Class members’ medical
22 information possessed in connection with performing administrative functions for a program, except
23 as reasonably necessary in connection with the administration or maintenance of the program, or as
24 required by law, or with an authorization.

25 31. As a provider of health care, a contractor, and/or other authorized recipient of
26 personal and confidential medical information, NH is required by the Act to ensure that medical
27 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
28

1 patients' authorization, and to protect and preserve the confidentiality of the medical information
2 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

3 32. At all times relevant to this action, including the period from October 22, 2020 to
4 December 3, 2020, pursuant to Civil Code § 56.06(a), NETGAIN, as a business that created,
5 maintained, preserved, and stored records of the care, products and services that Plaintiff and the
6 Class members received in the State of California from NH and/or other providers of health care,
7 health care service plans, pharmaceutical companies, and contractors, as defined by the Act, is and
8 was organized for the purpose of maintaining medical information, within the meaning of Civil
9 Code § 56.05(j), in order to make the information available to Plaintiff and the Class members or to
10 a provider of health care at the request of Plaintiff and the Class members or a provider of health
11 care, for purposes of allowing Plaintiff and the Class members to manage their information, or for
12 the diagnosis and treatment of Plaintiff and the Class members, is and was deemed to be a "provider
13 of health care," within the meaning of Civil Code § 56.05(m).

14 33. Alternatively, at all times relevant to this action, including the period from October
15 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NETGAIN is and was a recipient of
16 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
17 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
18 further disclosing that medical information except in accordance with a new authorization that
19 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
20 of this chapter or by law.

21 34. Alternatively, at all times relevant to this action, including the period from October
22 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NETGAIN is and was a recipient
23 of medical information of Plaintiff and the Class members pursuant to an authorization as provided
24 by the Act, and was prohibited from further disclosing such medical information unless in
25 accordance with a new authorization that meets the requirements of Section 56.21, or as specifically
26 required or permitted by other provisions of this chapter or by law.

27 35. As a provider of health care and/or other authorized recipient of personal and
28 confidential medical information, NETGAIN is required by the Act to ensure that medical

1 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
2 patients' authorization, and to protect and preserve the confidentiality of the medical information
3 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

4 36. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, HCP created, maintained, preserved, and stored records of the care, services and
6 products, including the names, addresses, dates of birth, diagnosis/treatment information and
7 treatment cost information of Plaintiff and the Class (all of which constitutes medical information,
8 as that term is defined and set forth in the Act), that Plaintiff and other Class members received in
9 the State of California from NH and other HCP providers of health care on its computer server.

10 37. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, NH created, maintained, preserved, and stored records of the care, services and
12 products, including the names, addresses, dates of birth, diagnosis/treatment information and
13 treatment cost information of Plaintiff and the SubClass (all of which constitutes medical
14 information, as that term is defined and set forth in the Act), that Plaintiff and other SubClass
15 members received in the State of California from NH on its computer network.

16 38. As a result, on or before October 30, 2020, Defendants possessed Plaintiff's,
17 SubClass' and the Class' medical information, in electronic and physical form, in possession of or
18 derived from Defendants regarding their medical history, mental or physical condition, or treatment.
19 Such medical information included or contained an element of personal identifying information
20 sufficient to allow identification of Plaintiff, the SubClass and the Class, such as their names,
21 addresses, dates of birth, social security numbers, phone numbers and/or email addresses, or other
22 information that, alone or in combination with other publicly available information, reveals their
23 identity.

24 39. As providers of health care, contractors, and/or other recipients of medical
25 information, Defendants are required by the Act to ensure that medical information regarding a
26 patient is not disclosed or disseminated or released without their patients' authorization, and to
27 protect and preserve the confidentiality of the medical information regarding a patient, under Civil
28 Code §§ 56.10, 56.26, 56.36, and 56.101.

1 40. As providers of health care, contractors, and/or other recipients of medical
2 information, Defendants are required by the Act not to disclose medical information regarding a
3 patient without first obtaining an authorization under Civil Code §§ 56.10 and 56.26.

4 41. As providers of health care, contractors, and/or other recipients of medical
5 information, Defendants are required by the Act to create, maintain, preserve, and store medical
6 information in a manner that preserves the confidentiality of the information contained therein
7 under Civil Code § 56.101(a).

8 42. As providers of health care, contractors, and/or other recipients of medical
9 information, Defendants are required by the Act to protect and preserve confidentiality of electronic
10 medical information of Plaintiff and the Class in its possession under Civil Code § 56.101(b)(1)(A).

11 43. As providers of health care, contractors, and/or other recipients of medical
12 information, Defendants are required by the Act to take appropriate preventive actions to protect the
13 confidential information or records against release consistent with Defendants' obligations under
14 the Act, under Civil Code § 56.36(e)(2)(E), or other applicable state law, and the Health Insurance
15 Portability and Accountability Act of 1996 (Public Law 104-191) (HIPAA) and all HIPAA
16 Administrative Simplification Regulations in effect on January 1, 2012, contained in Parts 160, 162,
17 and 164 of Title 45 of the Code of Federal Regulations, and Part 2 of Title 42 of the Code of
18 Federal Regulations, including, but not limited to, all of the following:

- 19 i. Developing and implementing security policies and procedures.
- 20 ii. Designating a security official who is responsible for developing and implementing
21 its security policies and procedures, including educating and training the workforce.
- 22 iii. Encrypting the information or records, and protecting against the release or use of
23 the encryption key and passwords, or transmitting the information or records in a
24 manner designed to provide equal or greater protections against improper
25 disclosures.

26 44. At all times relevant to this action, including the period from October 22, 2020 to
27 December 3, 2020, HCP created, maintained, preserved, and stored Plaintiff's and the Class
28 members' medical information in an un-encrypted format.

1 45. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, NH created, maintained, preserved, and stored Plaintiff’s and the SubClass
3 members’ medical information in an un-encrypted format.

4 46. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, NH disclosed and/or delivered Plaintiff’s and the SubClass members’ medical
6 information to HCP and NETGAIN. At all times relevant to this action, NH did not obtain written
7 authorization from the Plaintiff and the SubClass prior to disclosing and/or delivering Plaintiff’s and
8 the SubClass members’ medical information to HCP and NETGAIN. Furthermore, NH’s disclosure
9 of and/or delivery of Plaintiff’s and the SubClass members’ medical information to HCP and
10 NETGAIN was not permissible without written authorization from the Plaintiff and the SubClass or
11 under any exemption under Civil Code § 56.10(c).

12 47. At all times relevant to this action, including the period from October 22, 2020 to
13 December 3, 2020, HCP created, maintained, preserved, stored, disclosed and/or delivered
14 Plaintiff’s and the Class members’ medical information to NETGAIN on its computer servers. At
15 all times relevant to this action, HCP did not obtain written authorization from the Plaintiff and the
16 Class prior to creating, maintaining, preserving, storing, disclosing and/or delivering Plaintiff’s and
17 the Class members’ medical information to NETGAIN on its computer servers. Furthermore,
18 NETGAIN’s disclosure of and/or delivery of Plaintiff’s and the Class members’ medical
19 information to NETGAIN on its computer servers was not permissible without written authorization
20 from the Plaintiff and the Class or under any exemption under Civil Code § 56.10(c).

21 48. By law, the HIPAA Privacy Rule applies only to covered entities, e.g. health care
22 providers. However, most health care providers do not carry out all of their health care activities
23 and functions by themselves. Instead, they often use the services of a variety of other persons or
24 businesses. The Privacy Rule allows covered providers to disclose protected health information
25 (PHI) to these “business associates” if the providers obtain assurances that the business associate
26 will use the information only for the purposes for which it was engaged by the covered entity, will
27 safeguard the information from misuse, and will help the covered entity comply with some of the
28 covered entity’s duties under the Privacy Rule. Covered entities may disclose PHI to an entity in its

1 role as a business associate only to help the covered entity carry out its health care functions – not
2 for the business associate’s independent use or purposes, except as needed for the proper
3 management and administration of the business associate. The Privacy Rule requires that a covered
4 entity obtain assurances from its business associate that the business associate will appropriately
5 safeguard the PHI it receives or creates on behalf of the covered entity. The satisfactory assurances
6 must be in writing, whether in the form of a contract or other agreement between the covered entity
7 and the business associate.

8 49. When hiring and monitoring a service provider or business associate such as
9 NETGAIN, HCP and NH knew or should have known that they had a duty to inquire about
10 potential service providers’ and business associates’ cybersecurity programs and how such
11 programs are maintained. HCP and NH knew or should have known that they had a duty to
12 compare potential service providers’ and business associates’ cybersecurity programs to the
13 industry standards adopted by other healthcare providers, and should evaluate potential service
14 providers’ track records in the industry by reviewing public information about data security
15 incidents and litigation. HCP and NH knew or should have known that they had a duty to also ask
16 potential service providers and business associates about whether they have experienced any
17 cybersecurity incidents and how such incidents were handled, as well as whether the potential
18 service provider has an insurance policy in place that would cover losses caused by cybersecurity
19 breaches (including losses caused by internal and external threats). HCP and NH knew or should
20 have known that they had a duty to review service provider and business associates contracts to
21 ensure that the contracts require the service providers to comply, on an ongoing basis, with
22 cybersecurity and information security standards (and avoid contract provisions that limit service
23 providers’ responsibility for cybersecurity and information technology breaches). Finally, HCP and
24 NH knew or should have known that they had a duty to pay particular attention to contract terms
25 relating to confidentiality, the use and sharing of information, notice by the vendor of cybersecurity
26 risk assessments and audit reports, cybersecurity breaches and records retention and destruction.

27 50. Alternatively, Plaintiff alleges on information and belief that HCP’s and NH’s
28 disclosure of and/or delivery of Plaintiff’s, the Class’ and the SubClass’ medical information to

1 NETGAIN was either without a business associate agreement or pursuant to a business associate
2 agreement that was not permissible under the Privacy Rule or any exemption under Civil Code §
3 56.10(c), and/or because HCP and NH negligently failed to obtain reasonable assurances and
4 negligently failed to monitor and conduct assessments of NETGAIN to verify that NETGAIN
5 would comply with HIPAA privacy regulations and to follow guidelines and policies to maintain
6 the privacy, confidentiality, including by encryption, and otherwise reasonably protect Plaintiff’s
7 and the Class’ medical information from disclosure and/or release to at least one unauthorized third
8 party “user” prior to and after HCP’s and NH’s disclosure of and/or delivery of Plaintiff’s and the
9 Class members’ medical information to NETGAIN.

10 51. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, at least one “unauthorized third party gained access to Netgain’s digital
12 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
13 obtained certain files” containing including Plaintiff’s, the SubClass’ and the Class’ medical
14 information (i.e., their names, addresses, dates of birth, diagnosis/treatment information and
15 treatment cost information) that was located on a NETGAIN server in an un-encrypted format, as
16 represented in HCP’s “**Notice of Data Breach**” form letter submitted to the Attorney General of the
17 State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**.

18 52. Defendants had the resources necessary to protect and preserve confidentiality of
19 electronic medical information of Plaintiff, the SubClass and the Class in their possession, but
20 neglected to adequately implement data security measures as required by HIPPA and the Act,
21 despite their obligation to do so.

22 53. Additionally, the risk of vulnerabilities in its computer and data systems of being
23 exploited by an unauthorized third party trying to steal Plaintiff’s, the SubClass’ and the Class’
24 electronic personally identifying and medical information was foreseeable and/or known to
25 Defendants. The California Data Breach Report 2012-2015, issued in February 2016 by Attorney
26 General, Kamala D. Harris, reported, “Malware and hacking presents the greatest threat, both in the
27 number of breaches and the number of records breached” and “Social Security numbers and
28 medical information – was breached than other data types.” Moreover, as Attorney General further

1 reported, just because “[e]xternal adversaries cause most data breaches, [] this does not mean that
2 organizations are solely victims; they are also stewards of the data they collect and maintain. People
3 entrust businesses and other organizations with their data on the understanding that the
4 organizations have a both an ethical and a legal obligation to protect it from unauthorized access.
5 Neglecting to secure systems and data opens a gateway for attackers, who take advantage of
6 uncontrolled vulnerabilities.” Regarding encryption, Attorney General instructed in California Data
7 Breach Report 2012-2015, “As we have said in the past, breaches of this type are preventable.
8 Affordable solutions are widely available: strong full-disk encryption on portable devices and
9 desktop computers when not in use.[] Even small businesses that lack full time information security
10 and IT staff can do this. They owe it to their patients, customers, and employees to do it now.”

11 54. More recently the HIPAA Journal posted on November 1, 2018 warned, “Healthcare
12 organization[s] need to ensure that their systems are well protected against cyberattacks, which
13 means investing in technologies to secure the network perimeter, detect intrusions, and block
14 malware and phishing threats.”

15 55. Further, it also was foreseeable and/or known to Defendants that negligently
16 creating, maintaining, preserving, and/or storing Plaintiff’s, the SubClass’ and the Class’ medical
17 and personal identifying information, in electronic form, onto Defendants’ computer networks in a
18 manner that did not preserve the confidentiality of the information could have a devastating effect
19 on them. As reported in the California Data Breach Report 2012-2015, “There are real costs to
20 individuals. Victims of a data breach are more likely to experience fraud than the general public,
21 according to Javelin Strategy & Research. In 2014, 67 percent of breach victims in the U.S. were
22 also victims of fraud, compared to just 25 percent of all consumers.”

23 56. To be successful, phishing relies on a series of affirmative acts by a company and its
24 employees such as clicking a link, downloading a file, or providing sensitive information. Once
25 criminals gained access to the email accounts of a company and its employees, the email servers
26 communicated—that is, disclosed—the contents of those accounts to the criminals. “Phishing
27 scams are one of the most common ways hackers gain access to sensitive or confidential
28 information. Phishing involves sending fraudulent emails that appear to be from a reputable

1 company, with the goal of deceiving recipients into either clicking on a malicious link or
2 downloading an infected attachment, usually to steal financial or confidential information.”
3 (<https://www.varonis.com/blog/data-breach-statistics/>). As posted on April 21, 2020, the FBI had
4 issued a fresh warning [Alert Number MI-000122-MW] following an increase in COVID-19
5 phishing scams targeting healthcare providers.

6 57. At all times relevant to this action, including the period from October 22, 2020 to
7 December 3, 2020, Defendants negligently created, maintained, preserved, and/or stored Plaintiff’s,
8 the SubClass’ and the Class’ medical information, including Plaintiff’s, the SubClass’ and the
9 Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
10 information, in electronic form, onto Defendants’ computer networks in a manner that did not
11 preserve the confidentiality of the information, and negligently failed to protect and preserve
12 confidentiality of electronic medical information of Plaintiff, the SubClass and the Class in their
13 possession, as required by HIPPA and the Act, and specifically, under Civil Code §§ 56.10(a),
14 56.26(a), 56.36(e)(2)(E), 56.101(a), and 56.101(b)(1)(A), and according to their written
15 representations to Plaintiff and the Class.

16 58. Had Defendants taken such appropriate preventive actions, fix the deficiencies in
17 their data security systems and adopted security measures as required by HIPPA and the Act from
18 October 22, 2020 to December 3, 2020, Defendants could have prevented Plaintiff’s and the Class’
19 electronic medical information within Defendants’ computer networks from being accessed and
20 actually viewed by unauthorized third parties.

21 59. At all times relevant to this action, including the period of from October 22, 2020 to
22 December 3, 2020, NH, by disclosing and/or delivering Plaintiff’s and the SubClass’ personal
23 identifying and medical information to HCP, allowed Plaintiff’s and the SubClass’ personal
24 identifying and medical information to be accessed and actually viewed by at least one unauthorized
25 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
26 Code § 56.10(a).

27 60. At all times relevant to this action, including the period of from October 22, 2020 to
28 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic

1 medical information of Plaintiff and the SubClass on NETGAIN’s computer server, allowed
2 Plaintiff’s and the SubClass’ medical and personal identifying information to be accessed and
3 actually viewed by at least one unauthorized third party, without first obtaining an authorization,
4 constituting a disclosure in violation of Civil Code § 56.10(a).

5 61. At all times relevant to this action, including the period from October 22, 2020 to
6 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
7 medical information of Plaintiff and the Class on NETGAIN’s computer server, allowed Plaintiff’s
8 and the Class’ medical and personal identifying information to be accessed and actually viewed by
9 at least one unauthorized third party, without first obtaining an authorization, constituting a
10 disclosure in violation of Civil Code § 56.10(a).

11 62. At all times relevant to this action, including the period from October 22, 2020 to
12 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
13 medical information of Plaintiff and the Class on NETGAIN’s computer server, allowed Plaintiff’s
14 and the Class’ medical and personal identifying information to be accessed and actually viewed by
15 at least one unauthorized third party, without first obtaining an authorization, constituting a
16 disclosure in violation of Civil Code § 56.26(a).

17 63. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, NH, by disclosing and/or delivering Plaintiff’s and the SubClass members’
19 medical and personal identifying information to HCP, allowed Plaintiff’s and the SubClass’ medical
20 and personal identifying information to be accessed and actually viewed by at least one
21 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

22 64. At all times relevant to this action, including the period from October 22, 2020 to
23 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic
24 medical information of Plaintiff and the SubClass on NETGAIN’s computer server, allowed
25 Plaintiff’s and the SubClass’ medical and personal identifying information to be accessed and
26 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
27 Code § 56.101(a).

28

1 65. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
3 medical information of Plaintiff and the Class on NETGAIN’s computer server, allowed Plaintiff’s
4 and the Class’ medical and personal identifying information to be accessed and actually viewed by
5 at least one unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

6 66. At all times relevant to this action, including the period from October 22, 2020 to
7 December 3, 2020, NH, by disclosing and/or delivering Plaintiff’s and the SubClass members’
8 medical and personal identifying information to HCP, allowed Plaintiff’s and the SubClass’ medical
9 and personal identifying information to be accessed and actually viewed by at least one
10 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

11 67. At all times relevant to this action, including the period from October 22, 2020 to
12 December 3, 2020, NH’s negligent failure to protect and preserve confidentiality of electronic
13 medical information of Plaintiff and the SubClass, on NETGAIN’s computer server, allowed
14 Plaintiff’s and the SubClass’ medical and personal identifying information to be accessed and
15 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
16 Code § 56.101(b)(1)(A).

17 68. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, HCP’s negligent failure to protect and preserve confidentiality of electronic
19 medical information of Plaintiff and the Class, on NETGAIN’s computer server, allowed Plaintiff’s
20 and the Class’ medical and personal identifying information to be accessed and actually viewed by
21 at least one unauthorized third party, constituting a release in violation of Civil Code §
22 56.101(b)(1)(A).

