

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
09/13/2021 at 04:59:10 PM
Clerk of the Superior Court
By Melinda McClure, Deputy Clerk

5 Attorneys for Plaintiff JOHN DOE

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

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

10 Plaintiff,

11 vs.

12 HEALTH CENTER PARTNERS OF
13 SOUTHERN CALIFORNIA; and DOE
14 DEFENDANTS 1-100;

15 Defendants.
16
17
18

) Case No. 37-2021-00038892-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**
)

19 Plaintiff John Doe (or "Plaintiff"), by and through his attorneys, bring this class action on
20 behalf of himself individually and all others similarly situated, against Defendants Health Center
21 Partners of Southern California and Doe Defendants 1-100 (collectively referred to as
22 "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 all
7 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
21 provides, “The court having jurisdiction over a civil proceeding under this title shall take all steps
22 ***reasonably necessary to safeguard the individual privacy and prevent harassment of a health care***
23 ***patient***, licensed health practitioner, or employee, client, or customer of a health care facility who is
24 a party or witness in the proceeding, including granting protective orders. ***Health care patients***,
25 licensed health practitioners, and employees, clients, and customers of the health care facility ***may***
26 ***use pseudonyms to protect their privacy.***” Cal. Civ. Code § 3427.3 (emphasis added). Additionally,
27 California courts have permitted plaintiffs to proceed under a fictitious name when circumstances
28 justify protecting his or her true identity, including matters of a highly sensitive and personal nature.
Doe v. Sup.Ct. (Luster) (2011) 194 Cal.App.4th 750, 754. Similarly, federal courts have also
permitted the use of a pseudonym in cases where concealing a party’s identity is necessary to
protect that party from “harassment, injury, ridicule, or personal embarrassment.” *United States v.*
Doe, 655 F.2d 920, 922 n. 1 (9th Cir. 1981); and *Does I thru XXIII v. Advanced Textile*, 214 F.3d
1058, 1086 (9th Cir. 2000). 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
serious nature of the data breach.

1 without Plaintiff's and the Class members' prior written authorization, which constitutes
2 unauthorized disclosure and/or release of their information in violation of Civil Code §§ 56.10(a)
3 and 56.101(a) of the Act. In fact, Defendant Health Center Partners of Southern California's form
4 letter, entitled "**Notice of Data Breach**," dated April 12, 2021, signed by Henry Tuttle, President &
5 Chief Executive Officer, Health Center Partners of Southern California, sent to Plaintiff and all
6 other persons similarly situated, informing them, in part, of "a recent data security incident
7 experienced by Netgain Technology, LLC ('Netgain'), the IT service provider for Health Center
8 Partners of Southern California ('HCP')" and stating, in part, "**What Happened**: Netgain recently
9 informed HCP that it had experienced a data security incident that involved systems containing
10 HCP data.... According to Netgain, in late September 2020, an unauthorized third party gained
11 access to Netgain's digital environment, and between October 22, 2020 to December 3, 2020, the
12 unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an
13 undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies
14 of this data and that it will not publish, sell, or otherwise disclose the data.... The information
15 involved varies depending on the individual but may include the following: name, address, date of
16 birth, diagnosis/treatment information and treatment cost information. Once we learned that HCP
17 data may have been involved in the incident, we worked with our cybersecurity experts to review
18 the impacted files and identify the individuals whose information was contained in such files so that
19 we may notify such individuals. Our investigation revealed that the impacted files contained your
20 personal information." An exemplar of Defendant Health Center Partners of Southern California's
21 "**Notice of Data Breach**" form letter submitted to the Attorney General of the State of California is
22 attached hereto as **Exhibit A**.