23 69. On or about April 12, 2021, HCP caused a form letter, entitled “**Notice of Data**
24 **Breach,**” dated April 12, 2021, signed by Henry Tuttle, President & Chief Executive Officer,
25 Health Center Partners of Southern California, to be mailed to Plaintiff and the Class, informing
26 them, in part, of “a recent data security incident experienced by Netgain Technology, LLC
27 (‘Netgain’), the IT service provider for Health Center Partners of Southern California (‘HCP’)” and
28 stating, in part, “HCP supports community health centers in a variety of ways, including

1 collaborative grant-funded programs and services for Neighborhood Healthcare.... **What**
2 **Happened:** Netgain recently informed HCP that it had experienced a data security incident that
3 involved systems containing HCP data.... According to Netgain, in late September 2020, an
4 unauthorized third party gained access to Netgain’s digital environment, and between October 22,
5 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data.
6 Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the
7 attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the
8 data.... The information involved varies depending on the individual but may include the following:
9 name, address, date of birth, diagnosis/treatment information and treatment cost information. Once
10 we learned that HCP data may have been involved in the incident, we worked with our
11 cybersecurity experts to review the impacted files and identify the individuals whose information
12 was contained in such files so that we may notify such individuals. Our investigation revealed that
13 the impacted files contained your personal information.” An exemplar of HCP’s “**Notice of Data**
14 **Breach**” form letter submitted to the Attorney General of the State of California and mailed to
15 Plaintiff and the Class is attached hereto as **Exhibit A**. Plaintiff received in the mail a HCP “**Notice**
16 **of Data Breach**” form letter, addressed to her, which alerted Plaintiff that her medical and personal
17 identifying information, along with other Class members, was improperly accessed by at least one
18 unauthorized third party. As a result, Plaintiff fears that disclosure and/or release of her medical
19 and personal identifying information created, maintained, preserved, and/or stored on Defendants’
20 computer networks could subject her to harassment or abuse. Moreover, although thereafter, on
21 May 4, 2021, Plaintiff wrote both HCP and NH separately requesting further information about this
22 security incident, neither HCP nor NH provided a substantive response to her requests.

23 70. HCP’s “**Notice of Data Breach**” form letter submitted to the Attorney General of
24 the State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**, further
25 states, “**What We Are Doing:** [] We are providing you with steps that you can take to help protect
26 your personal information, and as an added precaution, we are offering you complimentary identity
27 protection services through IDX, a leader in risk mitigation and response.”

28

1 71. HCP’s “**Notice of Data Breach**” form letter concludes by making the following
2 hollow gesture, “The security of your information is a top priority for HCP, and we are committed
3 to safeguarding your data and privacy.” Other than offering “steps that you can take to help protect
4 your personal information” and “complimentary identity protection services through IDX” “as an
5 added precaution,” HCP’s “**Notice of Data Breach**” form letter does nothing to further protect
6 Plaintiff and the Class from future incidents of identity theft despite the severity of the unauthorized
7 access, viewing, exfiltration, theft, disclosure and/or release of their electronic medical and personal
8 information caused by Defendants’ violations of their duty to implement and maintain reasonable
9 security procedures and practices.

10 72. To date, other than offering “steps that you can take to help protect your personal
11 information” and “complimentary identity protection services through IDX” “as an added
12 precaution,” HCP has not offered any monetary compensation for the unauthorized disclosure
13 and/or release of Plaintiff’s and the Class’ electronic medical information under the Act. In effect,
14 HCP is shirking its responsibility for the harm it has caused, while shifting the burdens and costs of
15 its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

16 73. To date, NH has not offered any compensation for the unauthorized disclosure and/or
17 release of Plaintiff’s and SubClass’ electronic medical information under the Act. In effect, NH is
18 shirking its responsibility for the harm it has caused, while shifting the burdens and costs of its
19 wrongful conduct onto its patients, i.e. Plaintiff and the SubClass.

20 74. To date, NETGAIN has not offered any monetary compensation for the unauthorized
21 disclosure and/or release of Plaintiff’s and the Class’ electronic medical information under the Act.
22 In effect, NETGAIN is shirking its responsibility for the harm it has caused, while shifting the
23 burdens and costs of its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

24 75. Based upon the information posted on the U.S. Department of Health and Human
25 Services’ official website, HCP reported on “04/09/2021” a “Hacking/IT Incident” involving
26 “Network Server” affecting “293,516” persons, which involved a “Business Associate,” to the U.S.
27 Department of Health & Human Services’ Office for Civil Rights.

28

1 76. Based upon the information posted on the U.S. Department of Health and Human
2 Services’ official website, NH reported on “04/14/2021” a “Hacking/IT Incident” involving
3 “Network Server” affecting “45,200” persons, which involved a “Business Associate,” to the U.S.
4 Department of Health & Human Services’ Office for Civil Rights.

5 77. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA
6 covered entities to provide notification following a breach of unsecured protected health
7 information. Following a breach of unsecured protected health information, covered entities must
8 provide notification of the breach to affected individuals. Covered entities must *only* provide the
9 required notifications if the breach involved unsecured protected health information. Unsecured
10 protected health information is protected health information (PHI) that has not been rendered
11 unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or
12 methodology specified by the Secretary of the U.S. Department of Health and Human Services in
13 guidance. Under approved guidance of the U.S. Department of Health and Human Services, PHI is
14 rendered unusable, unreadable, or indecipherable to unauthorized individuals if (1) electronic PHI
15 has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process
16 to transform data into a form in which there is a low probability of assigning meaning without use
17 of a confidential process or key” (45 CFR 164.304 definition of encryption) and (2) such
18 confidential process or key that might enable decryption has not been breached. By reporting this
19 incident to the U.S. Department of Health and Human Services, HCP and NH each has separately
20 determined and is affirming that Plaintiff’s, the Class’ and the SubClass’ electronic PHI was either
21 not encrypted at all, or if it was encrypted, the encryption has been breached by the unauthorized
22 third party. Further, because Plaintiff’s, the Class’ and the SubClass’ identifiable medical
23 information contained in NETGAIN’s computer server was not rendered unusable, unreadable, or
24 indecipherable, the unauthorized third party or parties who “obtained” and downloaded Plaintiff’s
25 and the Class’ identifiable medical information was able to and did actually view Plaintiff’s, the
26 Class’ and the SubClass’ electronic medical information contained in and “obtained” and
27 downloaded from NETGAIN’s computer server. As a result, HCP and NH each has separately
28 determined and have affirmed that Plaintiff’s, the Class’ and the SubClass’ identifiable medical

1 information contained in NETGAIN’s computer server was unencrypted and thus, the unauthorized
2 third party or parties who “obtained” and downloaded Plaintiff’s, the Class’ and the SubClass’
3 identifiable medical information was able to and did actually view Plaintiff’s, the Class’ and the
4 SubClass’ electronic medical information contained in and “obtained” and downloaded from
5 NETGAIN’s computer server. Therefore, HCP, NH and NETGAIN was negligent for failing to
6 encrypt or adequately encrypt Plaintiff’s, the Class’ and the SubClass’ electronic medical
7 information contained in NETGAIN’s computer server.

8 78. As a result, Defendants were negligent for failing to encrypt or adequately encrypt
9 Plaintiff’s, the Class’ and the SubClass’ electronic medical information on their computer networks.
10 Further, because Plaintiff’s, the Class’ and the SubClass’ identifiable medical information on
11 Defendants’ computer networks was not rendered unusable, unreadable, or indecipherable, the
12 unauthorized third party or parties who accessed Plaintiff’s, the Class’ and the SubClass’
13 identifiable medical information was able to and did view Plaintiff’s, the Class’ and the SubClass’
14 electronic medical information contained within NETGAIN’s computer server.

15 **CLASS ACTION ALLEGATIONS**

16 79. Plaintiff brings this action on behalf of herself individually and on behalf of all
17 others similarly situated. The putative class and subclass that Plaintiff seeks to represent is defined
18 as follows:

19 Class: All persons to whom Health Center Partners of Southern California sent a
20 notification letter of a data security incident that has occurred between October
21 22, 2020 to December 3, 2020, an exemplar of which is attached hereto as
Exhibit A.

22 SubClass: All persons to whom Neighborhood Healthcare sent a notification
23 letter of a data security incident that has occurred between November 24, 2020 to
December 3, 2020, an exemplar of which is attached hereto as **Exhibit B**.

24 The officers, directors, employees, and agents of Defendants and any “affiliate,” “principal” or
25 “subsidiary” of Defendants, as defined in the Corporations Code §§ 150, 175, and 189, respectively,
26 are excluded from the Class and the SubClass. Plaintiff reserves the right under California Rule of
27 Court 3.765 to amend or modify the Class definition with greater particularity or further division
28

1 into subclasses or limitation to particular issues as warranted, and as additional facts are discovery
2 by Plaintiff during her future investigations.

3 80. This action is properly maintainable as a class action. The members of the Class and
4 the SubClass are so numerous that joinder of all members is impracticable, if not completely
5 impossible. While the exact number of the Class is unknown to Plaintiff at this time, HCP filed a
6 report with the U.S. Department of Health & Human Services' Office for Civil Rights, on or about
7 December 28, 2020, that this incident affected 293,516 persons. The disposition of the claims of
8 the members of Class through this class action will benefit both the parties and this Court. In
9 addition, the Class and the SubClass is readily identifiable from information and records in the
10 possession of Defendants and their agents, and the Class and the SubClass is defined in objective
11 terms that make the eventual identification of the Class and the SubClass members possible and/or
12 sufficient to allow members of the Class and the SubClass identify themselves as having a right to
13 recover.

14 81. There is a well-defined community of interest among the members of the Class and
15 the SubClass because common questions of law and fact predominate, Plaintiff's claims are typical
16 of the members of the class, and Plaintiff can fairly and adequately represent the interests of the
17 Class.

18 82. Common questions of law and fact exist as to all members of the Class and the
19 SubClass and predominate over any questions affecting solely individual members of the Class and
20 the SubClass. Among the questions of law and fact common to the Class that predominate over
21 questions which may affect individual Class members, including the following:

- 22 a) Whether Defendants possessed Plaintiff's, the SubClass' and the Class' medical and
23 personal identifying information from October 22, 2020 to December 3, 2020;
24 b) Whether Defendants created, maintained, preserved and/or stored Plaintiff's, the
25 SubClass' and the Class' medical and personal identifying information, in electronic
26 form, onto Defendants' computer networks from October 22, 2020 to December 3,
27 2020;

- 1 c) Whether Defendants implemented and maintained reasonable security procedures
2 and practices to protect Plaintiff's, the SubClass' and the Class' medical and
3 personal identifying information, in electronic form, within Defendants' computer
4 networks from October 22, 2020 to December 3, 2020;
- 5 d) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
6 information, in electronic form, within Defendants' computer networks from October
7 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
8 exposed by an unauthorized third party;
- 9 e) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
10 information, in electronic form, within Defendants' computer networks from October
11 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
12 exposed by an unauthorized third party without the prior written authorization of
13 Plaintiff, the SubClass and the Class, as required by Civil Code §§ 56.10 and 56.26;
- 14 f) Whether Defendants' creation, maintenance, preservation and/or storage of
15 Plaintiff's, the SubClass' and the Class' medical and personal identifying
16 information, in electronic form, within Defendants' computer networks, accessed,
17 viewed, exfiltrated and/or publicly exposed by an unauthorized third party was
18 permissible without written authorization from Plaintiff, the SubClass and the Class
19 or under any exemption under Civil Code § 56.10(c);
- 20 g) Whether Defendants' creation, maintenance, preservation and/or storage of
21 Plaintiff's, the SubClass' and the Class' medical and personal identifying
22 information, in electronic form, within Defendants' computer networks, accessed,
23 viewed, exfiltrated and/or publicly exposed by an unauthorized third party
24 constitutes a release in violation of Civil Code §56.101;
- 25 h) Whether the timing of HCP's notice that Plaintiff's and the Class' medical and
26 personal identifying information, in electronic form, was accessed, viewed,
27 exfiltrated and/or publicly exposed by an unauthorized third party, was given in the
28 most expedient time possible and without reasonable delay;

- 1 i) Whether Defendants' conduct constitute unlawful, fraudulent or unfair practices in
- 2 violation of Business and Professions Code §§ 17200, *et seq.*; and
- 3 j) Whether Plaintiff, the SubClass and the Class are entitled to actual, nominal or
- 4 statutory damages, injunctive relief and/or restitution.

5 83. Plaintiff's claims are typical of those of the other SubClass and Class members
6 because Plaintiff, like every other SubClass and Class member, were exposed to virtually identical
7 conduct and now suffer from the same violations of the law as other SubClass and Class members.

8 84. Plaintiff will fairly and adequately protect the interests of the SubClass and the
9 Class. Moreover, Plaintiff has no interest that is contrary to or in conflict with those of the
10 SubClass and the Class, she seeks to represent. In addition, Plaintiff has retained competent counsel
11 experienced in class action litigation to further ensure such protection and intend to prosecute this
12 action vigorously.

13 85. The nature of this action and the nature of laws available to Plaintiff and the other
14 SubClass and Class members make the use of the class action format a particularly efficient and
15 appropriate procedure to afford relief to Plaintiff and the other SubClass and Class members for the
16 claims alleged and the disposition of whose claims in a class action will provide substantial benefits
17 to both the parties and the Court because:

- 18 a) If each of the SubClass and the Class members were required to file an individual
- 19 lawsuit, the Defendants would necessarily gain an unconscionable advantage since
- 20 they would be able to exploit and overwhelm the limited resources of each individual
- 21 member of the SubClass and Class with its vastly superior financial and legal
- 22 resources;
- 23 b) The costs of individual suits could unreasonably consume the amounts that would be
- 24 recovered;
- 25 c) Proof of a common business practice or factual pattern which Plaintiff experienced is
- 26 representative of that experienced by the SubClass and the Class and will establish
- 27 the right of each of the members to recover on the causes of action alleged;
- 28

- 1 d) Individual actions would create a risk of inconsistent results and would be
- 2 unnecessary and duplicative of this litigation; and
- 3 e) The disposition of the claims of the members of the SubClass and the Class through
- 4 this class action will produce salutary by-products, including a therapeutic effect
- 5 upon those who indulge in fraudulent practices, and aid to legitimate business
- 6 enterprises by curtailing illegitimate competition.

7 86. The prosecution of separate actions by individual members of the SubClass and the
8 Class would create a risk of inconsistent or varying adjudications with respect to individual
9 members of the SubClass and the Class, which would establish incompatible standards of conduct
10 for the Defendants in the State of California and would lead to repetitious trials of the numerous
11 common questions of fact and law in the State of California. Plaintiff knows of no difficulty that
12 will be encountered in the management of this litigation that would preclude its maintenance as a
13 class action. As a result, a class action is superior to other available methods for the fair and
14 efficient adjudication of this controversy.

15 87. Notice to the members of the SubClass and the Class may be made by e-mail or first-
16 class mail addressed to all persons who have been individually identified by Defendants and who
17 have been given notice of the data breach.

18 88. Plaintiff, the SubClass and the Class have suffered irreparable harm and damages
19 because of Defendants' wrongful conduct as alleged herein. Absent certification, Plaintiff, the
20 SubClass and the Class will continue to be damaged and to suffer by the unauthorized disclosure
21 and/or release of their medical and personal identifying information, thereby allowing these
22 violations of law to proceed without remedy.

23 89. Moreover, Plaintiff's, the SubClass' and the Class' individual damages are
24 insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendants'
25 violations of law inflicting substantial damages in the aggregate would go unremedied. In addition,
26 Defendants have acted or refused to act on grounds generally applicable to Plaintiff, the SubClass
27 and the Class, thereby making appropriate final injunctive relief with respect to, the Class as a
28 whole.

FIRST CAUSE OF ACTION
Violations of the Confidentiality of Medical Information Act
California Civil Code §§ 56, et seq.
(On Behalf of Plaintiff and the SubClass Against NH)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

90. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if fully stated herein.

91. At all times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH is considered a “provider of health care,” within the meaning of Civil Code § 56.05(m), and maintained and continues to maintain “medical information” within the meaning of Civil Code § 56.05(j), of Plaintiff and the SubClass.

92. Plaintiff and the SubClass are “patients” of NH within the meaning of Civil Code § 56.05(k) and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure and/or release of their medical information could subject them to harassment or abuse.

93. At all times relevant to this action, including the period from October 22, 2020 to December 3, 2020, NH negligently created, maintained, preserved, and/or stored Plaintiff’s and the SubClass’ medical information, including Plaintiff’s and the SubClass’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in electronic form, onto Defendants’ computer networks in a manner that did not preserve the confidentiality of the information, and negligently failed to protect and preserve confidentiality of electronic medical information of Plaintiff and the SubClass in its possession, as required by the Act, and specifically, under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and 56.36(e)(2)(E), and according to their written representations to Plaintiff and the SubClass.

94. Due to NH’s disclosure and/or delivery Plaintiff’s and the SubClass members’ medical and personal identifying information to HCP without written authorization from Plaintiff and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff’s and the SubClass’ medical information, including Plaintiff’s and the SubClass’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be accessed and actually viewed by at least one unauthorized third party, without first obtaining an

1 authorization, constituting a disclosure in violation of Civil Code §§ 56.10, 56.13, 56.245, and
2 56.26(a).

3 95. Due to NH's negligent creation, maintenance, preservation and/or storage of
4 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server, NH
5 allowed Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass'
6 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
7 electronic form, to be accessed and actually viewed by at least one unauthorized third party, without
8 first obtaining an authorization, constituting a disclosure in violation of Civil Code §§ 56.10, 56.13,
9 56.245, and 56.26(a).

10 96. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass members'
11 medical and personal identifying information to HCP without written authorization from Plaintiff
12 and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff's and
13 the SubClass' medical information, including Plaintiff's and the SubClass' names, addresses, dates
14 of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be
15 accessed and actually viewed by at least one unauthorized third party, constituting a release in
16 violation of Civil Code § 56.101(a).

17 97. Due to NH's negligent creation, maintenance, preservation and/or storage of
18 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server,
19 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
20 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
21 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
22 constituting a release in violation of Civil Code § 56.101(a).

23 98. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass' medical
24 information and personal identifying information to HCP without written authorization from
25 Plaintiff and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed
26 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
27 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
28

1 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
2 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

3 99. Due to NH’s negligent creation, maintenance, preservation and/or storage of
4 Plaintiff’s and the SubClass members’ medical information on NETGAIN’s computer server, NH
5 allowed Plaintiff’s and the SubClass’ medical information, including Plaintiff’s and the SubClass’
6 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
7 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
8 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

9 100. As a result of NH’s above-described conduct in violation of the Act, Plaintiff and the
10 SubClass have suffered damages from the unauthorized disclosure and/or release of their medical
11 and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

12 101. As a result of NHs’ above-described conduct in violation of the Act, Plaintiff and the
13 SubClass seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
14 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
15 Code § 56.36(b)(2).

16 **SECOND CAUSE OF ACTION**
17 **Violations of the Confidentiality of Medical Information Act**
18 **California Civil Code §§ 56, et seq.**
19 **(On Behalf of Plaintiff and the Class Against HCP)**

20 102. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
21 fully stated herein.