23 3. Additionally, Netgain Technology, LLC ("NETGAIN") stated in a blog post, entitled
24 "What we learned as a ransomware victim – so you don't become one," that "late last year, Netgain
25 was the victim of a criminal ransomware attack.... to become a victim of such an attack is both
26 humbling and galvanizing.... we identified additional opportunities to strengthn our security posture
27 in a continuous journey with an ongoing commitment to ensure this remains top-of-mind. As part
28 of our incident response, we have implemented a number of these identified enhancements to our

1 security posture and have continued to progress a multipronged approach. We've deployed new
2 tools, revised policies and enforcement procedures, and implemented an advanced around-the-clock
3 managed detections and response service for proactive threat monitoring.”

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

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

18 JURISDICTION AND VENUE

19 6. This Court has jurisdiction over this action under California Code of Civil Procedure
20 § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class in the aggregate
21 exceeds the \$25,000 jurisdictional minimum of this Court. Further, the amount in controversy as to
22 Plaintiff individually does not exceed \$75,000.

23 7. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of
24 Civil Procedure §§ 395(a) and 395.5 because Defendants have obtained medical information of
25 Plaintiff and the Class in the transaction of business in the State of California and in this judicial
26 district, which has caused both obligations and liability of Defendants to arise in the State of
27 California and in this judicial district.

28

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 his
3 medical information created, maintained, preserved and/or stored on Defendants’ computer
4 networks could subject his to harassment or abuse.

5 **B. DEFENDANTS**

6 10. Defendant Health Center Partners of Southern California (“HCP”) is a business
7 entity doing business in the State of California, with its principal business office located at 3710
8 Ruffin Road, San Diego, CA 92123. On or about April 12, 2021, HCP caused a form letter sent on
9 its behalf, entitled “**Notice of Data Breach**,” dated April 12, 2021, signed by Henry Tuttle,
10 President & Chief Executive Officer, Health Center Partners of Southern California, an exemplar of
11 which is attached hereto as **Exhibit A**, to be submitted to the Attorney General of the State of
12 California and to be mailed to Plaintiff and the Class. At all times relevant to this action, HCP was
13 and is a “business” within the meaning of Civil Code § 1798.140(c)(1), owns or licenses
14 computerized data which includes Plaintiff’s and the Class’ personal information, within the
15 meaning of Civil Code § 1798.82(h), collected Plaintiff’s and the Class’ personal information
16 within the meaning of Civil Code § 1798.81.5(d)(1)(A).

17 **C. DOE DEFENDANTS**

18 11. 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 12. 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 13. 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 14. On its website, HCP represents that “[o]ur members collectively serve 917,000
16 unduplicated patients each year, for 3.9 million patient visits each year, at 160 practice sites across
17 San Diego, Riverside, Imperial counties.”² Plaintiff alleges on information and belief that at all
18 times relevant to this action, including the period from October 22, 2020 to December 3, 2020,
19 HCP’s referred to “members,” including to NH and other providers of health care, disclosed and/or
20 released Plaintiff’s and the Class’ medical information, in electronic and physical form, in
21 possession of or derived from HCP’s referred to “members,” including to NH and other providers of
22 health care, regarding Plaintiff’s and the Class’ medical history, mental or physical condition, or
23 treatment, to HCP, pursuant to a business associate agreement and/or a service provider agreement.
24 Such medical information included or contained an element of personal identifying information
25 sufficient to allow identification of Plaintiff and the Class, such as their names, date of birth,
26 addresses, medical record numbers, insurance provider, electronic mail addresses, telephone

27
28

² (<https://hcpsocal.org/members/>)

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

14 15. Plaintiff alleges on information and belief that at all times relevant to this action,
15 including the period from October 22, 2020 to December 3, 2020, HCP disclosed and/or released
16 Plaintiff's and the Class' medical information, in electronic and physical form, in possession of or
17 derived from HCP's referred to "members," including to NH and other providers of health care,
18 regarding Plaintiff's and the Class' medical history, mental or physical condition, or treatment, to
19 NETGAIN, pursuant to their business associate agreement and/or service provider agreement. As a
20 result, at all times relevant to this action, including the period from October 22, 2020 to December
21 3, 2020, NETGAIN possessed Plaintiff's and the Class' medical information, in electronic and
22 physical form, in possession of or derived from Defendants regarding Plaintiff's and the Class'
23 medical history, mental or physical condition, or treatment. Such medical information included or
24 contained an element of personal identifying information sufficient to allow identification of
25 Plaintiff and the Class, such as their names, date of birth, addresses, medical record numbers,
26 insurance provider, electronic mail addresses, telephone numbers, or social security numbers, or
27 other information that, alone or in combination with other publicly available information, reveals
28 their identity. Therefore, at all times relevant to this action, including the period from October 22,

1 2020 to December 3, 2020, NETGAIN maintained and continues to maintain “medical
2 information,” within the meaning of Civil Code § 56.05(j), of Plaintiff and the Class, each of which
3 are “patients” within the meaning of Civil Code § 56.05(k).

4 16. At all times relevant to this action, including the period from October 22, 2020 to
5 December 3, 2020, pursuant to Civil Code § 56.06(a), HCP qualifies as a provider of health care
6 because it created, maintained, preserved, and stored records of the care, products and services that
7 Plaintiff and the Class members received in the State of California from HCP’s over 16 member
8 community health centers, 160 member practice sites, 917,000 patients served, and/or other
9 providers of health care, health care service plans, pharmaceutical companies, and contractors, as
10 defined by the Act, is and was organized for the purpose of maintaining medical information, within
11 the meaning of Civil Code § 56.05(j), in order to make the information available to Plaintiff and the
12 Class members or to a provider of health care at the request of Plaintiff and the Class members or a
13 provider of health care, for purposes of allowing Plaintiff and the Class members to manage their
14 information, or for the diagnosis and treatment of Plaintiff and the Class members.

15 17. Alternatively, at all times relevant to this action, including the period from October
16 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.06(b), HCP qualifies as a provider of
17 health care because it offers software and hardware to consumers (including HCP’s referred to
18 “members,” including to NH and other providers of health care) (1) in order to make the
19 information available to an individual or a provider of health care at the request of the individual or
20 a provider of health care, (2) for purposes of allowing the individual to manage his or his
21 information, and (3) for the diagnosis, treatment, or management of a medical condition of the
22 individual.

23 18. Alternatively, at all times relevant to this action, including the period from October
24 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.05(d), HCP, as an entity that is a
25 medical group, independent practice association, pharmaceutical benefits manager, or a medical
26 service organization, and is not a health care service plan or provider of health care to Plaintiff and
27 the Class members, is and was a “contractor” under Civil Code § 56.05(d).

28

1 19. Alternatively, at all times relevant to this action, including the period from October
2 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.13, HCP 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 or pursuant to the provisions of subdivision (c) of Section 56.10 and was prohibited from
5 further disclosing that medical information except in accordance with a new authorization that
6 meets the requirements of Section 56.11, or as specifically required or permitted by other provisions
7 of this chapter or by law.

8 20. Alternatively, at all times relevant to this action, including the period from October
9 22, 2020 to December 3, 2020, pursuant to Civil Code § 56.245, HCP is and was a recipient of
10 medical information of Plaintiff and the Class members pursuant to an authorization as provided by
11 the Act, and was prohibited from further disclosing such medical information unless in accordance
12 with a new authorization that meets the requirements of Section 56.21, or as specifically required or
13 permitted by other provisions of this chapter or by law.

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

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

27 23. At all times relevant to this action, including the period from October 22, 2020 to
28 December 3, 2020, HCP created, maintained, preserved, and stored records of the care, services and

1 products, including the names, addresses, dates of birth, diagnosis/treatment information and
2 treatment cost information of Plaintiff and the Class (all of which constitutes medical information,
3 as that term is defined and set forth in the Act), that Plaintiff and other Class members received in
4 the State of California from HCP's referred to "members," including to NH and other providers of
5 health care, on its computer networks.