22 103. At all times relevant to this action, including the period from October 22, 2020 to
23 December 3, 2020, HCP is considered a “provider of health care” within the meaning of Civil Code
24 § 56.05(m), a “contractor” under Civil Code § 56.05(d), and/or “engaged in the business of
25 furnishing administrative services to programs that provide payment for health care services” under
26 Civil Code § 56.26(a), and maintained and continues to maintain “medical information” within the
27 meaning of Civil Code § 56.05(j), of Plaintiff and the Class.
28

1 104. Plaintiff and the Class are “patients” within the meaning of Civil Code § 56.05(k)
2 and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure
3 and/or release of their medical information could subject them to harassment or abuse.

4 105. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, HCP negligently created, maintained, preserved, and/or stored Plaintiff’s and the
6 Class’ medical information, including Plaintiff’s and the Class’ names, addresses, dates of birth,
7 diagnosis/treatment information and treatment cost information, in electronic form, onto
8 NETGAIN’s computer server in a manner that did not preserve the confidentiality of the
9 information, and negligently failed to protect and preserve confidentiality of electronic medical
10 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
11 under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
12 56.36(e)(2)(E).

13 106. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
14 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
15 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
16 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
17 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
18 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
19 Code §§ 56.10, 56.13, 56.245, and 56.26(a).

20 107. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
21 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
22 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
23 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
24 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
25 third party, constituting a release in violation of Civil Code § 56.101(a).

26 108. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
27 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
28 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s

1 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
2 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
3 third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

4 109. As a result of HCP’s above-described conduct in violation of the Act, Plaintiff and
5 the Class have suffered damages from the unauthorized disclosure and/or release of their medical
6 and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

7 110. As a result of HCP’s above-described conduct in violation of the Act, Plaintiff and
8 the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
9 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
10 Code § 56.36(b)(2).

11 **THIRD CAUSE OF ACTION**
12 **Violations of the Confidentiality of Medical Information Act**
13 **California Civil Code §§ 56, et seq.**
14 **(On Behalf of Plaintiff and the Class Against NETGAIN)**

15 111. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
16 fully stated herein.

17 112. At all times relevant to this action, including the period from October 22, 2020 to
18 December 3, 2020, NETGAIN is considered a “provider of health care” within the meaning of Civil
19 Code § 56.05(m), and maintained and continues to maintain “medical information” within the
20 meaning of Civil Code § 56.05(j), of Plaintiff and the Class.

21 113. Plaintiff and the Class are “patients” within the meaning of Civil Code § 56.05(k)
22 and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure
23 and/or release of their medical information could subject them to harassment or abuse.

24 114. At all times relevant to this action, including the period from October 22, 2020 to
25 December 3, 2020, NETGAIN negligently created, maintained, preserved, and/or stored Plaintiff’s
26 and the Class’ medical information, including Plaintiff’s and the Class’ names, addresses, dates of
27 birth, diagnosis/treatment information and treatment cost information, in electronic form, onto
28 NETGAIN’s computer server in a manner that did not preserve the confidentiality of the
information, and negligently failed to protect and preserve confidentiality of electronic medical

1 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
2 under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
3 56.36(e)(2)(E).

4 115. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
5 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
6 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
7 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
8 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
9 unauthorized third party, without first obtaining an authorization, constituting a disclosure in
10 violation of Civil Code §§ 56.10, 56.13, 56.245, and 56.26(a).

11 116. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
12 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
13 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
14 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
15 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
16 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

17 117. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
18 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
19 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
20 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
21 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
22 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

23 118. As a result of NETGAIN's above-described conduct in violation of the Act, Plaintiff
24 and the Class have suffered damages from the unauthorized disclosure and/or release of their
25 medical and personal identifying information made unlawful by Civil Code §§ 56.10, 56.101.

26 119. As a result of NETGAIN's above-described conduct in violation of the Act, Plaintiff
27 and the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
28

1 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
2 Code § 56.36(b)(2).

3 **FOURTH CAUSE OF ACTION**
4 **Breach of California Security Notification Laws**
5 **California Civil Code § 1798.82**
6 **(On Behalf of Plaintiff and the Class Against HCP)**

7 120. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
8 fully stated herein.

9 121. Pursuant to Civil Code § 1798.82(a), “A person or business that conducts business in
10 California, and that owns or licenses computerized data that includes personal information, shall
11 disclose a breach of the security of the system following discovery or notification of the breach in
12 the security of the data to a resident of California (1) whose unencrypted personal information was,
13 or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted
14 personal information was, or is reasonably believed to have been, acquired by an unauthorized
15 person and the encryption key or security credential was, or is reasonably believed to have been,
16 acquired by an unauthorized person and the person or business that owns or licenses the encrypted
17 information has a reasonable belief that the encryption key or security credential could render that
18 personal information readable or usable. The disclosure shall be made in the most expedient time
19 possible and without unreasonable delay, consistent with the legitimate needs of law enforcement,
20 as provided in subdivision (c), or any measures necessary to determine the scope of the breach and
21 restore the reasonable integrity of the data system.” Prior to passages of such statute, the California
22 State Assembly cited an incident where authorities knew of the breach in security for 21 days
23 “before state workers were told” as an example of “late notice.”

24 122. Civil Code § 1798.82 further provides, “(h) For purposes of this section, ‘personal
25 information’ means an individual’s first name or first initial and last name in combination with any
26 one or more of the following data elements, when either the name or the data elements are not
27 encrypted: (1) Social security number. (2) Driver’s license number or California Identification Card
28 number. (3) Account number, credit or debit card number, in combination with any required
security code, access code, or password that would permit access to an individual's financial

1 account. (4) Medical information. (5) Health insurance information. (i) (2) For purposes of this
2 section, ‘medical information’ means any information regarding an individual’s medical history,
3 mental or physical condition, or medical treatment or diagnosis by a health care professional. (3)
4 For purposes of this section, ‘health insurance information’ means an individual’s health insurance
5 policy number or subscriber identification number, any unique identifier used by a health insurer to
6 identify the individual, or any information in an individual’s application and claims history,
7 including any appeals records.”

8 123. HCP conducts business in California and owns or licenses computerized data which
9 includes the personal information, within the meaning of Civil Code § 1798.82(h), of Plaintiff and
10 the Class.

11 124. Based upon NH’s “**Notice of Data Breach**” form letter, HCP was aware that
12 Plaintiff’s and the Class’ unencrypted personal information on NETGAIN’s computer server was,
13 or is reasonably believed to have been, acquired by an unauthorized person no later than December
14 3, 2020, but did not begin to mail notification letters to Plaintiff and the Class until April 12, 2021.
15 Thus, HCP waited at least 131 days before *beginning* to inform Plaintiff and the Class of this
16 incident and the subsequent threat to Plaintiff’s and the Class’ personal information. As a result,
17 HCP did not disclose to Plaintiff and the Class that their personal information was, or was
18 reasonably believed to have been, acquired by an unauthorized person, in the most expedient time
19 possible and without reasonable delay in violation of Civil Code § 1798.82(a). Given the example
20 of the Legislature finding that a delay of 21 days to be “late notice” under the statute, HCP’s delay
21 of 131 days before *beginning* to inform Plaintiff and the Class that their personal information was,
22 or was reasonably believed to have been, acquired by an unauthorized person by mailing HCP’s
23 form letter to Plaintiff and the Class is presumptively unreasonable notice in violation of Civil Code
24 § 1798.82(a).

25 125. Plaintiff and the Class have been injured by fact that HCP did not disclose their
26 personal information was, or was reasonably believed to have been, acquired by an unauthorized
27 person in the most expedient time possible and without reasonable delay in violation of Civil Code
28 § 1798.82(a). HCP’s delays in informing required by Civil Code § 1798.82(a) and providing all of

1 the information required by Civil Code § 1798.82(d) to Plaintiff and the Class that their personal
2 information was, or was reasonably believed to have been, acquired by an unauthorized person,
3 have prevented Plaintiff and the Class from taking steps to protect their personal information from
4 unauthorized use and/or identify theft.

5 126. Plaintiff and the Class seek recovery of their damages pursuant to Civil Code §
6 1798.84(b) and injunctive relief pursuant to Civil Code § 1798.84(e).

7 **FIFTH CAUSE OF ACTION**
8 **Unlawful and Unfair Business Acts and Practices in Violation of**
9 **California Business & Professions Code §17200, *et seq.***
10 **(On Behalf of Plaintiff, the SubClass and the Class Against All Defendants)**

11 127. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
12 fully stated herein.

13 128. The acts, misrepresentations, omissions, practices, and non-disclosures of
14 Defendants as alleged herein constituted unlawful and unfair business acts and practices within the
15 meaning of California Business & Professions Code §§ 17200, *et seq.*

16 129. By the aforementioned business acts or practices, Defendants have engaged in
17 “unlawful” business acts and practices in violation of the aforementioned statutes, including Civil
18 Code §§ 56.10(a), 56.26(a), 56.36(e)(2)(E), 56.101(a), 56.101(b)(1)(A), 1798.82(a) and 1798.82(d).
19 Plaintiff reserves the right to allege other violations of law committed by Defendants which
20 constitute unlawful acts or practices within the meaning of California Business & Professions Code
21 §§ 17200, *et seq.*

22 130. By the aforementioned business acts or practices, Defendants have also engaged in
23 “unfair” business acts or practices in that the harm caused by Defendants’ failure to maintain
24 adequate information security procedures and practices, including but not limited to, failing to take
25 adequate and reasonable measures to ensure its data systems were protected against unauthorized
26 intrusions, failing to properly and adequately educate and train its employees, failing to put into
27 place reasonable or adequately computer systems and security practices to safeguard patients’
28 identifiable medical information including access restrictions and encryption, failing to have
adequate privacy policies and procedures in place that did not preserve the confidentiality of the

1 medical and personal identifying information of Plaintiff, the SubClass and the Class in their
2 possession, and failing to protect and preserve confidentiality of electronic medical information of
3 Plaintiff, the SubClass and the Class in their possession against disclosure and/or release, outweighs
4 the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous,
5 unethical, deceitful and offensive, and causes substantial injury to Plaintiff, the SubClass and the
6 Class.

7 131. Defendants have obtain money and property from Plaintiff, the SubClass and the
8 Class because of the payment of the services and products they received from Defendants. Plaintiff,
9 the SubClass and the Class have suffered an injury in fact by acquiring less in their transactions
10 with Defendants for the services and products they received from Defendants than they otherwise
11 would have if Defendants would had adequately protected the confidentiality of their medical and
12 personal identifying information.

13 132. Pursuant to the Business & Professions Code § 17203, Plaintiff, the SubClass and the
14 Class seek an order of this Court requiring Defendants awarding Plaintiff and the Class restitution
15 of monies wrongfully acquired by Defendants in the form of payments for services by means of
16 such unlawful, fraudulent and unfair business acts and practices, so as to restore any and all monies
17 to Plaintiff, the SubClass and the Class which were acquired and obtained by means of such
18 unlawful, fraudulent and unfair business acts and practices, which ill-gotten gains are still retained
19 by Defendants.

20 133. The aforementioned unlawful, fraudulent and unfair business acts or practices
21 conducted by Defendants have been committed in the past and continues to this day. Defendants
22 have failed to acknowledge the wrongful nature of their actions. Defendants have not corrected or
23 publicly issued comprehensive corrective notices to Plaintiff, the SubClass and the Class, and have
24 not corrected or enacted adequate privacy policies and procedures to protect and preserve
25 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
26 Class in their possession.

27
28

1 134. Because of Defendants’ aforementioned conduct, Plaintiff, the SubClass and the
2 Class have no other adequate remedy of law in that absent injunctive relief from the Court and
3 Defendants are likely to continue to injure Plaintiff, the SubClass and the Class.

4 135. Pursuant to Business & Professions Code § 17203, Plaintiff, the SubClass and the
5 Class also seek an order of this Court for equitable and/or injunctive relief in the form of requiring
6 Defendants to correct its illegal conduct that is necessary and proper to prevent Defendants from
7 repeating their illegal and wrongful practices as alleged above and protect and preserve
8 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
9 Class in Defendants’ possession that has already been accessed, viewed, exfiltrated and/or publicly
10 exposed by at least one unauthorized third party because by way of Defendants’ illegal and
11 wrongful practices set forth above. Pursuant to Business & Professions Code § 17203, Plaintiff, the
12 SubClass and the Class further seek an order of this Court for equitable and/or injunctive relief in
13 the form of requiring Defendants to publicly issue comprehensive corrective notices.

14 136. Because this case is brought for the purposes of enforcing important rights affecting
15 the public interest, Plaintiff, the SubClass and the Class also seek the recovery of attorneys’ fees
16 and costs in prosecuting this action against Defendants under Code of Civil Procedure § 1021.5 and
17 other applicable law.

18 **PRAYER FOR RELIEF**

19 WHEREFORE, Plaintiff respectfully request that the Court grant Plaintiff and the proposed
20 SubClass and Class the following relief against Defendants, and each of them:

21 **As for the First, Second and Third Causes of Action**

- 22 1. For nominal damages in the amount of one thousand dollar (\$1,000) per violation to Plaintiff
- 23 individually and to each member of the SubClass and the Class pursuant to Civil Code §
- 24 56.36(b)(1);
- 25 2. For actual damages according to proof per violation pursuant to Civil Code § 56.36(b)(2);

26 **As for the Fourth Cause of Action**

- 27 3. For damages according to proof to Plaintiff individually and to each member of the Class
- 28 pursuant to California Civil Code § Civil Code § 1798.84(b);

1 4. For injunctive relief pursuant to California Civil Code § Civil Code § 1798.84(e);

2 **As for the Fifth Cause of Action**

3 5. For an order awarding Plaintiff, the SubClass and the Class restitution of all monies
4 wrongfully acquired by Defendants by means of such unlawful, fraudulent and unfair
5 business acts and practices;

6 6. For injunctive relief in the form of an order instructing Defendants to prohibit the
7 unauthorized release of medical and personal identifying information of Plaintiff, the
8 SubClass and the Class, and to adequately maintain the confidentiality of the medical and
9 personal identifying information of Plaintiff and the Class;

10 7. For injunctive relief in the form of an order enjoining Defendants from disclosing the
11 medical and personal identifying information of Plaintiff, the SubClass and the Class
12 without the prior written authorization of each Plaintiff, the SubClass and the Class member;

13 **As to All Causes of Action**

14 8. That the Court issue an Order certifying this action be certified as a class action on behalf of
15 the proposed SubClass and Class, appointing Plaintiff as representative of the proposed
16 SubClass and Class, and appointing Plaintiff's attorneys, as counsel for members of the
17 proposed SubClass and Class;

18 9. For an award of attorneys' fees as authorized by statute, including, but not limited to, the
19 provisions of California Code of Civil Procedure § 1021.5, and as authorized under the
20 "common fund" doctrine, and as authorized by the "substantial benefit" doctrine;

21 10. For costs of the suit;

22 11. For prejudgment interest at the legal rate; and

23 12. Any such further relief as this Court deems necessary, just, and proper.

24 Dated: June 1, 2021

KEEGAN & BAKER LLP

25 By: 
26 Patrick N. Keegan, Esq.
27 Attorney for Plaintiff
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

Plaintiff, the SubClass and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

Dated: June 1, 2021

KEEGAN & BAKER LLP

By: 
Patrick N. Keegan, Esq.
Attorney for Plaintiff

Exhibit A



HEALTH CENTER PARTNERS
of Southern California

C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE



NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

SEQ
CODE 2D
Ver 1

BREAK

To Enroll, Please Call:
1-833-416-0926
Or Visit:
<https://response.idx.us/hcp-netgain-incident>
Enrollment Code: <<XXXXXXXXXX>>

April 12, 2021

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by Netgain Technology, LLC (“Netgain”), the IT service provider for Health Center Partners of Southern California (“HCP”). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTHCENTER>>. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, we engaged our own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, our health center members and partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain’s cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

Once we learned that HCP data may have been involved in the incident, we worked with our cybersecurity experts to review the impacted files and identify the individuals whose information was contained in such files so that we may notify such individuals. Our investigation revealed that the impacted files contained your personal information. **Again, we are not aware of any misuse of your personal information as a result of this incident.** Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your information.

What Information Was Involved: The information involved varies depending on the individual but may include the following: <<VARPARAGRAPH>>.

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, we have reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and we are committed to assisting their investigation into the matter.

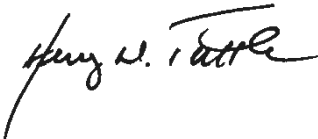
We are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include **xx** months of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What You Can Do: As we have stated, we are not aware of any misuse of your information as a result of this incident. However, we encourage you to follow the recommendations on the next page to help protect your information. We also encourage you to enroll in the complimentary services offered by going to <https://response.idx.us/hcp-netgain-incident> or calling 1-833-416-0926 and using the enrollment code provided above. Please note that the deadline to enroll is July 12, 2021.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-833-416-0926 between 6:00 a.m. and 6:00 p.m. Pacific Time.

The security of your information is a top priority for HCP, and we are committed to safeguarding your data and privacy.

Sincerely,

A handwritten signature in black ink, appearing to read "Henry W. Tuttle". The signature is fluid and cursive, with the first name "Henry" being the most prominent.

Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
www.consumer.ftc.gov ,	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
and	1-888-743-0023	1-877-566-7226	1-401-274-4400
www.ftc.gov/idtheft			
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Exhibit B



To Enroll, Please Call:
(833) 903-3642
Or Visit:
<https://response.idx.us/nhc-netgain-incident>
Enrollment Code: <<ENROLLMENT>>

C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

April 8, 2021

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

The privacy and security of your personal information is very important to Neighborhood Healthcare. We are writing to make you aware of an issue brought to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud hosting and managed services provider. Neighborhood Healthcare used Netgain to host some Neighborhood Healthcare files.

What Happened

On November 24, 2020, Netgain became aware of a security incident that involved unauthorized access to portions of the Netgain environment and Netgain client environments and began taking steps to investigate this incident. But, on December 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain took additional measures to contain the threat and address the issue. Netgain’s technical teams worked closely with third-party experts to remove the threat in the impacted environments and confirm that client and internal systems are protected.

Neighborhood Healthcare learned of the ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to believe that the protected health information (“PHI”) of our patients had been impacted in the incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some information including, potentially, some files containing patient PHI may have been impacted in the incident. Netgain could not confirm, at that time, what records may have been impacted in the incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood Healthcare that Netgain believed were impacted by the attackers. Those files came from a Neighborhood Healthcare server accessible by the Netgain environment. Since that time, Neighborhood Healthcare has worked to review those records, to identify individuals impacted, conduct an investigation into the incident with the assistance outside experts, and to transmit this letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood Healthcare determined that the impacted files included some of your information.

What Information Was Involved

The information involved may have included some of the following: your name, date of birth, address, Social Security Number and information about the care that you received from Neighborhood Healthcare such as insurance coverage information, physician you saw, and treatment codes. Neighborhood Healthcare is offering credit monitoring services to you at no charge. Please see the **What You Can Do** section below for information about these services including how to enroll. Please also see the **Additional Important Information** section below for further precautionary measures you may wish to take. Netgain has received assurances that the data has not gone beyond the attacker, that the data was not and will not be misused, and that the data will not be disseminated or otherwise be made publicly available.