6 24. As a result, on or before October 30, 2020, Defendants possessed Plaintiff's and the
7 Class' medical information, in electronic and physical form, in possession of or derived
8 from Defendants regarding their medical history, mental or physical condition, or treatment. Such
9 medical information included or contained an element of personal identifying information sufficient
10 to allow identification of Plaintiff and the Class, such as their names, addresses, dates of birth,
11 social security numbers, phone numbers and/or email addresses, or other information that, alone or
12 in combination with other publicly available information, reveals their identity.

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

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

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

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

28

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

- 9 i. Developing and implementing security policies and procedures.
10 ii. Designating a security official who is responsible for developing and implementing
11 its security policies and procedures, including educating and training the workforce.
12 iii. Encrypting the information or records, and protecting against the release or use of
13 the encryption key and passwords, or transmitting the information or records in a
14 manner designed to provide equal or greater protections against improper
15 disclosures.

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

19 31. At all times relevant to this action, including the period from October 22, 2020 to
20 December 3, 2020, HCP created, maintained, preserved, stored, disclosed and/or delivered
21 Plaintiff's and the Class members' medical information to NETGAIN. At all times relevant to this
22 action, HCP did not obtain written authorization from the Plaintiff and the Class prior to creating,
23 maintaining, preserving, storing, disclosing and/or delivering Plaintiff's and the Class members'
24 medical information to NETGAIN. Furthermore, HCP's disclosure of and/or delivery of Plaintiff's
25 and the Class members' medical information to NETGAIN was not permissible without written
26 authorization from the Plaintiff and the Class or under any exemption under Civil Code § 56.10(c).

27 32. By law, the HIPAA Privacy Rule applies only to covered entities, e.g. health care
28 providers. However, most health care providers do not carry out all of their health care activities

1 and functions by themselves. Instead, they often use the services of a variety of other persons or
2 businesses. The Privacy Rule allows covered providers to disclose protected health information
3 (PHI) to these “business associates” if the providers obtain assurances that the business associates
4 will use the information only for the purposes for which it was engaged by the covered entity, will
5 safeguard the information from misuse, and will help the covered entity comply with some of the
6 covered entity’s duties under the Privacy Rule. Covered entities may disclose PHI to an entity in its
7 role as a business associate only to help the covered entity carry out its health care functions – not
8 for the business associate’s independent use or purposes, except as needed for the proper
9 management and administration of the business associate. The Privacy Rule requires that a covered
10 entity obtain assurances from its business associate that the business associate will appropriately
11 safeguard the PHI it receives or creates on behalf of the covered entity. The satisfactory assurances
12 must be in writing, whether in the form of a contract or other agreement between the covered entity
13 and the business associate, and requires a covered entity to obtain satisfactory assurances, on an
14 ongoing basis, that the business associate is complying, on an ongoing basis, with cybersecurity and
15 information security standards, and appropriately safeguarding the PHI it receives or creates on
16 behalf of the covered entity.

17 33. When hiring and monitoring a service provider or business associate such as
18 NETGAIN, HCP knew or should have known that they had a duty to inquire about potential service
19 providers’ and business associates’ cybersecurity programs and how such programs are maintained.
20 HCP knew or should have known that they had a duty to compare potential service providers’ and
21 business associates’ cybersecurity programs to the industry standards adopted by other healthcare
22 providers, and should evaluate potential service providers’ track records in the industry by
23 reviewing public information about data security incidents and litigation. HCP knew or should have
24 known that they had a duty to also ask potential service providers and business associates about
25 whether they have experienced any cybersecurity incidents and how such incidents were handled, as
26 well as whether the potential service provider has an insurance policy in place that would cover
27 losses caused by cybersecurity breaches (including losses caused by internal and external threats).
28 HCP knew or should have known that they had a duty to review service provider and business

1 associate contracts to ensure that the contracts require the service providers to comply, on an
2 ongoing basis, with cybersecurity and information security standards (and avoid contract provisions
3 that limit service providers' responsibility for cybersecurity and information technology breaches).
4 HCP knew or should have known that they had a duty to obtain satisfactory assurances that their
5 service providers and business associates were complying, on an ongoing basis, with cybersecurity
6 and information security standards, and were properly creating, maintaining, preserving, and/or
7 storing the PHI it receives or creates on behalf of HCP, including the confidential, medical and
8 personal identifying information of Plaintiff and the Class. Finally, HCP knew or should have
9 known that they had a duty to pay particular attention to contract terms relating to confidentiality,
10 the use and sharing of information, notice by the vendor of cybersecurity risk assessments and audit
11 reports, cybersecurity breaches and records retention and destruction.