What We Are Doing

Please know that we take this incident and the security of your personal information very seriously. Ensuring the safety of our patients' data is of the utmost importance to us. Since we learned of this incident, we have been working with Netgain to seek assurances that they are taking appropriate steps to respond to this incident. We have also conducted an investigation of the incident with the help of outside experts, and we have transitioned to a new hosting provider (a transition that was already in process when this incident occurred).

In addition, we are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include <<12/24 months>> of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What Netgain Is Doing

Netgain took several steps to strengthen its environment following the incident, including international Geo-fencing for Azure-hosted environments, deploying additional log monitoring across all servers, and additional hardening of network security rules and protocols to restrict lateral movement across environments. Netgain stated that it paid a significant amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

What You Can Do

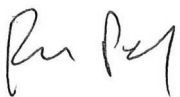
We recommend that you review the additional information enclosed. Additionally, we encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 903-3642 or going to <https://response.idx.us/nhc-netgain-incident> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 8, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

We very much regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, please call (833) 903-3642, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely



Rakesh Patel
CEO
Neighborhood Healthcare

Additional Important Information

1. Website and Enrollment. Go to <https://response.idx.us/nhc-netgain-incident> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 903-3642 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Generally. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing financial account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state's Attorney General.

5. The FTC. You can obtain information from Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

6. Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

7. Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788 equifax.com/personal/credit-report-services/ 800-525-6285	Experian Security Freeze P.O. Box 9554 Allen, TX 75013-9544 experian.com/freeze/center.html 888-397-3742	TransUnion (FVAD) P.O. Box 160 Woodlyn, PA 19094 transunion.com/credit-freeze 888-909-8872
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

More information can also be obtained by contacting the Federal Trade Commission listed above.

8. Protecting Medical Information: To date, we have no reason to believe that your PHI potentially involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following steps can help protect you from medical identity theft issues.

- Do not share health insurance cards with anyone apart from your care providers and other family members who are covered under the insurance plan or who help you with your medical care.
- Review the “explanation of benefits statements” that you receive from your health insurance company. If you see something amiss, follow up with your insurance company or the health care provider identified on the explanation of benefits to request further information.
- Ask your health insurance company for a report on all services they have paid for you for the current year. If you do not recognize an item in that list, speak with your insurance company to verify it.

9. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Telephone: (760) 929-9303
4 Facsimile: (760) 929-9260

5 Attorneys for Plaintiff JANE DOE

6
7 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
8 **FOR THE COUNTY OF COUNTY OF SAN DIEGO**

9 JANE DOE, individually and on behalf of all
others similarly situated,

10 Plaintiff,

11 vs.

12 NEIGHBORHOOD HEALTHCARE; HEALTH
13 CENTER PARTNERS OF SOUTHERN
CALIFORNIA; NETGAIN TECHNOLOGY,
14 LLC; and DOE DEFENDANTS 1-100;

15 Defendants.
16

) Case No. 37-2021-00023936-CU-BT-CTL
)

) **FIRST AMENDED CLASS ACTION**
) **COMPLAINT FOR DAMAGES,**
) **RESTITUTION, AND INJUNCTIVE**
) **RELIEF FOR VIOLATIONS OF:**

-) (1) **THE CONFIDENTIALITY OF**
) **MEDICAL INFORMATION ACT,**
) **CIVIL CODE §§ 56, ET SEQ.;**
) (2) **BREACH OF CALIFORNIA**
) **SECURITY NOTIFICATION**
) **LAWS, CALIFORNIA CIVIL CODE**
) **§ 1798.82; AND**
) (3) **BUSINESS AND PROFESSIONS**
) **CODE §§ 17200, ET SEQ.**

) **JURY TRIAL DEMANDED**
)

17
18
19 Plaintiff Jane Doe (or “Plaintiff”), by and through her attorneys, bring this class action on
20 behalf of herself individually and all others similarly situated, against Defendants Neighborhood
21 Healthcare, Health Center Partners of Southern California, and Netgain Technology, LLC
22 (collectively referred to as “Defendants”), and alleges upon information and belief as follows:

23 **INTRODUCTION**

24 1. This class action arises from the negligent and failure of Defendants to properly
25 create, maintain, preserve, and/or store confidential, medical and personal identifying information
26 of Plaintiff¹ and all other persons similarly situated which allowed an unauthorized person to gain
27

28 ¹ Pursuant to the Court’s Order Granting Plaintiff’s Ex Parte Application to Appear by Pseudonym
(ROA #14), a pseudonym has been used in place of the real name of Plaintiff because at all times

1 access to a computer database server of Defendants from October 22, 2020 to December 3, 2020,
2 causing unauthorized access, viewing, exfiltration, theft, and/or disclosure of unencrypted medical
3 and personal identifying information of Plaintiff and other persons similarly situated, to at least one
4 unauthorized person resulting in violations of the Confidentiality of Medical Information Act, Civil
5 Code §§ 56, *et seq.* (hereinafter referred to as the “Act”), the Security Notification Laws, Civil Code
6 § 1798.82, and the Business and Professions Code §§ 17200 *et seq.* Under the Act, Plaintiff, and
7 all other persons similarly situated, have the right to expect that the confidentiality of their medical
8 information in possession of Defendants and/or derived from Defendants to be reasonably
9 preserved and protected from unauthorized access, viewing, exfiltration, theft, and/or disclosure.

10 2. As alleged more fully below, failing to take adequate and reasonable measures to
11 ensure its data systems were protected against unauthorized intrusions, by failing to invest in cyber
12 security and data protection safeguards, failing to implement adequate and reasonable security
13 controls and user authorization and authentication processes, failing to limit the types of data
14 permitted to be transferred, failing to properly and adequately educate and train its employees, and
15 to put into place reasonable or adequate computer systems and security practices to safeguard
16 customers’ and patients’ medical and personal identifying information, Defendants negligently
17 created, maintained, preserved, and stored Plaintiff’s and the Class (defined *infra*) members’
18 medical and personal identifying information in possession of or derived from Defendants allowed
19 such information to be accessed and actually viewed by at least one unauthorized third party,
20 without Plaintiff’s and the Class members’ prior written authorization, which constitutes
21 unauthorized disclosure and/or release of their information in violation of Civil Code §§ 56.10(a)
22 and 56.101(a) of the Act. In fact, Defendant Health Center Partners of Southern California’s form
23 letter, entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle, President &
24 Chief Executive Officer, Health Center Partners of Southern California, sent to Plaintiff and all
25 other persons similarly situated, informing them, in part, of “a recent data security incident
26 experienced by Netgain Technology, LLC (‘Netgain’), the IT service provider for Health Center
27

28 relevant to this action, Plaintiff is a health care patient under Civil Code § 56.05(k) and has individual privacy concerns and a reasonable fear of harassment in light of the nature of the case.

1 Partners of Southern California (“HCP”)) and stating, in part, “HCP supports community health
2 centers in a variety of ways, including collaborative grant-funded programs and services for
3 Neighborhood Healthcare.... **What Happened:** Netgain recently informed HCP that it had
4 experienced a data security incident that involved systems containing HCP data.... According to
5 Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital
6 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
7 obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the
8 attacker in exchange for assurances that the attacker will delete all copies of this data and that it will
9 not publish, sell, or otherwise disclose the data.... The information involved varies depending on the
10 individual but may include the following: name, address, date of birth, diagnosis/treatment
11 information and treatment cost information. Once we learned that HCP data may have been
12 involved in the incident, we worked with our cybersecurity experts to review the impacted files and
13 identify the individuals whose information was contained in such files so that we may notify such
14 individuals. Our investigation revealed that the impacted files contained your personal information.”
15 An exemplar of Defendant Health Center Partners of Southern California’s “**Notice of Data**
16 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
17 as **Exhibit A**.

18 3. Additionally, Defendant Neighborhood Healthcare caused a form letter sent on its
19 behalf, entitled “**Notice of Data Breach**,” dated April 8, 2021, signed by Rakesh Patel, CEO,
20 Neighborhood Healthcare, stating, in part, “We are writing to make you aware of an issue brought
21 to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud
22 hosting and managed services provider. Neighborhood Healthcare used Netgain to host some
23 Neighborhood Healthcare files. **What Happened** On November 24, 2020, Netgain became aware
24 of a security incident that involved unauthorized access to portions of the Netgain environment and
25 Netgain client environments and began taking steps to investigate this incident. But, on December
26 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files
27 owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain
28 took additional measures to contain the threat and address the issue. Netgain’s technical teams

1 worked closely with third-party experts to remove the threat in the impacted environments and
2 confirm that client and internal systems are protected. Neighborhood Healthcare learned of the
3 ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to
4 believe that the protected health information (“PHI”) of our patients had been impacted in the
5 incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some
6 information including, potentially, some files containing patient PHI may have been impacted in the
7 incident. Netgain could not confirm, at that time, what records may have been impacted in the
8 incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood
9 Healthcare that Netgain believed were impacted by the attackers. Those files came from a
10 Neighborhood Healthcare server accessible by the Netgain environment. Since that time,
11 Neighborhood Healthcare has worked to review those records, to identify individuals impacted,
12 conduct an investigation into the incident with the assistance outside experts, and to transmit this
13 letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood
14 Healthcare determined that the impacted files included some of your information. **What**
15 **Information Was Involved** The information involved may have included some of the following:
16 your name, date of birth, address, Social Security Number and information about the care that you
17 received from Neighborhood Healthcare such as insurance coverage information, physician you
18 saw, and treatment codes.” An exemplar of Defendant Neighborhood Healthcare’s “**Notice of Data**
19 **Breach**” form letter submitted to the Attorney General of the State of California is attached hereto
20 as **Exhibit B**.

21 4. Additionally, Defendant Netgain Technology, LLC stated in a blog post, entitled
22 “What we learned as a ransomware victim – so you don’t become one,” that “late last year, Netgain
23 was the victim of a criminal ransomware attack.... to become a victim of such an attack is both
24 humbling and galvanizing.... we identified additional opportunities to strengthn our security posture
25 in a continuous journey with an ongoing commitment to ensure this remains top-of-mind. As part
26 of our incident response, we have implemented a number of these identified enhancements to our
27 security posture and have continued to progress a multipronged approach. We’ve deployed new
28

1 tools, revised policies and enforcement procedures, and implemented an advanced around-the-clock
2 managed detections and response service for proactive threat monitoring.”

3 5. Because the individually identifiable medical information and other personal
4 identifying information of Plaintiff and the Class was subject to unauthorized access and viewing by
5 at least one unauthorized third party and in violation of the Act, Plaintiff, individually and on behalf
6 of all others similarly situated, seeks from Defendants nominal damages in the amount of one
7 thousand dollars (\$1,000) for each violation under Civil Code §56.36(b)(1) and actual damages,
8 according to proof, for each violation pursuant to Civil Code § 56.36(b)(2). Further, because
9 Plaintiff also alleges Defendants’ conduct violates Business & Professions Code §§ 17200, *et seq.*,
10 Plaintiff, individually and on behalf of others similarly situated, seeks injunctive relief and
11 restitution from Defendants under Business and Professions Code § 17203.

12 6. This action, if successful, will enforce an important right affecting the public interest
13 and would confer a significant benefit, whether pecuniary or non-pecuniary, on a large class of
14 persons. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff
15 in relation to Plaintiff’s stake in the matter, and therefore class certification is appropriate in this
16 matter.

17 **JURISDICTION AND VENUE**

18 7. This Court has jurisdiction over this action under California Code of Civil Procedure
19 § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class in the aggregate
20 exceeds the \$25,000 jurisdictional minimum of this Court. Further, the amount in controversy as to
21 Plaintiff individually does not exceed \$75,000.

22 8. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of
23 Civil Procedure §§ 395(a) and 395.5 because Defendant Neighborhood Healthcare is incorporated
24 in and does business in the State of California, and employs persons located in the County of San
25 Diego and in this judicial district. Defendants have obtained medical information of Plaintiff and
26 the Class in the transaction of business in the State of California and in this judicial district, which
27 has caused both obligations and liability of Defendants to arise in the State of California and in this
28 judicial district.

1 9. Further, this action does not qualify for federal jurisdiction under the Class Action
2 Fairness Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies
3 to this action because (1) more than two-thirds of the members of the proposed Class and SubClass
4 are citizens of the State of California, and (2) Defendants are citizens of the State of California.

5 **PARTIES**

6 **A. PLAINTIFF**

7 10. Plaintiff Jane Doe is and was at all times relevant to this action a resident of the State
8 of California and citizen of the State of California. At all times relevant to this action, Plaintiff
9 JANE DOE was a patient of, received medical treatment and diagnosis from, and provided her
10 personal information, including her name, address, date of birth, social security number, phone
11 number and email address to Defendant Neighborhood Healthcare. Additionally, Plaintiff received
12 a letter addressed to her, sent on Defendant Health Center Partners of Southern California’s behalf,
13 entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle, President & Chief
14 Executive Officer, Health Center Partners of Southern California, informing her, in part, of “a
15 recent data security incident experienced by Netgain Technology, LLC (‘Netgain’), the IT service
16 provider for Health Center Partners of Southern California (‘HCP’)” and stating, in part, “HCP
17 supports community health centers in a variety of ways, including collaborative grant-funded
18 programs and services for Neighborhood Healthcare.... **What Happened:** Netgain recently
19 informed HCP that it had experienced a data security incident that involved systems containing
20 HCP data.... According to Netgain, in late September 2020, an unauthorized third party gained
21 access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the
22 unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an
23 undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies
24 of this data and that it will not publish, sell, or otherwise disclose the data.... The information
25 involved varies depending on the individual but may include the following: name, address, date of
26 birth, diagnosis/treatment information and treatment cost information. Once we learned that HCP
27 data may have been involved in the incident, we worked with our cybersecurity experts to review
28 the impacted files and identify the individuals whose information was contained in such files so that

1 we may notify such individuals. Our investigation revealed that the impacted files contained your
2 personal information.” As a result, Plaintiff reasonably fears that disclosure and/or release of her
3 medical information created, maintained, preserved and/or stored on Defendants’ computer
4 networks could subject her to harassment or abuse.

5 **B. DEFENDANTS**

6 11. Defendant Neighborhood Healthcare (“NH”) is a California corporation, is registered
7 to do business and does business in the State of California (CA Corp. No. C0667935), with its
8 principal business office located at 1540 E. Valley Parkway, Escondido CA 92026, and with its
9 registered agent of service of process located at 150 La Terraza Blvd, Suite 201, Escondido CA
10 92025. On or about April 8, 2021, NH caused a form letter sent on its behalf, entitled “**Notice of**
11 **Data Breach,**” dated April 8, 2021, signed by Rakesh Patel, CEO, Neighborhood Healthcare, an
12 exemplar of which is attached hereto as **Exhibit B**, to be submitted to the Attorney General of the
13 State of California. At all times relevant to this action, NH was and is a provider of health care, a
14 contractor, and/or other authorized recipient of personal and confidential medical information, as
15 that term is defined and set forth in the Act, including the names, addresses, dates of birth,
16 diagnosis/treatment information and treatment cost information of Plaintiff and the SubClass
17 (defined *infra*), and is subject to the requirements and mandates of the Act, including but not limited
18 to Civil Code §§ 56.10, 56.101 and 56.36. At all times relevant to this action, NH was and is a
19 provider of health care and employed and employs persons located in the County of San Diego
20 and in this judicial district.

21 12. Defendant Health Center Partners of Southern California (“HCP”) is a business
22 entity doing business in the State of California, with its principal business office located at 3710
23 Ruffin Road, San Diego, CA 92123. On or about April 12, 2021, HCP caused a form letter sent on
24 its behalf, entitled “**Notice of Data Breach,**” dated April 12, 2021, signed by Henry Tuttle,
25 President & Chief Executive Officer, Health Center Partners of Southern California, an exemplar of
26 which is attached hereto as **Exhibit A**, to be submitted to the Attorney General of the State of
27 California and to be mailed to Plaintiff and the Class. At all times relevant to this action, HCP was
28 and is a “business” within the meaning of Civil Code § 1798.140(c)(1), owns or licenses

1 computerized data which includes Plaintiff’s and the Class’ personal information, within the
2 meaning of Civil Code § 1798.82(h), collected Plaintiff’s and the Class’ personal information
3 within the meaning of Civil Code § 1798.81.5(d)(1)(A).

4 13. Defendant Netgain Technology, LLC (“NETGAIN”) is a business entity doing
5 business in the State of California, with a principal business office located at 5353 Mission Center
6 Road, Suite 202, San Diego, CA 92108. At all times relevant to this action, NETGAIN was and is
7 NH’s and HCP’s third-party vendor. On March 24, 2021, NETGAIN posted on its website a blog,
8 entitled “What we learned as a ransomware victim – so you don’t become one,” which stated, in
9 part, “In our case, late last year, Netgain was the victim of a criminal ransomware attack.... to
10 become a victim of such an attack is both humbling and galvanizing.... we identified additional
11 opportunities to strengthn our security posture in a continuous journey with an ongoing commitment
12 to ensure this remains top-of-mind. As part of our incident response, we have implemented a
13 number of these identified enhancements to our security posture and have continued to progress a
14 multipronged approach. We’ve deployed new tools, revised policies and enforcement procedures,
15 and implemented an advanced around-the-clock managed detections and response service for
16 proactive threat monitoring.”

17 **C. DOE DEFENDANTS**

18 14. The true names and capacities, whether individual, corporate, associate, or otherwise,
19 of Defendants sued herein as Doe Defendants 1 through 100, inclusive, are currently unknown to
20 Plaintiff, who therefore sue the Defendants by such fictitious names under the Code of Civil
21 Procedure § 474. Each of the Defendants designated herein as a Doe Defendant is legally
22 responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of
23 court and/or amend this complaint to reflect the true names and capacities of the Defendants
24 designated hereinafter as Doe Defendants 1 through 100 when such identities become known. Any
25 reference made to a named Defendant by specific name or otherwise, individually or plural, is also a
26 reference to the actions or inactions of Doe Defendants 1 through 100, inclusive.

27 ///

28 ///

1 **D. AGENCY/AIDING AND ABETTING**

2 15. At all times herein mentioned, Defendants, and each of them, were an agent or joint
3 venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the
4 course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the
5 acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized
6 the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

7 16. Defendants, and each of them, aided and abetted, encouraged and rendered
8 substantial assistance to the other Defendants in breaching their obligations to Plaintiff and the
9 Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially
10 assist the commissions of these wrongful acts and other wrongdoings complained of, each of the
11 Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its
12 conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals,
13 and wrongdoing.

14 **FACTUAL ALLEGATIONS**

15 17. Plaintiff alleges on information and belief that at all times relevant to this action,
16 including the period from October 22, 2020 to December 3, 2020, NH disclosed and/or released
17 Plaintiff's and the Class' medical information, in electronic and physical form, in possession of or
18 derived from NH, regarding their medical history, mental or physical condition, or treatment, to
19 HCP, pursuant to a business associate agreement. Such medical information included or contained
20 an element of personal identifying information sufficient to allow identification of Plaintiff and the
21 Class, such as their names, date of birth, addresses, medical record numbers, insurance provider,
22 electronic mail addresses, telephone numbers, or social security numbers, or other information that,
23 alone or in combination with other publicly available information, reveals their identity. As a
24 result, at all times relevant to this action, including the period from October 22, 2020 to December
25 3, 2020, HCP possessed Plaintiff's and the Class' medical information, in electronic and physical
26 form, in possession of or derived from Defendant regarding their medical history, mental or
27 physical condition, or treatment. Such medical information included or contained an element of
28 personal identifying information sufficient to allow identification of Plaintiff and the Class, such as

1 their names, date of birth, addresses, medical record numbers, insurance provider, electronic mail
2 addresses, telephone numbers, or social security numbers, or other information that, alone or in
3 combination with other publicly available information, reveals their identity. On its website, HCP
4 represents that “[o]ur members collectively serve 917,000 unduplicated patients each year, for 3.9
5 million patient visits each year, at 160 practice sites across San Diego, Riverside, Imperial
6 counties.”² At all times relevant to this action, including the period from October 22, 2020 to
7 December 3, 2020, HCP maintained and continues to maintain “medical information,” within the
8 meaning of Civil Code § 56.05(j), of Plaintiff and the Class, each of which are “patients” within the
9 meaning of Civil Code § 56.05(k).

10 18. On its website, NH represents, “At Neighborhood, our vision is a community where
11 everyone is healthy and happy. That includes you. Our innovative services include quality care for
12 every stage of life—from prenatal to pediatrics to primary care and beyond. From your head to your
13 feet and everything in between, we’ve got you covered. We’re in this together.”³ On its website, NH
14 represents that, “Primary Care [¶] Our friendly doctors are here for you when you’re sick—and
15 when you’re feeling well and want to stay that way.”⁴ On its website, NH maintains an online
16 Patient Portal⁵ and represents on its website that, “Neighborhood’s Patient Portal is a secure and
17 personal way to manage your health care online. Through the Patient Portal, you can review
18 doctor’s notes, get your lab results, update your personal information, request refills for your
19 prescriptions, send and receive messages from your Care Team, and schedule an appointment. The
20 Patient Portal is available online, as well as on Apple and Android devices through the dedicated
21 Patient Portal companion app. Sign up today or call 1-833-867-4642 for more information.”⁶ At all
22 times relevant to this action, including the period from October 22, 2020 to December 3, 2020,
23 Plaintiff and the Class were patients of, received medical treatment and diagnosis from, and
24 provided their personal information, including her name, address, date of birth, social security

25 _____
26 ² (<https://hcpsocal.org/members/>)

27 ³ (<https://www.nhcare.org/services/>)

28 ⁴ (<https://www.nhcare.org/services/>)

⁵ **(Error! Main Document**

Only. https://mycw32.eclinicalweb.com/portal3449/jsp/100mp/login_otp.jsp).

⁶ (<https://www.nhcare.org/programs-resources/>)

1 number, phone number and email address to NH. As a result, at all times relevant to this action,
2 including the period from October 22, 2020 to December 3, 2020, NH possessed Plaintiff's and the
3 SubClass' medical information, in electronic and physical form, in possession of or derived
4 from Defendant regarding their medical history, mental or physical condition, or treatment. Such
5 medical information included or contained an element of personal identifying information sufficient
6 to allow identification of Plaintiff and the SubClass, such as their names, date of birth, addresses,
7 medical record numbers, insurance provider, electronic mail addresses, telephone numbers, or social
8 security numbers, or other information that, alone or in combination with other publicly available
9 information, reveals their identity. At all times relevant to this action, including the period from
10 October 22, 2020 to December 3, 2020, NH maintained and continues to maintain "medical
11 information," within the meaning of Civil Code § 56.05(j), of Plaintiff and the SubClass, each of
12 which are "patients" within the meaning of Civil Code § 56.05(k). At all times relevant to this
13 action, including the period from October 22, 2020 to December 3, 2020, NH was and is a "provider
14 of health care" within the meaning of Civil Code § 56.05(m). At all times relevant to this action,
15 including the period from October 22, 2020 to December 3, 2020, Plaintiff and SubClass members
16 were patients, within the meaning of Civil Code § 56.05(k).

17 19. Plaintiff alleges on information and belief that at all times relevant to this action,
18 including the period from October 22, 2020 to December 3, 2020, NH and HCP disclosed and/or
19 released Plaintiff's, the Class' and the SubClass' medical information, in electronic and physical
20 form, in possession of or derived from NH and/or other providers of health care, regarding their
21 medical history, mental or physical condition, or treatment, to NETGAIN, pursuant to their business
22 associate agreement and/or a service provider agreement. As a result, at all times relevant to this
23 action, including the period from October 22, 2020 to December 3, 2020, NETGAIN possessed
24 Plaintiff's, the SubClass' and the Class' medical information, in electronic and physical form, in
25 possession of or derived from Defendant regarding their medical history, mental or physical
26 condition, or treatment. Such medical information included or contained an element of personal
27 identifying information sufficient to allow identification of Plaintiff, the SubClass and the Class,
28 such as their names, date of birth, addresses, medical record numbers, insurance provider, electronic

1 mail addresses, telephone numbers, or social security numbers, or other information that, alone or in
2 combination with other publicly available information, reveals their identity. At all times relevant
3 to this action, including the period from October 22, 2020 to December 3, 2020, NETGAIN
4 maintained and continues to maintain “medical information,” within the meaning of Civil Code §
5 56.05(j), of Plaintiff and the Class, each of which are “patients” within the meaning of Civil Code §
6 56.05(k).

7 20. At all times relevant to this action, including the period from October 22, 2020 to
8 December 3, 2020, pursuant to Civil Code § 56.06(a), HCP qualifies as a provider of health care
9 because it created, maintained, preserved, and stored records of the care, products and services that
10 Plaintiff and the Class members received in the State of California from HCP’s over 16 member
11 community health centers, 160 member practice sites, 917,000 patients served, and/or other
12 providers of health care, health care service plans, pharmaceutical companies, and contractors, as
13 defined by the Act, is and was organized for the purpose of maintaining medical information, within
14 the meaning of Civil Code § 56.05(j), in order to make the information available to Plaintiff and the
15 Class members or to a provider of health care at the request of Plaintiff and the Class members or a
16 provider of health care, for purposes of allowing Plaintiff and the Class members to manage their
17 information, or for the diagnosis and treatment of Plaintiff and the Class members.

18 21. Alternatively, at all times relevant to this action, including the period from October
19 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.06(b), HCP qualifies as a provider of
20 health care because it offers software and hardware to consumers (including NH) (1) in order to
21 make the information available to an individual or a provider of health care at the request of the
22 individual or a provider of health care, (2) for purposes of allowing the individual to manage his or
23 her information, and (3) for the diagnosis, treatment, or management of a medical condition of the
24 individual.

25 22. Alternatively, at all times relevant to this action, including the period from October
26 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), HCP, as an entity that is a
27 medical group, independent practice association, pharmaceutical benefits manager, or a medical
28

1 service organization, and is not a health care service plan or provider of health care to Plaintiff and
2 the Class members, is and was a “contractor” under Civil Code § 56.05(d).

3 23. Alternatively, at all times relevant to this action, including the period from October
4 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, HCP is and was a recipient of
5 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
6 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
7 further disclosing that medical information except in accordance with a new authorization that
8 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
9 of this chapter or by law.

10 24. Alternatively, at all times relevant to this action, including the period from October
11 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, HCP is and was a recipient of
12 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
13 the Act, and was prohibited from further disclosing such medical information unless in accordance
14 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
15 permitted by other provisions of this chapter or by law.

16 25. Additionally, at all times relevant to this action, including prior to the period from
17 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), HCP is and was an entity
18 engaged in the business of furnishing administrative services to programs that provide payment for
19 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
20 or permitting its employees or agents to use or disclose Plaintiff’s and the Class members’ medical
21 information possessed in connection with performing administrative functions for a program, except
22 as reasonably necessary in connection with the administration or maintenance of the program, or as
23 required by law, or with an authorization.

24 26. As a provider of health care, a contractor, and/or other authorized recipient of
25 personal and confidential medical information, HCP is required by the Act to ensure that medical
26 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
27 patients’ authorization, and to protect and preserve the confidentiality of the medical information
28 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

1 27. Alternatively, at all times relevant to this action, including the period from October
2 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.06(a), NH qualifies as a provider of
3 health care because it created, maintained, preserved, and stored records of the care, products and
4 services that Plaintiff and the Class members received in the State of California from NH and/or
5 other providers of health care, health care service plans, pharmaceutical companies, and contractors,
6 as defined by the Act, is and was organized for the purpose of maintaining medical information,
7 within the meaning of Civil Code § 56.05(j), in order to make the information available to Plaintiff
8 and the Class members or to a provider of health care at the request of Plaintiff and the Class
9 members or a provider of health care, for purposes of allowing Plaintiff and the Class members to
10 manage their information, or for the diagnosis and treatment of Plaintiff and the Class members.

11 28. Alternatively, at all times relevant to this action, including the period from October
12 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.06(b), NH qualifies as a provider of
13 health care because it offers software (an app) to consumers (1) in order to make the information
14 available to an individual or a provider of health care at the request of the individual or a provider of
15 health care, (2) for purposes of allowing the individual to manage his or her information, and (3) for
16 the diagnosis, treatment, or management of a medical condition of the individual.

17 29. Alternatively, at all times relevant to this action, including the period from October
18 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), NH, as an entity that is a medical
19 group, independent practice association, pharmaceutical benefits manager, or a medical service
20 organization, and is not a health care service plan or provider of health care to Plaintiff and the
21 Class members, is and was a “contractor” under Civil Code § 56.05(d).

22 30. Alternatively, at all times relevant to this action, including the period from October
23 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NH is and was a recipient of
24 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
25 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
26 further disclosing that medical information except in accordance with a new authorization that
27 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
28 of this chapter or by law.

1 31. Alternatively, at all times relevant to this action, including the period from October
2 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NH is and was a recipient of
3 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
4 the Act, and was prohibited from further disclosing such medical information unless in accordance
5 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
6 permitted by other provisions of this chapter or by law.

7 32. Additionally, at all times relevant to this action, including prior to the period from
8 October 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.26(a), NH is and was an entity
9 engaged in the business of furnishing administrative services to programs that provide payment for
10 health care services to Plaintiff and the Class, and was prohibited from knowingly using, disclosing
11 or permitting its employees or agents to use or disclose Plaintiff's and the Class members' medical
12 information possessed in connection with performing administrative functions for a program, except
13 as reasonably necessary in connection with the administration or maintenance of the program, or as
14 required by law, or with an authorization.

15 33. As a provider of health care, a contractor, and/or other authorized recipient of
16 personal and confidential medical information, NH is required by the Act to ensure that medical
17 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
18 patients' authorization, and to protect and preserve the confidentiality of the medical information
19 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

20 34. At all times relevant to this action, including the period from October 22, 2020 to
21 December 3, 2020, pursuant to Civil Code § 56.06(a), NETGAIN qualifies as a provider of health
22 care because it created, maintained, preserved, and stored records of the care, products and services
23 that Plaintiff and the Class members received in the State of California from NH and/or other
24 providers of health care, health care service plans, pharmaceutical companies, and contractors, as
25 defined by the Act, is and was organized for the purpose of maintaining medical information, within
26 the meaning of Civil Code § 56.05(j), in order to make the information available to Plaintiff and the
27 Class members or to a provider of health care at the request of Plaintiff and the Class members or a
28

1 provider of health care, for purposes of allowing Plaintiff and the Class members to manage their
2 information, or for the diagnosis and treatment of Plaintiff and the Class members.

3 35. Alternatively, at all times relevant to this action, including the period from October
4 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.06(b), NETGAIN qualifies as a provider
5 of health care because it offers software and hardware to consumers (NH and HCP included) (1) in
6 order to make the information available to an individual or a provider of health care at the request of
7 the individual or a provider of health care, (2) for purposes of allowing the individual to manage his
8 or her information, and (3) for the diagnosis, treatment, or management of a medical condition of
9 the individual.

10 36. Alternatively, at all times relevant to this action, including the period from October
11 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, NETGAIN is and was a recipient of
12 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
13 the Act or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
14 further disclosing that medical information except in accordance with a new authorization that
15 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
16 of this chapter or by law.

17 37. Alternatively, at all times relevant to this action, including the period from October
18 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, NETGAIN is and was a recipient
19 of medical information of Plaintiff and the Class members pursuant to an authorization as provided
20 by the Act, and was prohibited from further disclosing such medical information unless in
21 accordance with a new authorization that meets the requirements of Section 56.21, or as specifically
22 required or permitted by other provisions of this chapter or by law.

23 38. As a provider of health care and/or other authorized recipient of personal and
24 confidential medical information, NETGAIN is required by the Act to ensure that medical
25 information regarding Plaintiff and the Class is not disclosed or disseminated or released without
26 patients' authorization, and to protect and preserve the confidentiality of the medical information
27 regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

28

1 39. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, HCP created, maintained, preserved, and stored records of the care, services and
3 products, including the names, addresses, dates of birth, diagnosis/treatment information and
4 treatment cost information of Plaintiff and the Class (all of which constitutes medical information,
5 as that term is defined and set forth in the Act), that Plaintiff and other Class members received in
6 the State of California from NH and other HCP providers of health care on its computer server.

7 40. At all times relevant to this action, including the period from October 22, 2020 to
8 December 3, 2020, NH created, maintained, preserved, and stored records of the care, services and
9 products, including the names, addresses, dates of birth, diagnosis/treatment information and
10 treatment cost information of Plaintiff and the SubClass (all of which constitutes medical
11 information, as that term is defined and set forth in the Act), that Plaintiff and other SubClass
12 members received in the State of California from NH on its computer network.

13 41. As a result, on or before October 30, 2020, Defendants possessed Plaintiff's,
14 SubClass' and the Class' medical information, in electronic and physical form, in possession of or
15 derived from Defendants regarding their medical history, mental or physical condition, or treatment.
16 Such medical information included or contained an element of personal identifying information
17 sufficient to allow identification of Plaintiff, the SubClass and the Class, such as their names,
18 addresses, dates of birth, social security numbers, phone numbers and/or email addresses, or other
19 information that, alone or in combination with other publicly available information, reveals their
20 identity.

21 42. As providers of health care, contractors, and/or other recipients of medical
22 information, Defendants are required by the Act to ensure that medical information regarding a
23 patient is not disclosed or disseminated or released without their patients' authorization, and to
24 protect and preserve the confidentiality of the medical information regarding a patient, under Civil
25 Code §§ 56.10, 56.26, 56.36, and 56.101.

26 43. As providers of health care, contractors, and/or other recipients of medical
27 information, Defendants are required by the Act not to disclose medical information regarding a
28 patient without first obtaining an authorization under Civil Code §§ 56.10 and 56.26.

1 44. As providers of health care, contractors, and/or other recipients of medical
2 information, Defendants are required by the Act to create, maintain, preserve, and store medical
3 information in a manner that preserves the confidentiality of the information contained therein
4 under Civil Code § 56.101(a).

5 45. As providers of health care, contractors, and/or other recipients of medical
6 information, Defendants are required by the Act to protect and preserve confidentiality of electronic
7 medical information of Plaintiff and the Class in its possession under Civil Code § 56.101(b)(1)(A).

8 46. As providers of health care, contractors, and/or other recipients of medical
9 information, Defendants are required by the Act to take appropriate preventive actions to protect the
10 confidential information or records against release consistent with Defendants' obligations under
11 the Act, under Civil Code § 56.36(e)(2)(E), or other applicable state law, and the Health Insurance
12 Portability and Accountability Act of 1996 (Public Law 104-191) (HIPAA) and all HIPAA
13 Administrative Simplification Regulations in effect on January 1, 2012, contained in Parts 160, 162,
14 and 164 of Title 45 of the Code of Federal Regulations, and Part 2 of Title 42 of the Code of
15 Federal Regulations, including, but not limited to, all of the following:

- 16 i. Developing and implementing security policies and procedures.
17 ii. Designating a security official who is responsible for developing and implementing
18 its security policies and procedures, including educating and training the workforce.
19 iii. Encrypting the information or records, and protecting against the release or use of
20 the encryption key and passwords, or transmitting the information or records in a
21 manner designed to provide equal or greater protections against improper
22 disclosures.

23 47. At all times relevant to this action, including the period from October 22, 2020 to
24 December 3, 2020, HCP created, maintained, preserved, and stored Plaintiff's and the Class
25 members' medical information in an un-encrypted format.

26 48. At all times relevant to this action, including the period from October 22, 2020 to
27 December 3, 2020, NH created, maintained, preserved, and stored Plaintiff's and the SubClass
28 members' medical information in an un-encrypted format.

1 49. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, NH disclosed and/or delivered Plaintiff’s and the SubClass members’ medical
3 information to HCP and NETGAIN. At all times relevant to this action, NH did not obtain written
4 authorization from the Plaintiff and the SubClass prior to disclosing and/or delivering Plaintiff’s and
5 the SubClass members’ medical information to HCP and NETGAIN. Furthermore, NH’s disclosure
6 of and/or delivery of Plaintiff’s and the SubClass members’ medical information to HCP and
7 NETGAIN was not permissible without written authorization from the Plaintiff and the SubClass or
8 under any exemption under Civil Code § 56.10(c).

9 50. At all times relevant to this action, including the period from October 22, 2020 to
10 December 3, 2020, HCP created, maintained, preserved, stored, disclosed and/or delivered
11 Plaintiff’s and the Class members’ medical information to NETGAIN on its computer servers. At
12 all times relevant to this action, HCP did not obtain written authorization from the Plaintiff and the
13 Class prior to creating, maintaining, preserving, storing, disclosing and/or delivering Plaintiff’s and
14 the Class members’ medical information to NETGAIN on its computer servers. Furthermore,
15 NETGAIN’s disclosure of and/or delivery of Plaintiff’s and the Class members’ medical
16 information to NETGAIN on its computer servers was not permissible without written authorization
17 from the Plaintiff and the Class or under any exemption under Civil Code § 56.10(c).

18 51. By law, the HIPAA Privacy Rule applies only to covered entities, e.g. health care
19 providers. However, most health care providers do not carry out all of their health care activities
20 and functions by themselves. Instead, they often use the services of a variety of other persons or
21 businesses. The Privacy Rule allows covered providers to disclose protected health information
22 (PHI) to these “business associates” if the providers obtain assurances that the business associates
23 will use the information only for the purposes for which it was engaged by the covered entity, will
24 safeguard the information from misuse, and will help the covered entity comply with some of the
25 covered entity’s duties under the Privacy Rule. Covered entities may disclose PHI to an entity in its
26 role as a business associate only to help the covered entity carry out its health care functions – not
27 for the business associate’s independent use or purposes, except as needed for the proper
28 management and administration of the business associate. The Privacy Rule requires that a covered

1 entity obtain assurances from its business associate that the business associate will appropriately
2 safeguard the PHI it receives or creates on behalf of the covered entity. The satisfactory assurances
3 must be in writing, whether in the form of a contract or other agreement between the covered entity
4 and the business associate, and requires a covered entity to obtain satisfactory assurances, on an
5 ongoing basis, that the business associate is complying, on an ongoing basis, with cybersecurity and
6 information security standards, and appropriately safeguarding the PHI it receives or creates on
7 behalf of the covered entity.