12 34. Plaintiff alleges on information and belief that HCP's disclosure and/or release of
13 Plaintiff's and the Class' medical information to NETGAIN was pursuant to their business associate
14 agreement and/or a service provider agreement that was not permissible under the Privacy Rule or
15 any exemption under Civil Code § 56.10(c), and/or because HCP negligently entered into an
16 agreement with NETGAIN that contained provisions that purport or seek to limit NETGAIN's
17 financial responsibility for cybersecurity and information technology breaches, and negligently
18 failed to obtain reasonable assurances and negligently failed to monitor and conduct assessments of
19 NETGAIN to verify that NETGAIN was properly creating, maintaining, preserving, and/or storing
20 the PHI it receives or creates on behalf of HCP, including the confidential, medical and personal
21 identifying information of Plaintiff and the Class, NETGAIN would comply with HIPAA privacy
22 regulations and to follow guidelines and policies to maintain the privacy, confidentiality, including
23 by encryption, and otherwise reasonably protect Plaintiff's and the Class' medical information from
24 disclosure and/or release to at least one unauthorized third party "user" prior to and after HCP's
25 disclosure and/or release of Plaintiff's and the Class members' medical information to NETGAIN.

26 35. At all times relevant to this action, including the period from October 22, 2020 to
27 December 3, 2020, at least one "unauthorized third party gained access to Netgain's digital
28 environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party

1 obtained certain files” containing Plaintiff’s and the Class’ medical information (i.e., their names,
2 addresses, dates of birth, diagnosis/treatment information and treatment cost information) that was
3 located on a NETGAIN server in an un-encrypted format, as represented in HCP’s “**Notice of Data**
4 **Breach**” form letter submitted to the Attorney General of the State of California and mailed to
5 Plaintiff and the Class, attached hereto as **Exhibit A**.

6 36. Defendants had the resources necessary to protect and preserve confidentiality of
7 electronic medical information of Plaintiff and the Class in their possession, but neglected to
8 adequately implement data security measures as required by HIPPA and the Act, despite their
9 obligation to do so.

10 37. Additionally, the risk of vulnerabilities in its computer and data systems of being
11 exploited by an unauthorized third party trying to steal Plaintiff’s and the Class’ electronic
12 personally identifying and medical information was foreseeable and/or known to Defendants. The
13 California Data Breach Report 2012-2015, issued in February 2016 by Attorney General, Kamala
14 D. Harris, reported, “Malware and hacking presents the greatest threat, both in the number of
15 breaches and the number of records breached” and “Social Security numbers and medical
16 information – was breached than other data types.” Moreover, as Attorney General further reported,
17 just because “[e]xternal adversaries cause most data breaches, [] this does not mean that
18 organizations are solely victims; they are also stewards of the data they collect and maintain. People
19 entrust businesses and other organizations with their data on the understanding that the
20 organizations have a both an ethical and a legal obligation to protect it from unauthorized access.
21 Neglecting to secure systems and data opens a gateway for attackers, who take advantage of
22 uncontrolled vulnerabilities.” Regarding encryption, Attorney General instructed in California Data
23 Breach Report 2012-2015, “As we have said in the past, breaches of this type are preventable.
24 Affordable solutions are widely available: strong full-disk encryption on portable devices and
25 desktop computers when not in use.[] Even small businesses that lack full time information security
26 and IT staff can do this. They owe it to their patients, customers, and employees to do it now.”

27 38. More recently the HIPAA Journal posted on November 1, 2018 warned, “Healthcare
28 organization[s] need to ensure that their systems are well protected against cyberattacks, which

1 means investing in technologies to secure the network perimeter, detect intrusions, and block
2 malware and phishing threats.”

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

11 40. To be successful, phishing relies on a series of affirmative acts by a company and its
12 employees such as clicking a link, downloading a file, or providing sensitive information. Once
13 criminals gained access to the email accounts of a company and its employees, the email servers
14 communicated—that is, disclosed—the contents of those accounts to the criminals. “Phishing
15 scams are one of the most common ways hackers gain access to sensitive or confidential
16 information. Phishing involves sending fraudulent emails that appear to be from a reputable
17 company, with the goal of deceiving recipients into either clicking on a malicious link or
18 downloading an infected attachment, usually to steal financial or confidential information.”
19 (<https://www.varonis.com/blog/data-breach-statistics/>). As posted on April 21, 2020, the FBI had
20 issued a fresh warning [Alert Number MI-000122-MW] following an increase in COVID-19
21 phishing scams targeting healthcare providers.

22 41. At all times relevant to this action, including the period from October 22, 2020 to
23 December 3, 2020, Defendants negligently created, maintained, preserved, and/or stored Plaintiff’s
24 and the Class’ medical information, including Plaintiff’s and the Class’ 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 Class in their possession, as required by HIPPA and the Act, and

1 specifically, under Civil Code §§ 56.10(a), 56.26(a), 56.36(e)(2)(E), 56.101(a), and
2 56.101(b)(1)(A), and according to their written representations to Plaintiff and the Class.

3 42. Had Defendants taken such appropriate preventive actions, fix the deficiencies in
4 their data security systems and adopted security measures as required by HIPPA and the Act from
5 October 22, 2020 to December 3, 2020, Defendants could have prevented Plaintiff's and the Class'
6 electronic medical information within Defendants' computer networks from being accessed and
7 actually viewed by unauthorized third parties.

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

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

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

25 46. At all times relevant to this action, including the period from October 22, 2020 to
26 December 3, 2020, HCP's negligent failure to protect and preserve confidentiality of electronic
27 medical information of Plaintiff and the Class, on NETGAIN's computer server, allowed Plaintiff's
28 and the Class' medical and personal identifying information to be accessed and actually viewed by

1 at least one unauthorized third party, constituting a release in violation of Civil Code §
2 56.101(b)(1)(A).

3 47. On or about April 12, 2021, HCP caused a form letter, entitled “**Notice of Data**
4 **Breach**,” dated April 12, 2021, signed by Henry Tuttle, President & Chief Executive Officer,
5 Health Center Partners of Southern California, to be mailed to Plaintiff and the Class, informing
6 them, in part, of “a recent data security incident experienced by Netgain Technology, LLC
7 (‘Netgain’), the IT service provider for Health Center Partners of Southern California (‘HCP’)” and
8 stating, in part, “**What Happened:** Netgain recently informed HCP that it had experienced a data
9 security incident that involved systems containing HCP data.... According to Netgain, in late
10 September 2020, an unauthorized third party gained access to Netgain’s digital environment, and
11 between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files
12 containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange
13 for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or
14 otherwise disclose the data.... The information involved varies depending on the individual but may
15 include the following: name, address, date of birth, diagnosis/treatment information and treatment
16 cost information. Once we learned that HCP data may have been involved in the incident, we
17 worked with our cybersecurity experts to review the impacted files and identify the individuals
18 whose information was contained in such files so that we may notify such individuals. Our
19 investigation revealed that the impacted files contained your personal information.” An exemplar of
20 HCP’s “**Notice of Data Breach**” form letter submitted to the Attorney General of the State of
21 California and mailed to Plaintiff and the Class is attached hereto as **Exhibit A**. Plaintiff received
22 in the mail a HCP “**Notice of Data Breach**” form letter, addressed to him, which alerted Plaintiff
23 that his medical and personal identifying information, along with other Class members, was
24 improperly accessed by at least one unauthorized third party. As a result, Plaintiff fears that
25 disclosure and/or release of his medical and personal identifying information created, maintained,
26 preserved, and/or stored on Defendants’ computer networks could subject his to harassment or
27 abuse. Moreover, although thereafter, on May 4, 2021, Plaintiff wrote both HCP and NH separately
28

1 requesting further information about this security incident, neither HCP nor NH provided a
2 substantive response to his requests.