8 52. When hiring and monitoring a service provider or business associate such as
9 NETGAIN, HCP and NH knew or should have known that they had a duty to inquire about
10 potential service providers' and business associates' cybersecurity programs and how such
11 programs are maintained. HCP and NH knew or should have known that they had a duty to
12 compare potential service providers' and business associates' cybersecurity programs to the
13 industry standards adopted by other healthcare providers, and should evaluate potential service
14 providers' track records in the industry by reviewing public information about data security
15 incidents and litigation. HCP and NH knew or should have known that they had a duty to also ask
16 potential service providers and business associates about whether they have experienced any
17 cybersecurity incidents and how such incidents were handled, as well as whether the potential
18 service provider has an insurance policy in place that would cover losses caused by cybersecurity
19 breaches (including losses caused by internal and external threats). HCP and NH knew or should
20 have known that they had a duty to review service provider and business associate contracts to
21 ensure that the contracts require the service providers to comply, on an ongoing basis, with
22 cybersecurity and information security standards (and avoid contract provisions that limit service
23 providers' responsibility for cybersecurity and information technology breaches). HCP and NH
24 knew or should have known that they had a duty to obtain satisfactory assurances that their service
25 providers and business associates were complying, on an ongoing basis, with cybersecurity and
26 information security standards, and were properly creating, maintaining, preserving, and/or storing
27 the PHI it receives or creates on behalf of HCP and NH, including the confidential, medical and
28 personal identifying information of Plaintiff and the Class. Finally, HCP and NH knew or should

1 have known that they had a duty to pay particular attention to contract terms relating to
2 confidentiality, the use and sharing of information, notice by the vendor of cybersecurity risk
3 assessments and audit reports, cybersecurity breaches and records retention and destruction.

4 53. Plaintiff alleges on information and belief that HCP's and NH's disclosure and/or
5 release of Plaintiff's, the Class' and the SubClass' medical information to NETGAIN was pursuant
6 to their business associate agreement and/or a service provider agreement that was not permissible
7 under the Privacy Rule or any exemption under Civil Code § 56.10(c), and/or because HCP and NH
8 negligently entered into an agreement with NETGAIN that contained provisions that purport or seek
9 to limit NETGAIN's financial responsibility for cybersecurity and information technology breaches,
10 and negligently failed to obtain reasonable assurances and negligently failed to monitor and conduct
11 assessments of NETGAIN to verify that NETGAIN was properly creating, maintaining, preserving,
12 and/or storing the PHI it receives or creates on behalf of HCP and NH, including the confidential,
13 medical and personal identifying information of Plaintiff and the Class, NETGAIN would comply
14 with HIPAA privacy regulations and to follow guidelines and policies to maintain the privacy,
15 confidentiality, including by encryption, and otherwise reasonably protect Plaintiff's and the Class'
16 medical information from disclosure and/or release to at least one unauthorized third party "user"
17 prior to and after HCP's and NH's disclosure and/or release of Plaintiff's and the Class members'
18 medical information to NETGAIN.

19 54. At all times relevant to this action, including the period from October 22, 2020 to
20 December 3, 2020, at least one "unauthorized third party gained access to Netgain's digital
21 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party
22 obtained certain files" containing including Plaintiff's, the SubClass' and the Class' medical
23 information (i.e., their names, addresses, dates of birth, diagnosis/treatment information and
24 treatment cost information) that was located on a NETGAIN server in an un-encrypted format, as
25 represented in HCP's "Notice of Data Breach" form letter submitted to the Attorney General of the
26 State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**.

27 55. Defendants had the resources necessary to protect and preserve confidentiality of
28 electronic medical information of Plaintiff, the SubClass and the Class in their possession, but

1 neglected to adequately implement data security measures as required by HIPPA and the Act,
2 despite their obligation to do so.

3 56. Additionally, the risk of vulnerabilities in its computer and data systems of being
4 exploited by an unauthorized third party trying to steal Plaintiff's, the SubClass' and the Class'
5 electronic personally identifying and medical information was foreseeable and/or known to
6 Defendants. The California Data Breach Report 2012-2015, issued in February 2016 by Attorney
7 General, Kamala D. Harris, reported, "Malware and hacking presents the greatest threat, both in the
8 number of breaches and the number of records breached" and "Social Security numbers and
9 medical information – was breached than other data types." Moreover, as Attorney General further
10 reported, just because "[e]xternal adversaries cause most data breaches, [] this does not mean that
11 organizations are solely victims; they are also stewards of the data they collect and maintain. People
12 entrust businesses and other organizations with their data on the understanding that the
13 organizations have a both an ethical and a legal obligation to protect it from unauthorized access.
14 Neglecting to secure systems and data opens a gateway for attackers, who take advantage of
15 uncontrolled vulnerabilities." Regarding encryption, Attorney General instructed in California Data
16 Breach Report 2012-2015, "As we have said in the past, breaches of this type are preventable.
17 Affordable solutions are widely available: strong full-disk encryption on portable devices and
18 desktop computers when not in use.[] Even small businesses that lack full time information security
19 and IT staff can do this. They owe it to their patients, customers, and employees to do it now."

20 57. More recently the HIPAA Journal posted on November 1, 2018 warned, "Healthcare
21 organization[s] need to ensure that their systems are well protected against cyberattacks, which
22 means investing in technologies to secure the network perimeter, detect intrusions, and block
23 malware and phishing threats."

24 58. Further, it also was foreseeable and/or known to Defendants that negligently
25 creating, maintaining, preserving, and/or storing Plaintiff's, the SubClass' and the Class' medical
26 and personal identifying information, in electronic form, onto Defendants' computer networks in a
27 manner that did not preserve the confidentiality of the information could have a devastating effect
28 on them. As reported in the California Data Breach Report 2012-2015, "There are real costs to

1 individuals. Victims of a data breach are more likely to experience fraud than the general public,
2 according to Javelin Strategy & Research. In 2014, 67 percent of breach victims in the U.S. were
3 also victims of fraud, compared to just 25 percent of all consumers.”

4 59. To be successful, phishing relies on a series of affirmative acts by a company and its
5 employees such as clicking a link, downloading a file, or providing sensitive information. Once
6 criminals gained access to the email accounts of a company and its employees, the email servers
7 communicated—that is, disclosed—the contents of those accounts to the criminals. “Phishing
8 scams are one of the most common ways hackers gain access to sensitive or confidential
9 information. Phishing involves sending fraudulent emails that appear to be from a reputable
10 company, with the goal of deceiving recipients into either clicking on a malicious link or
11 downloading an infected attachment, usually to steal financial or confidential information.”
12 (<https://www.varonis.com/blog/data-breach-statistics/>). As posted on April 21, 2020, the FBI had
13 issued a fresh warning [Alert Number MI-000122-MW] following an increase in COVID-19
14 phishing scams targeting healthcare providers.

15 60. At all times relevant to this action, including the period from October 22, 2020 to
16 December 3, 2020, Defendants negligently created, maintained, preserved, and/or stored Plaintiff’s,
17 the SubClass’ and the Class’ medical information, including Plaintiff’s, the SubClass’ and the
18 Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
19 information, in electronic form, onto Defendants’ computer networks in a manner that did not
20 preserve the confidentiality of the information, and negligently failed to protect and preserve
21 confidentiality of electronic medical information of Plaintiff, the SubClass and the Class in their
22 possession, as required by HIPPA and the Act, and specifically, under Civil Code §§ 56.10(a),
23 56.26(a), 56.36(e)(2)(E), 56.101(a), and 56.101(b)(1)(A), and according to their written
24 representations to Plaintiff and the Class.

25 61. Had Defendants taken such appropriate preventive actions, fix the deficiencies in
26 their data security systems and adopted security measures as required by HIPPA and the Act from
27 October 22, 2020 to December 3, 2020, Defendants could have prevented Plaintiff’s and the Class’
28

1 electronic medical information within Defendants' computer networks from being accessed and
2 actually viewed by unauthorized third parties.

3 62. At all times relevant to this action, including the period of from October 22, 2020 to
4 December 3, 2020, NH, by disclosing and/or delivering Plaintiff's and the SubClass' personal
5 identifying and medical information to HCP, allowed Plaintiff's and the SubClass' personal
6 identifying and medical information to be accessed and actually viewed by at least one unauthorized
7 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
8 Code § 56.10(a).

9 63. At all times relevant to this action, including the period of from October 22, 2020 to
10 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic
11 medical information of Plaintiff and the SubClass on NETGAIN's computer server, allowed
12 Plaintiff's and the SubClass' medical and personal identifying information to be accessed and
13 actually viewed by at least one unauthorized third party, without first obtaining an authorization,
14 constituting a disclosure in violation of Civil Code § 56.10(a).

15 64. At all times relevant to this action, including the period from October 22, 2020 to
16 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
17 medical information of Plaintiff and the Class on NETGAIN's computer server, allowed Plaintiff's
18 and the Class' medical and personal identifying information to be accessed and actually viewed by
19 at least one unauthorized third party, without first obtaining an authorization, constituting a
20 disclosure in violation of Civil Code § 56.10(a).

21 65. At all times relevant to this action, including the period from October 22, 2020 to
22 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
23 medical information of Plaintiff and the Class on NETGAIN's computer server, allowed Plaintiff's
24 and the Class' medical and personal identifying information to be accessed and actually viewed by
25 at least one unauthorized third party, without first obtaining an authorization, constituting a
26 disclosure in violation of Civil Code § 56.26(a).

27 66. At all times relevant to this action, including the period from October 22, 2020 to
28 December 3, 2020, NH, by disclosing and/or delivering Plaintiff's and the SubClass members'

1 medical and personal identifying information to HCP, allowed Plaintiff's and the SubClass' medical
2 and personal identifying information to be accessed and actually viewed by at least one
3 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

4 67. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, NH, by negligently creating, maintaining, preserving, and storing the electronic
6 medical information of Plaintiff and the SubClass on NETGAIN's computer server, allowed
7 Plaintiff's and the SubClass' medical and personal identifying information to be accessed and
8 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
9 Code § 56.101(a).

10 68. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, HCP, by negligently creating, maintaining, preserving, and storing the electronic
12 medical information of Plaintiff and the Class on NETGAIN's computer server, allowed Plaintiff's
13 and the Class' medical and personal identifying information to be accessed and actually viewed by
14 at least one unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

15 69. At all times relevant to this action, including the period from October 22, 2020 to
16 December 3, 2020, NH, by disclosing and/or delivering Plaintiff's and the SubClass members'
17 medical and personal identifying information to HCP, allowed Plaintiff's and the SubClass' medical
18 and personal identifying information to be accessed and actually viewed by at least one
19 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

20 70. At all times relevant to this action, including the period from October 22, 2020 to
21 December 3, 2020, NH's negligent failure to protect and preserve confidentiality of electronic
22 medical information of Plaintiff and the SubClass, on NETGAIN's computer server, allowed
23 Plaintiff's and the SubClass' medical and personal identifying information to be accessed and
24 actually viewed by at least one unauthorized third party, constituting a release in violation of Civil
25 Code § 56.101(b)(1)(A).

26 71. At all times relevant to this action, including the period from October 22, 2020 to
27 December 3, 2020, HCP's negligent failure to protect and preserve confidentiality of electronic
28 medical information of Plaintiff and the Class, on NETGAIN's computer server, allowed Plaintiff's

1 and the Class' medical and personal identifying information to be accessed and actually viewed by
2 at least one unauthorized third party, constituting a release in violation of Civil Code §
3 56.101(b)(1)(A).

4 72. On or about April 12, 2021, HCP caused a form letter, entitled "**Notice of Data**
5 **Breach**," dated April 12, 2021, signed by Henry Tuttle, President & Chief Executive Officer,
6 Health Center Partners of Southern California, to be mailed to Plaintiff and the Class, informing
7 them, in part, of "a recent data security incident experienced by Netgain Technology, LLC
8 ('Netgain'), the IT service provider for Health Center Partners of Southern California ('HCP')" and
9 stating, in part, "HCP supports community health centers in a variety of ways, including
10 collaborative grant-funded programs and services for Neighborhood Healthcare.... **What**
11 **Happened:** Netgain recently informed HCP that it had experienced a data security incident that
12 involved systems containing HCP data.... According to Netgain, in late September 2020, an
13 unauthorized third party gained access to Netgain's digital environment, and between October 22,
14 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data.
15 Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the
16 attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the
17 data.... The information involved varies depending on the individual but may include the following:
18 name, address, date of birth, diagnosis/treatment information and treatment cost information. Once
19 we learned that HCP data may have been involved in the incident, we worked with our
20 cybersecurity experts to review the impacted files and identify the individuals whose information
21 was contained in such files so that we may notify such individuals. Our investigation revealed that
22 the impacted files contained your personal information." An exemplar of HCP's "**Notice of Data**
23 **Breach**" form letter submitted to the Attorney General of the State of California and mailed to
24 Plaintiff and the Class is attached hereto as **Exhibit A**. Plaintiff received in the mail a HCP "**Notice**
25 **of Data Breach**" form letter, addressed to her, which alerted Plaintiff that her medical and personal
26 identifying information, along with other Class members, was improperly accessed by at least one
27 unauthorized third party. As a result, Plaintiff fears that disclosure and/or release of her medical
28 and personal identifying information created, maintained, preserved, and/or stored on Defendants'

1 computer networks could subject her to harassment or abuse. Moreover, although thereafter, on
2 May 4, 2021, Plaintiff wrote both HCP and NH separately requesting further information about this
3 security incident, neither HCP nor NH provided a substantive response to her requests.

4 73. HCP’s “**Notice of Data Breach**” form letter submitted to the Attorney General of
5 the State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**, further
6 states, “**What We Are Doing:** [] We are providing you with steps that you can take to help protect
7 your personal information, and as an added precaution, we are offering you complimentary identity
8 protection services through IDX, a leader in risk mitigation and response.”

9 74. HCP’s “**Notice of Data Breach**” form letter concludes by making the following
10 hollow gesture, “The security of your information is a top priority for HCP, and we are committed
11 to safeguarding your data and privacy.” Other than offering “steps that you can take to help protect
12 your personal information” and “complimentary identity protection services through IDX” “as an
13 added precaution,” HCP’s “**Notice of Data Breach**” form letter does nothing to further protect
14 Plaintiff and the Class from future incidents of identity theft despite the severity of the unauthorized
15 access, viewing, exfiltration, theft, disclosure and/or release of their electronic medical and personal
16 information caused by Defendants’ violations of their duty to implement and maintain reasonable
17 security procedures and practices.

18 75. To date, other than offering “steps that you can take to help protect your personal
19 information” and “complimentary identity protection services through IDX” “as an added
20 precaution,” HCP has not offered any monetary compensation for the unauthorized disclosure
21 and/or release of Plaintiff’s and the Class’ electronic medical information under the Act. In effect,
22 HCP is shirking its responsibility for the harm it has caused, while shifting the burdens and costs of
23 its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

24 76. To date, NH has not offered any compensation for the unauthorized disclosure and/or
25 release of Plaintiff’s and SubClass’ electronic medical information under the Act. In effect, NH is
26 shirking its responsibility for the harm it has caused, while shifting the burdens and costs of its
27 wrongful conduct onto its patients, i.e. Plaintiff and the SubClass.

28

1 77. To date, NETGAIN has not offered any monetary compensation for the unauthorized
2 disclosure and/or release of Plaintiff’s and the Class’ electronic medical information under the Act.
3 In effect, NETGAIN is shirking its responsibility for the harm it has caused, while shifting the
4 burdens and costs of its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

5 78. Based upon the information posted on the U.S. Department of Health and Human
6 Services’ official website, HCP reported on “04/09/2021” a “Hacking/IT Incident” involving
7 “Network Server” affecting “293,516” persons, which involved a “Business Associate,” to the U.S.
8 Department of Health & Human Services’ Office for Civil Rights.

9 79. Based upon the information posted on the U.S. Department of Health and Human
10 Services’ official website, NH reported on “04/14/2021” a “Hacking/IT Incident” involving
11 “Network Server” affecting “45,200” persons, which involved a “Business Associate,” to the U.S.
12 Department of Health & Human Services’ Office for Civil Rights.

13 80. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA
14 covered entities to provide notification following a breach of unsecured protected health
15 information. Following a breach of unsecured protected health information, covered entities must
16 provide notification of the breach to affected individuals. Covered entities must *only* provide the
17 required notifications if the breach involved unsecured protected health information. Unsecured
18 protected health information is protected health information (PHI) that has not been rendered
19 unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or
20 methodology specified by the Secretary of the U.S. Department of Health and Human Services in
21 guidance. Under approved guidance of the U.S. Department of Health and Human Services, PHI is
22 rendered unusable, unreadable, or indecipherable to unauthorized individuals if (1) electronic PHI
23 has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process
24 to transform data into a form in which there is a low probability of assigning meaning without use
25 of a confidential process or key” (45 CFR 164.304 definition of encryption) and (2) such
26 confidential process or key that might enable decryption has not been breached. By reporting this
27 incident to the U.S. Department of Health and Human Services, HCP and NH each has separately
28 determined and is affirming that Plaintiff’s, the Class’ and the SubClass’ electronic PHI was either

1 not encrypted at all, or if it was encrypted, the encryption has been breached by the unauthorized
2 third party. Further, because Plaintiff's, the Class' and the SubClass' identifiable medical
3 information contained in NETGAIN's computer server was not rendered unusable, unreadable, or
4 indecipherable, the unauthorized third party or parties who "obtained" and downloaded Plaintiff's
5 and the Class' identifiable medical information was able to and did actually view Plaintiff's, the
6 Class' and the SubClass' electronic medical information contained in and "obtained" and
7 downloaded from NETGAIN's computer server. As a result, HCP and NH each has separately
8 determined and have affirmed that Plaintiff's, the Class' and the SubClass' identifiable medical
9 information contained in NETGAIN's computer server was unencrypted and thus, the unauthorized
10 third party or parties who "obtained" and downloaded Plaintiff's, the Class' and the SubClass'
11 identifiable medical information was able to and did actually view Plaintiff's, the Class' and the
12 SubClass' electronic medical information contained in and "obtained" and downloaded from
13 NETGAIN's computer server. Therefore, HCP, NH and NETGAIN was negligent for failing to
14 encrypt or adequately encrypt Plaintiff's, the Class' and the SubClass' electronic medical
15 information contained in NETGAIN's computer server.