3 48. HCP's "Notice of Data Breach" form letter submitted to the Attorney General of
4 the State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**, further
5 states, "**What We Are Doing:** [] We are providing you with steps that you can take to help protect
6 your personal information, and as an added precaution, we are offering you complimentary identity
7 protection services through IDX, a leader in risk mitigation and response."

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

17 50. To date, other than offering "steps that you can take to help protect your personal
18 information" and "complimentary identity protection services through IDX" "as an added
19 precaution," HCP has not offered any monetary compensation for the unauthorized disclosure
20 and/or release of Plaintiff's and the Class' electronic medical information under the Act. In effect,
21 HCP is shirking its responsibility for the harm it has caused, while shifting the burdens and costs of
22 its wrongful conduct onto its patients, i.e. Plaintiff and the Class.

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

27 52. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA
28 covered entities to provide notification following a breach of unsecured protected health

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

28

1 possible and/or sufficient to allow members of the Class identify themselves as having a right to
2 recover.

3 56. There is a well-defined community of interest among the members of the Class
4 because common questions of law and fact predominate, Plaintiff's claims are typical of the
5 members of the class, and Plaintiff can fairly and adequately represent the interests of the Class.

6 57. Common questions of law and fact exist as to all members of the Class and
7 predominate over any questions affecting solely individual members of the Class. Among the
8 questions of law and fact common to the Class that predominate over questions which may affect
9 individual Class members, including the following:

- 10 a) Whether Defendants possessed Plaintiff's and the Class' medical and personal
11 identifying information from October 22, 2020 to December 3, 2020;
- 12 b) Whether Defendants created, maintained, preserved and/or stored Plaintiff's and the
13 Class' medical and personal identifying information, in electronic form, onto
14 Defendants' computer networks from October 22, 2020 to December 3, 2020;
- 15 c) Whether Defendants implemented and maintained reasonable security procedures
16 and practices to protect Plaintiff's and the Class' medical and personal identifying
17 information, in electronic form, within Defendants' computer networks from October
18 22, 2020 to December 3, 2020;
- 19 d) Whether Plaintiff's and the Class' medical and personal identifying information, in
20 electronic form, within Defendants' computer networks from October 22, 2020 to
21 December 3, 2020 was accessed, viewed, exfiltrated and/or publicly exposed by an
22 unauthorized third party;
- 23 e) Whether Plaintiff's and the Class' medical and personal identifying information, in
24 electronic form, within Defendants' computer networks from October 22, 2020 to
25 December 3, 2020 was accessed, viewed, exfiltrated and/or publicly exposed by an
26 unauthorized third party without the prior written authorization of Plaintiff and the
27 Class, as required by Civil Code §§ 56.10 and 56.26;
- 28

1 f) Whether Defendants' creation, maintenance, preservation and/or storage of
2 Plaintiff's and the Class' medical and personal identifying information, in electronic
3 form, within Defendants' computer networks, accessed, viewed, exfiltrated and/or
4 publicly exposed by an unauthorized third party was permissible without written
5 authorization from Plaintiff and the Class or under any exemption under Civil Code
6 § 56.10(c);

7 g) Whether Defendants' creation, maintenance, preservation and/or storage of
8 Plaintiff's and the Class' medical and personal identifying information, in electronic
9 form, within Defendants' computer networks, accessed, viewed, exfiltrated and/or
10 publicly exposed by an unauthorized third party constitutes a release in violation of
11 Civil Code §56.101;

12 h) Whether the timing of HCP's notice that Plaintiff's and the Class' medical and
13 personal identifying information, in electronic form, was accessed, viewed,
14 exfiltrated and/or publicly exposed by an unauthorized third party, was given in the
15 most expedient time possible and without reasonable delay;

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

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

20 58. Plaintiff's claims are typical of those of the other Class members because Plaintiff,
21 like every other Class member, were exposed to virtually identical conduct and now suffer from the
22 same violations of the law as other Class members.