16 81. As a result, Defendants were negligent for failing to encrypt or adequately encrypt
17 Plaintiff's, the Class' and the SubClass' electronic medical information on their computer networks.
18 Further, because Plaintiff's, the Class' and the SubClass' identifiable medical information on
19 Defendants' computer networks was not rendered unusable, unreadable, or indecipherable, the
20 unauthorized third party or parties who accessed Plaintiff's, the Class' and the SubClass'
21 identifiable medical information was able to and did view Plaintiff's, the Class' and the SubClass'
22 electronic medical information contained within NETGAIN's computer server.

23 **CLASS ACTION ALLEGATIONS**

24 82. Plaintiff brings this action on behalf of herself individually and on behalf of all
25 others similarly situated. The putative class and subclass that Plaintiff seeks to represent is defined
26 as follows:

27 Class: All persons to whom Health Center Partners of Southern California sent a
28 notification letter of a data security incident that has occurred between October

1 22, 2020 to December 3, 2020, an exemplar of which is attached hereto as
2 **Exhibit A.**

3 SubClass: All persons to whom Neighborhood Healthcare sent a notification
4 letter of a data security incident that has occurred between November 24, 2020 to
December 3, 2020, an exemplar of which is attached hereto as **Exhibit B.**

5 The officers, directors, employees, and agents of Defendants and any “affiliate,” “principal” or
6 “subsidiary” of Defendants, as defined in the Corporations Code §§ 150, 175, and 189, respectively,
7 are excluded from the Class and the SubClass. Plaintiff reserves the right under California Rule of
8 Court 3.765 to amend or modify the Class definition with greater particularity or further division
9 into subclasses or limitation to particular issues as warranted, and as additional facts are discovery
10 by Plaintiff during her future investigations.

11
12 83. This action is properly maintainable as a class action. The members of the Class and
13 the SubClass are so numerous that joinder of all members is impracticable, if not completely
14 impossible. While the exact number of the Class is unknown to Plaintiff at this time, HCP filed a
15 report with the U.S. Department of Health & Human Services’ Office for Civil Rights, on or about
16 December 28, 2020, that this incident affected 293,516 persons. The disposition of the claims of
17 the members of Class through this class action will benefit both the parties and this Court. In
18 addition, the Class and the SubClass is readily identifiable from information and records in the
19 possession of Defendants and their agents, and the Class and the SubClass is defined in objective
20 terms that make the eventual identification of the Class and the SubClass members possible and/or
21 sufficient to allow members of the Class and the SubClass identify themselves as having a right to
22 recover.

23 84. There is a well-defined community of interest among the members of the Class and
24 the SubClass because common questions of law and fact predominate, Plaintiff’s claims are typical
25 of the members of the class, and Plaintiff can fairly and adequately represent the interests of the
26 Class.

27 85. Common questions of law and fact exist as to all members of the Class and the
28 SubClass and predominate over any questions affecting solely individual members of the Class and

1 the SubClass. Among the questions of law and fact common to the Class that predominate over
2 questions which may affect individual Class members, including the following:

- 3 a) Whether Defendants possessed Plaintiff's, the SubClass' and the Class' medical and
4 personal identifying information from October 22, 2020 to December 3, 2020;
- 5 b) Whether Defendants created, maintained, preserved and/or stored Plaintiff's, the
6 SubClass' and the Class' medical and personal identifying information, in electronic
7 form, onto Defendants' computer networks from October 22, 2020 to December 3,
8 2020;
- 9 c) Whether Defendants implemented and maintained reasonable security procedures
10 and practices to protect Plaintiff's, the SubClass' and the Class' medical and
11 personal identifying information, in electronic form, within Defendants' computer
12 networks from October 22, 2020 to December 3, 2020;
- 13 d) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
14 information, in electronic form, within Defendants' computer networks from October
15 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
16 exposed by an unauthorized third party;
- 17 e) Whether Plaintiff's, the SubClass' and the Class' medical and personal identifying
18 information, in electronic form, within Defendants' computer networks from October
19 22, 2020 to December 3, 2020 was accessed, viewed, exfiltrated and/or publicly
20 exposed by an unauthorized third party without the prior written authorization of
21 Plaintiff, the SubClass and the Class, as required by Civil Code §§ 56.10 and 56.26;
- 22 f) Whether Defendants' creation, maintenance, preservation and/or storage of
23 Plaintiff's, the SubClass' and the Class' medical and personal identifying
24 information, in electronic form, within Defendants' computer networks, accessed,
25 viewed, exfiltrated and/or publicly exposed by an unauthorized third party was
26 permissible without written authorization from Plaintiff, the SubClass and the Class
27 or under any exemption under Civil Code § 56.10(c);
- 28

- 1 g) Whether Defendants’ creation, maintenance, preservation and/or storage of
- 2 Plaintiff’s, the SubClass’ and the Class’ medical and personal identifying
- 3 information, in electronic form, within Defendants’ computer networks, accessed,
- 4 viewed, exfiltrated and/or publicly exposed by an unauthorized third party
- 5 constitutes a release in violation of Civil Code §56.101;
- 6 h) Whether the timing of HCP’s notice that Plaintiff’s and the Class’ medical and
- 7 personal identifying information, in electronic form, was accessed, viewed,
- 8 exfiltrated and/or publicly exposed by an unauthorized third party, was given in the
- 9 most expedient time possible and without reasonable delay;
- 10 i) Whether Defendants’ conduct constitute unlawful, fraudulent or unfair practices in
- 11 violation of Business and Professions Code §§ 17200, *et seq.*; and
- 12 j) Whether Plaintiff, the SubClass and the Class are entitled to actual, nominal or
- 13 statutory damages, injunctive relief and/or restitution.

14 86. Plaintiff’s claims are typical of those of the other SubClass and Class members
15 because Plaintiff, like every other SubClass and Class member, were exposed to virtually identical
16 conduct and now suffer from the same violations of the law as other SubClass and Class members.

17 87. Plaintiff will fairly and adequately protect the interests of the SubClass and the
18 Class. Moreover, Plaintiff has no interest that is contrary to or in conflict with those of the
19 SubClass and the Class, she seeks to represent. In addition, Plaintiff has retained competent counsel
20 experienced in class action litigation to further ensure such protection and intend to prosecute this
21 action vigorously.

22 88. The nature of this action and the nature of laws available to Plaintiff and the other
23 SubClass and Class members make the use of the class action format a particularly efficient and
24 appropriate procedure to afford relief to Plaintiff and the other SubClass and Class members for the
25 claims alleged and the disposition of whose claims in a class action will provide substantial benefits
26 to both the parties and the Court because:

- 27 a) If each of the SubClass and the Class members were required to file an individual
- 28 lawsuit, the Defendants would necessarily gain an unconscionable advantage since

- 1 they would be able to exploit and overwhelm the limited resources of each individual
2 member of the SubClass and Class with its vastly superior financial and legal
3 resources;
- 4 b) The costs of individual suits could unreasonably consume the amounts that would be
5 recovered;
- 6 c) Proof of a common business practice or factual pattern which Plaintiff experienced is
7 representative of that experienced by the SubClass and the Class and will establish
8 the right of each of the members to recover on the causes of action alleged;
- 9 d) Individual actions would create a risk of inconsistent results and would be
10 unnecessary and duplicative of this litigation; and
- 11 e) The disposition of the claims of the members of the SubClass and the Class through
12 this class action will produce salutary by-products, including a therapeutic effect
13 upon those who indulge in fraudulent practices, and aid to legitimate business
14 enterprises by curtailing illegitimate competition.

15 89. The prosecution of separate actions by individual members of the SubClass and the
16 Class would create a risk of inconsistent or varying adjudications with respect to individual
17 members of the SubClass and the Class, which would establish incompatible standards of conduct
18 for the Defendants in the State of California and would lead to repetitious trials of the numerous
19 common questions of fact and law in the State of California. Plaintiff knows of no difficulty that
20 will be encountered in the management of this litigation that would preclude its maintenance as a
21 class action. As a result, a class action is superior to other available methods for the fair and
22 efficient adjudication of this controversy.

23 90. Notice to the members of the SubClass and the Class may be made by e-mail or first-
24 class mail addressed to all persons who have been individually identified by Defendants and who
25 have been given notice of the data breach.

26 91. Plaintiff, the SubClass and the Class have suffered irreparable harm and damages
27 because of Defendants' wrongful conduct as alleged herein. Absent certification, Plaintiff, the
28 SubClass and the Class will continue to be damaged and to suffer by the unauthorized disclosure

1 and/or release of their medical and personal identifying information, thereby allowing these
2 violations of law to proceed without remedy.

3 92. Moreover, Plaintiff’s, the SubClass’ and the Class’ individual damages are
4 insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendants’
5 violations of law inflicting substantial damages in the aggregate would go unremedied. In addition,
6 Defendants have acted or refused to act on grounds generally applicable to Plaintiff, the SubClass
7 and the Class, thereby making appropriate final injunctive relief with respect to, the Class as a
8 whole.

9 **FIRST CAUSE OF ACTION**
10 **Violations of the Confidentiality of Medical Information Act**
11 **California Civil Code §§ 56, et seq.**
12 **(On Behalf of Plaintiff and the SubClass Against NH)**

13 93. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
14 fully stated herein.

15 94. At all times relevant to this action, including the period from October 22, 2020 to
16 December 3, 2020, NH is considered a “provider of health care,” within the meaning of Civil Code
17 §§ 56.05(m) and 56.06(a) & (b), and maintained and continues to maintain “medical information”
18 within the meaning of Civil Code § 56.05(j), of Plaintiff and the SubClass.

19 95. Plaintiff and the SubClass are “patients” of NH within the meaning of Civil Code §
20 56.05(k) and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that
21 disclosure and/or release of their medical information could subject them to harassment or abuse.

22 96. At all times relevant to this action, including the period from October 22, 2020 to
23 December 3, 2020, NH negligently created, maintained, preserved, and/or stored Plaintiff’s and the
24 SubClass’ medical information, including Plaintiff’s and the SubClass’ names, addresses, dates of
25 birth, diagnosis/treatment information and treatment cost information, in electronic form, onto
26 Defendants’ computer networks in a manner that did not preserve the confidentiality of the
27 information, and negligently failed to protect and preserve confidentiality of electronic medical
28 information of Plaintiff and the SubClass in its possession, as required by the Act, and specifically,

1 under Civil Code §§ 56.06(d), 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
2 56.36(e)(2)(E), and according to their written representations to Plaintiff and the SubClass.

3 97. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass members'
4 medical and personal identifying information to HCP without written authorization from Plaintiff
5 and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff's and
6 the SubClass' medical information, including Plaintiff's and the SubClass' names, addresses, dates
7 of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be
8 accessed and actually viewed by at least one unauthorized third party, without first obtaining an
9 authorization, constituting a disclosure in violation of Civil Code §§ 56.06(d), 56.10, 56.13, 56.245,
10 and 56.26(a).

11 98. Due to NH's negligent creation, maintenance, preservation and/or storage of
12 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server, NH
13 allowed Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass'
14 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
15 electronic form, to be accessed and actually viewed by at least one unauthorized third party, without
16 first obtaining an authorization, constituting a disclosure in violation of Civil Code §§ 56.06(d),
17 56.10, 56.13, 56.245, and 56.26(a).

18 99. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass members'
19 medical and personal identifying information to HCP without written authorization from Plaintiff
20 and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed Plaintiff's and
21 the SubClass' medical information, including Plaintiff's and the SubClass' names, addresses, dates
22 of birth, diagnosis/treatment information and treatment cost information, in electronic form, to be
23 accessed and actually viewed by at least one unauthorized third party, constituting a release in
24 violation of Civil Code § 56.101(a).

25 100. Due to NH's negligent creation, maintenance, preservation and/or storage of
26 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server,
27 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
28 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in

1 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
2 constituting a release in violation of Civil Code § 56.101(a).

3 101. Due to NH's disclosure and/or delivery Plaintiff's and the SubClass' medical
4 information and personal identifying information to HCP without written authorization from
5 Plaintiff and the SubClass or under any exemption under Civil Code § 56.10(c), NH allowed
6 Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass' names,
7 addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
8 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
9 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

10 102. Due to NH's negligent creation, maintenance, preservation and/or storage of
11 Plaintiff's and the SubClass members' medical information on NETGAIN's computer server, NH
12 allowed Plaintiff's and the SubClass' medical information, including Plaintiff's and the SubClass'
13 names, addresses, dates of birth, diagnosis/treatment information and treatment cost information, in
14 electronic form, to be accessed and actually viewed by at least one unauthorized third party,
15 constituting a release in violation of Civil Code § 56.101(b)(1)(A).

16 103. As a result of NH's above-described conduct in violation of the Act, Plaintiff and the
17 SubClass have suffered damages from the unauthorized disclosure and/or release of their medical
18 and personal identifying information made unlawful by Civil Code §§ 56.06(d), 56.10, 56.101.

19 104. As a result of NHs' above-described conduct in violation of the Act, Plaintiff and the
20 SubClass seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
21 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
22 Code § 56.36(b)(2).

23 **SECOND CAUSE OF ACTION**
24 **Violations of the Confidentiality of Medical Information Act**
25 **California Civil Code §§ 56, et seq.**
(On Behalf of Plaintiff and the Class Against HCP)

26 105. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
27 fully stated herein.

28

1 106. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, HCP is considered a “provider of health care” within the meaning of Civil Code
3 § 56.05(m) and 56.06(a) & (b), a “contractor” under Civil Code § 56.05(d), and/or “engaged in the
4 business of furnishing administrative services to programs that provide payment for health care
5 services” under Civil Code § 56.26(a), and maintained and continues to maintain “medical
6 information” within the meaning of Civil Code § 56.05(j), of Plaintiff and the Class.

7 107. Plaintiff and the Class are “patients” within the meaning of Civil Code § 56.05(k)
8 and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure
9 and/or release of their medical information could subject them to harassment or abuse.

10 108. At all times relevant to this action, including the period from October 22, 2020 to
11 December 3, 2020, HCP negligently created, maintained, preserved, and/or stored Plaintiff’s and the
12 Class’ medical information, including Plaintiff’s and the Class’ names, addresses, dates of birth,
13 diagnosis/treatment information and treatment cost information, in electronic form, onto
14 NETGAIN’s computer server in a manner that did not preserve the confidentiality of the
15 information, and negligently failed to protect and preserve confidentiality of electronic medical
16 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
17 under Civil Code §§ 56.06(d), 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
18 56.36(e)(2)(E).

19 109. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
20 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
21 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
22 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
23 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
24 third party, without first obtaining an authorization, constituting a disclosure in violation of Civil
25 Code §§ 56.06(d), 56.10, 56.13, 56.245, and 56.26(a).

26 110. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
27 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
28 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s

1 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
2 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
3 third party, constituting a release in violation of Civil Code § 56.101(a).

4 111. Due to HCP’s negligent creation, maintenance, preservation and/or storage of
5 Plaintiff’s and the Class members’ medical and personal identifying information on NETGAIN’s
6 computer server, HCP allowed Plaintiff’s and the Class’ medical information, including Plaintiff’s
7 and the Class’ names, addresses, dates of birth, diagnosis/treatment information and treatment cost
8 information, in electronic form, to be accessed and actually viewed by at least one unauthorized
9 third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

10 112. As a result of HCP’s above-described conduct in violation of the Act, Plaintiff and
11 the Class have suffered damages from the unauthorized disclosure and/or release of their medical
12 and personal identifying information made unlawful by Civil Code §§ 56.06(d), 56.10, 56.101.

13 113. As a result of HCP’s above-described conduct in violation of the Act, Plaintiff and
14 the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
15 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
16 Code § 56.36(b)(2).

17 **THIRD CAUSE OF ACTION**
18 **Violations of the Confidentiality of Medical Information Act**
19 **California Civil Code §§ 56, et seq.**
20 **(On Behalf of Plaintiff and the Class Against NETGAIN)**

21 114. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
22 fully stated herein.

23 115. At all times relevant to this action, including the period from October 22, 2020 to
24 December 3, 2020, NETGAIN is considered a “provider of health care” within the meaning of Civil
25 Code §§ 56.05(m) and 56.06(a) & (b), and maintained and continues to maintain “medical
26 information” within the meaning of Civil Code § 56.05(j), of Plaintiff and the Class.

27 116. Plaintiff and the Class are “patients” within the meaning of Civil Code § 56.05(k)
28 and are “Endanger” within the meaning of Civil Code § 56.05(e) because they fear that disclosure
and/or release of their medical information could subject them to harassment or abuse.

1 117. At all times relevant to this action, including the period from October 22, 2020 to
2 December 3, 2020, NETGAIN negligently created, maintained, preserved, and/or stored Plaintiff's
3 and the Class' medical information, including Plaintiff's and the Class' names, addresses, dates of
4 birth, diagnosis/treatment information and treatment cost information, in electronic form, onto
5 NETGAIN's computer server in a manner that did not preserve the confidentiality of the
6 information, and negligently failed to protect and preserve confidentiality of electronic medical
7 information of Plaintiff and the Class in its possession, as required by the Act, and specifically,
8 under Civil Code §§ 56.06(d), 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and
9 56.36(e)(2)(E).

10 118. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
11 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
12 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
13 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
14 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
15 unauthorized third party, without first obtaining an authorization, constituting a disclosure in
16 violation of Civil Code §§ 56.06(d), 56.10, 56.13, 56.245, and 56.26(a).

17 119. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
18 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
19 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
20 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
21 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
22 unauthorized third party, constituting a release in violation of Civil Code § 56.101(a).

23 120. Due to NETGAIN's negligent creation, maintenance, preservation and/or storage of
24 Plaintiff's and the Class members' medical and personal identifying information on NETGAIN's
25 computer server, NETGAIN allowed Plaintiff's and the Class' medical information, including
26 Plaintiff's and the Class' names, addresses, dates of birth, diagnosis/treatment information and
27 treatment cost information, in electronic form, to be accessed and actually viewed by at least one
28 unauthorized third party, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

1 121. As a result of NETGAIN’s above-described conduct in violation of the Act, Plaintiff
2 and the Class have suffered damages from the unauthorized disclosure and/or release of their
3 medical and personal identifying information made unlawful by Civil Code §§ 56.06(d), 56.10,
4 56.101.

5 122. As a result of NETGAIN’s above-described conduct in violation of the Act, Plaintiff
6 and the Class seek nominal damages of one thousand dollars (\$1,000) for each violation under Civil
7 Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil
8 Code § 56.36(b)(2).

9 **FOURTH CAUSE OF ACTION**
10 **Breach of California Security Notification Laws**
11 **California Civil Code § 1798.82**
(On Behalf of Plaintiff and the Class Against HCP)

12 123. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
13 fully stated herein.

14 124. Pursuant to Civil Code § 1798.82(a), “A person or business that conducts business in
15 California, and that owns or licenses computerized data that includes personal information, shall
16 disclose a breach of the security of the system following discovery or notification of the breach in
17 the security of the data to a resident of California (1) whose unencrypted personal information was,
18 or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted
19 personal information was, or is reasonably believed to have been, acquired by an unauthorized
20 person and the encryption key or security credential was, or is reasonably believed to have been,
21 acquired by an unauthorized person and the person or business that owns or licenses the encrypted
22 information has a reasonable belief that the encryption key or security credential could render that
23 personal information readable or usable. The disclosure shall be made in the most expedient time
24 possible and without unreasonable delay, consistent with the legitimate needs of law enforcement,
25 as provided in subdivision (c), or any measures necessary to determine the scope of the breach and
26 restore the reasonable integrity of the data system.” Prior to passages of such statute, the California
27 State Assembly cited an incident where authorities knew of the breach in security for 21 days
28 “before state workers were told” as an example of “late notice.”

1 125. Civil Code § 1798.82 further provides, “(h) For purposes of this section, ‘personal
2 information’ means an individual’s first name or first initial and last name in combination with any
3 one or more of the following data elements, when either the name or the data elements are not
4 encrypted: (1) Social security number. (2) Driver’s license number or California Identification Card
5 number. (3) Account number, credit or debit card number, in combination with any required
6 security code, access code, or password that would permit access to an individual’s financial
7 account. (4) Medical information. (5) Health insurance information. (i) (2) For purposes of this
8 section, ‘medical information’ means any information regarding an individual’s medical history,
9 mental or physical condition, or medical treatment or diagnosis by a health care professional. (3)
10 For purposes of this section, ‘health insurance information’ means an individual’s health insurance
11 policy number or subscriber identification number, any unique identifier used by a health insurer to
12 identify the individual, or any information in an individual’s application and claims history,
13 including any appeals records.”

14 126. HCP conducts business in California and owns or licenses computerized data which
15 includes the personal information, within the meaning of Civil Code § 1798.82(h), of Plaintiff and
16 the Class.

17 127. Based upon NH’s “**Notice of Data Breach**” form letter, HCP was aware that
18 Plaintiff’s and the Class’ unencrypted personal information on NETGAIN’s computer server was,
19 or is reasonably believed to have been, acquired by an unauthorized person no later than December
20 3, 2020, but did not begin to mail notification letters to Plaintiff and the Class until April 12, 2021.
21 Thus, HCP waited at least 131 days before *beginning* to inform Plaintiff and the Class of this
22 incident and the subsequent threat to Plaintiff’s and the Class’ personal information. As a result,
23 HCP did not disclose to Plaintiff and the Class that their personal information was, or was
24 reasonably believed to have been, acquired by an unauthorized person, in the most expedient time
25 possible and without reasonable delay in violation of Civil Code § 1798.82(a). Given the example
26 of the Legislature finding that a delay of 21 days to be “late notice” under the statute, HCP’s delay
27 of 131 days before *beginning* to inform Plaintiff and the Class that their personal information was,
28 or was reasonably believed to have been, acquired by an unauthorized person by mailing HCP’s

1 form letter to Plaintiff and the Class is presumptively unreasonable notice in violation of Civil Code
2 § 1798.82(a).

3 128. Plaintiff and the Class have been injured by fact that HCP did not disclose their
4 personal information was, or was reasonably believed to have been, acquired by an unauthorized
5 person in the most expedient time possible and without reasonable delay in violation of Civil Code
6 § 1798.82(a). HCP’s delays in informing required by Civil Code § 1798.82(a) and providing all of
7 the information required by Civil Code § 1798.82(d) to Plaintiff and the Class that their personal
8 information was, or was reasonably believed to have been, acquired by an unauthorized person,
9 have prevented Plaintiff and the Class from taking steps to protect their personal information from
10 unauthorized use and/or identify theft.

11 129. Plaintiff and the Class seek recovery of their damages pursuant to Civil Code §
12 1798.84(b) and injunctive relief pursuant to Civil Code § 1798.84(e).

13 **FIFTH CAUSE OF ACTION**
14 **Unlawful and Unfair Business Acts and Practices in Violation of**
15 **California Business & Professions Code §17200, *et seq.***
16 **(On Behalf of Plaintiff, the SubClass and the Class Against All Defendants)**

17 130. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
18 fully stated herein.

19 131. The acts, misrepresentations, omissions, practices, and non-disclosures of
20 Defendants as alleged herein constituted unlawful and unfair business acts and practices within the
21 meaning of California Business & Professions Code §§ 17200, *et seq.*

22 132. By the aforementioned business acts or practices, Defendants have engaged in
23 “unlawful” business acts and practices in violation of the aforementioned statutes, including Civil
24 Code §§ 56.06(d), 56.10(a), 56.26(a), 56.36(e)(2)(E), 56.101(a), 56.101(b)(1)(A), 1798.82(a) and
25 1798.82(d). Plaintiff reserves the right to allege other violations of law committed by Defendants
26 which constitute unlawful acts or practices within the meaning of California Business & Professions
27 Code §§ 17200, *et seq.*

28 133. By the aforementioned business acts or practices, Defendants have also engaged in
“unfair” business acts or practices in that the harm caused by Defendants’ failure to maintain

1 adequate information security procedures and practices, including but not limited to, failing to take
2 adequate and reasonable measures to ensure its data systems were protected against unauthorized
3 intrusions, failing to properly and adequately educate and train its employees, failing to put into
4 place reasonable or adequately computer systems and security practices to safeguard patients'
5 identifiable medical information including access restrictions and encryption, failing to have
6 adequate privacy policies and procedures in place that did not preserve the confidentiality of the
7 medical and personal identifying information of Plaintiff, the SubClass and the Class in their
8 possession, and failing to protect and preserve confidentiality of electronic medical information of
9 Plaintiff, the SubClass and the Class in their possession against disclosure and/or release, outweighs
10 the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous,
11 unethical, deceitful and offensive, and causes substantial injury to Plaintiff, the SubClass and the
12 Class.

13 134. Defendants have obtain money and property from Plaintiff, the SubClass and the
14 Class because of the payment of the services and products they received from Defendants. Plaintiff,
15 the SubClass and the Class have suffered an injury in fact by acquiring less in their transactions
16 with Defendants for the services and products they received from Defendants than they otherwise
17 would have if Defendants would had adequately protected the confidentiality of their medical and
18 personal identifying information.

19 135. Pursuant to the Business & Professions Code § 17203, Plaintiff, the SubClass and the
20 Class seek an order of this Court requiring Defendants awarding Plaintiff and the Class restitution
21 of monies wrongfully acquired by Defendants in the form of payments for services by means of
22 such unlawful, fraudulent and unfair business acts and practices, so as to restore any and all monies
23 to Plaintiff, the SubClass and the Class which were acquired and obtained by means of such
24 unlawful, fraudulent and unfair business acts and practices, which ill-gotten gains are still retained
25 by Defendants.

26 136. The aforementioned unlawful, fraudulent and unfair business acts or practices
27 conducted by Defendants have been committed in the past and continues to this day. Defendants
28 have failed to acknowledge the wrongful nature of their actions. Defendants have not corrected or

1 publicly issued comprehensive corrective notices to Plaintiff, the SubClass and the Class, and have
2 not corrected or enacted adequate privacy policies and procedures to protect and preserve
3 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
4 Class in their possession.

5 137. Because of Defendants' aforementioned conduct, Plaintiff, the SubClass and the
6 Class have no other adequate remedy of law in that absent injunctive relief from the Court and
7 Defendants are likely to continue to injure Plaintiff, the SubClass and the Class.

8 138. Pursuant to Business & Professions Code § 17203, Plaintiff, the SubClass and the
9 Class also seek an order of this Court for equitable and/or injunctive relief in the form of requiring
10 Defendants to correct its illegal conduct that is necessary and proper to prevent Defendants from
11 repeating their illegal and wrongful practices as alleged above and protect and preserve
12 confidentiality of medical and personal identifying information of Plaintiff, the SubClass and the
13 Class in Defendants' possession that has already been accessed, viewed, exfiltrated and/or publicly
14 exposed by at least one unauthorized third party because by way of Defendants' illegal and
15 wrongful practices set forth above. Pursuant to Business & Professions Code § 17203, Plaintiff, the
16 SubClass and the Class further seek an order of this Court for equitable and/or injunctive relief in
17 the form of requiring Defendants to publicly issue comprehensive corrective notices.

18 139. Because this case is brought for the purposes of enforcing important rights affecting
19 the public interest, Plaintiff, the SubClass and the Class also seek the recovery of attorneys' fees
20 and costs in prosecuting this action against Defendants under Code of Civil Procedure § 1021.5 and
21 other applicable law.

22 **PRAYER FOR RELIEF**

23 WHEREFORE, Plaintiff respectfully request that the Court grant Plaintiff and the proposed
24 SubClass and Class the following relief against Defendants, and each of them:

25 **As for the First, Second and Third Causes of Action**

26 1. For nominal damages in the amount of one thousand dollar (\$1,000) per violation to Plaintiff
27 individually and to each member of the SubClass and the Class pursuant to Civil Code §
28 56.36(b)(1);

1 2. For actual damages according to proof per violation pursuant to Civil Code § 56.36(b)(2);

2 **As for the Fourth Cause of Action**

3 3. For damages according to proof to Plaintiff individually and to each member of the Class
4 pursuant to California Civil Code § Civil Code § 1798.84(b);

5 4. For injunctive relief pursuant to California Civil Code § Civil Code § 1798.84(e);

6 **As for the Fifth Cause of Action**

7 5. For an order awarding Plaintiff, the SubClass and the Class restitution of all monies
8 wrongfully acquired by Defendants by means of such unlawful, fraudulent and unfair
9 business acts and practices;

10 6. For injunctive relief in the form of an order instructing Defendants to prohibit the
11 unauthorized release of medical and personal identifying information of Plaintiff, the
12 SubClass and the Class, and to adequately maintain the confidentiality of the medical and
13 personal identifying information of Plaintiff and the Class;

14 7. For injunctive relief in the form of an order enjoining Defendants from disclosing the
15 medical and personal identifying information of Plaintiff, the SubClass and the Class
16 without the prior written authorization of each Plaintiff, the SubClass and the Class member;

17 **As to All Causes of Action**

18 8. That the Court issue an Order certifying this action be certified as a class action on behalf of
19 the proposed SubClass and Class, appointing Plaintiff as representative of the proposed
20 SubClass and Class, and appointing Plaintiff's attorneys, as counsel for members of the
21 proposed SubClass and Class;

22 9. For an award of attorneys' fees as authorized by statute, including, but not limited to, the
23 provisions of California Code of Civil Procedure § 1021.5, and as authorized under the
24 "common fund" doctrine, and as authorized by the "substantial benefit" doctrine;

25 10. For costs of the suit;

26 11. For prejudgment interest at the legal rate; and

27 12. Any such further relief as this Court deems necessary, just, and proper.

28

1 Dated: September 8, 2021

2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

KEEGAN & BAKER LLP

By  _____

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

Plaintiff, the SubClass and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

Dated: September 8, 2021

KEEGAN & BAKER LLP

By  _____

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

PROOF OF SERVICE

I, Stacy Johnson, declare that I am over the age of 18 years and am not a party to the case; I am employed in the County of San Diego, California; and my business address is 2292 Faraday Avenue, Suite 100, Carlsbad, California 92008. The mailing occurred in Wildomar, California.

I caused to be served the following document(s): **FIRST AMENDED CLASS ACTION COMPLAINT FOR DAMAGES, RESTITUTION, AND INJUNCTIVE RELIEF FOR VIOLATIONS OF: (1) THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CIVIL CODE §§ 56, ET SEQ.; (2) BREACH OF CALIFORNIA SECURITY NOTIFICATION LAWS, CALIFORNIA CIVIL CODE § 1798.82; AND (3) BUSINESS AND PROFESSIONS CODE §§ 17200, ET SEQ.** on the interested parties listed below:

Daniel T. Rockey, Esq.
daniel.rockey@bclplaw.com
BRYAN CAVE LLP
Three Embarcadero Center, 7th Floor
San Francisco, CA 94111
Tel: (415) 675-3400 / Fax: (415) 675-3434
Attorney for Defendant Neighborhood Healthcare

Craig J. Mariam, Esq.
cmariam@grsm.com
GORDON REES SCULLY MANSUKHANI, LLP
633 West Fifth Street, 52nd Floor
Los Angeles, CA 90071
Tel: (213) 270-7856 / Fax: (877) 306-0043
Attorney for Defendant Health Center Partners of Southern California

■ **BY ELECTRONIC SERVICE:** I transmitted the documents described above to One Legal for electronic service on Daniel T. Rockey, Esq. (Daniel.rockey@bclplaw.com); and Craig J. Mariam, Esq. (cmariam@grsm.com). In light of the COVID-19 pandemic in California and Governor Newsom’s Executive Order N-38-20, dated March 27, 2020, the requirements under Code of Civil Procedure section 1010.6 regarding agreement to electronic service have been suspended. Accordingly, all documents served in this matter will be done by electronic means consistent with other provisions of the Code of Civil Procedure.

■ (State) I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: September 8, 2021



Exhibit A



HEALTH CENTER PARTNERS
of Southern California

C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE



NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

SEQ
CODE 2D
Ver 1

BREAK

To Enroll, Please Call:
1-833-416-0926
Or Visit:
<https://response.idx.us/hcp-netgain-incident>
Enrollment Code: <<XXXXXXXXXX>>

April 12, 2021

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by Netgain Technology, LLC (“Netgain”), the IT service provider for Health Center Partners of Southern California (“HCP”). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTHCENTER>>. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, we engaged our own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, our health center members and partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain’s digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain’s cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

Once we learned that HCP data may have been involved in the incident, we worked with our cybersecurity experts to review the impacted files and identify the individuals whose information was contained in such files so that we may notify such individuals. Our investigation revealed that the impacted files contained your personal information. **Again, we are not aware of any misuse of your personal information as a result of this incident.** Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your information.

What Information Was Involved: The information involved varies depending on the individual but may include the following: <<VARPARAGRAPH>>.

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, we have reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and we are committed to assisting their investigation into the matter.

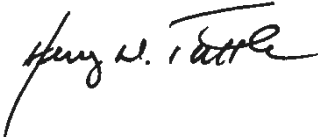
We are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include **xx** months of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What You Can Do: As we have stated, we are not aware of any misuse of your information as a result of this incident. However, we encourage you to follow the recommendations on the next page to help protect your information. We also encourage you to enroll in the complimentary services offered by going to <https://response.idx.us/hcp-netgain-incident> or calling 1-833-416-0926 and using the enrollment code provided above. Please note that the deadline to enroll is July 12, 2021.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-833-416-0926 between 6:00 a.m. and 6:00 p.m. Pacific Time.

The security of your information is a top priority for HCP, and we are committed to safeguarding your data and privacy.

Sincerely,

A handwritten signature in black ink, appearing to read "Henry W. Tuttle". The signature is fluid and cursive, with the first name "Henry" being the most prominent.

Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
www.consumer.ftc.gov ,	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
and	1-888-743-0023	1-877-566-7226	1-401-274-4400
www.ftc.gov/idtheft			
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Exhibit B



To Enroll, Please Call:
(833) 903-3642
Or Visit:
<https://response.idx.us/nhc-netgain-incident>
Enrollment Code: <<ENROLLMENT>>

C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

April 8, 2021

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

The privacy and security of your personal information is very important to Neighborhood Healthcare. We are writing to make you aware of an issue brought to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud hosting and managed services provider. Neighborhood Healthcare used Netgain to host some Neighborhood Healthcare files.

What Happened

On November 24, 2020, Netgain became aware of a security incident that involved unauthorized access to portions of the Netgain environment and Netgain client environments and began taking steps to investigate this incident. But, on December 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain took additional measures to contain the threat and address the issue. Netgain’s technical teams worked closely with third-party experts to remove the threat in the impacted environments and confirm that client and internal systems are protected.

Neighborhood Healthcare learned of the ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to believe that the protected health information (“PHI”) of our patients had been impacted in the incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some information including, potentially, some files containing patient PHI may have been impacted in the incident. Netgain could not confirm, at that time, what records may have been impacted in the incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood Healthcare that Netgain believed were impacted by the attackers. Those files came from a Neighborhood Healthcare server accessible by the Netgain environment. Since that time, Neighborhood Healthcare has worked to review those records, to identify individuals impacted, conduct an investigation into the incident with the assistance outside experts, and to transmit this letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood Healthcare determined that the impacted files included some of your information.

What Information Was Involved

The information involved may have included some of the following: your name, date of birth, address, Social Security Number and information about the care that you received from Neighborhood Healthcare such as insurance coverage information, physician you saw, and treatment codes. Neighborhood Healthcare is offering credit monitoring services to you at no charge. Please see the **What You Can Do** section below for information about these services including how to enroll. Please also see the **Additional Important Information** section below for further precautionary measures you may wish to take. Netgain has received assurances that the data has not gone beyond the attacker, that the data was not and will not be misused, and that the data will not be disseminated or otherwise be made publicly available.

What We Are Doing

Please know that we take this incident and the security of your personal information very seriously. Ensuring the safety of our patients' data is of the utmost importance to us. Since we learned of this incident, we have been working with Netgain to seek assurances that they are taking appropriate steps to respond to this incident. We have also conducted an investigation of the incident with the help of outside experts, and we have transitioned to a new hosting provider (a transition that was already in process when this incident occurred).

In addition, we are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include <<12/24 months>> of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What Netgain Is Doing

Netgain took several steps to strengthen its environment following the incident, including international Geo-fencing for Azure-hosted environments, deploying additional log monitoring across all servers, and additional hardening of network security rules and protocols to restrict lateral movement across environments. Netgain stated that it paid a significant amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

What You Can Do

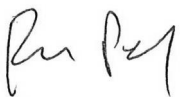
We recommend that you review the additional information enclosed. Additionally, we encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 903-3642 or going to <https://response.idx.us/nhc-netgain-incident> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 8, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

We very much regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, please call (833) 903-3642, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely



Rakesh Patel
CEO
Neighborhood Healthcare

Additional Important Information

1. Website and Enrollment. Go to <https://response.idx.us/nhc-netgain-incident> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 903-3642 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Generally. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing financial account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state's Attorney General.

5. The FTC. You can obtain information from Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

6. Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

7. Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788 equifax.com/personal/credit-report-services/ 800-525-6285	Experian Security Freeze P.O. Box 9554 Allen, TX 75013-9544 experian.com/freeze/center.html 888-397-3742	TransUnion (FVAD) P.O. Box 160 Woodlyn, PA 19094 transunion.com/credit-freeze 888-909-8872
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

More information can also be obtained by contacting the Federal Trade Commission listed above.

8. Protecting Medical Information: To date, we have no reason to believe that your PHI potentially involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following steps can help protect you from medical identity theft issues.

- Do not share health insurance cards with anyone apart from your care providers and other family members who are covered under the insurance plan or who help you with your medical care.
- Review the “explanation of benefits statements” that you receive from your health insurance company. If you see something amiss, follow up with your insurance company or the health care provider identified on the explanation of benefits to request further information.
- Ask your health insurance company for a report on all services they have paid for you for the current year. If you do not recognize an item in that list, speak with your insurance company to verify it.

9. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Netgain, Two Healthcare Providers Facing Lawsuit Over Dec. 2020 Ransomware Attack](#)