23 59. Plaintiff will fairly and adequately protect the interests of the Class. Moreover,
24 Plaintiff has no interest that is contrary to or in conflict with those of the Class, he seeks to
25 represent. In addition, Plaintiff has retained competent counsel experienced in class action litigation
26 to further ensure such protection and intend to prosecute this action vigorously.

27 60. The nature of this action and the nature of laws available to Plaintiff and the other
28 Class members make the use of the class action format a particularly efficient and appropriate

1 procedure to afford relief to Plaintiff and the other Class members for the claims alleged and the
2 disposition of whose claims in a class action will provide substantial benefits to both the parties and
3 the Court because:

- 4 a) If each of the Class members were required to file an individual lawsuit, the
5 Defendants would necessarily gain an unconscionable advantage since they would be
6 able to exploit and overwhelm the limited resources of each individual member of
7 the Class with its vastly superior financial and legal resources;
- 8 b) The costs of individual suits could unreasonably consume the amounts that would be
9 recovered;
- 10 c) Proof of a common business practice or factual pattern which Plaintiff experienced is
11 representative of that experienced by the Class and will establish the right of each of
12 the members to recover on the causes of action alleged;
- 13 d) Individual actions would create a risk of inconsistent results and would be
14 unnecessary and duplicative of this litigation; and
- 15 e) The disposition of the claims of the members of the Class through this class action
16 will produce salutary by-products, including a therapeutic effect upon those who
17 indulge in fraudulent practices, and aid to legitimate business enterprises by
18 curtailing illegitimate competition.

19 61. Plaintiff knows of no difficulty that will be encountered in the management of this
20 litigation that would preclude its maintenance as a class action. As a result, a class action is
21 superior to other available methods for the fair and efficient adjudication of this controversy.

22 62. Notice to the members of the Class may be made by e-mail or first-class mail
23 addressed to all persons who have been individually identified by Defendants and who have been
24 given notice of the data breach.

25 63. Plaintiff and the Class have suffered irreparable harm and damages because of
26 Defendants' wrongful conduct as alleged herein. Absent certification, Plaintiff and the Class will
27 continue to be damaged and to suffer by the unauthorized disclosure and/or release of their medical
28

1 and personal identifying information, thereby allowing these violations of law to proceed without
2 remedy.

3 64. Moreover, Plaintiff's and the Class' individual damages are insufficient to justify the
4 cost of litigation, so that in the absence of class treatment, Defendants' violations of law inflicting
5 substantial damages in the aggregate would go unremedied. In addition, Defendants have acted or
6 refused to act on grounds generally applicable to Plaintiff and the Class, thereby making appropriate
7 final injunctive relief with respect to, the Class as a whole.

8 **FIRST CAUSE OF ACTION**
9 **Violations of the Confidentiality of Medical Information Act**
10 **California Civil Code §§ 56, et seq.**
11 **(On Behalf of Plaintiff and the Class Against HCP)**

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

14 66. At all times relevant to this action, including the period from October 22, 2020 to
15 December 3, 2020, HCP is considered a "provider of health care" within the meaning of Civil Code
16 § 56.05(m) and 56.06(a) & (b), a "contractor" under Civil Code § 56.05(d), and/or "engaged in the
17 business of furnishing administrative services to programs that provide payment for health care
18 services" under Civil Code § 56.26(a), and maintained and continues to maintain "medical
19 information" within the meaning of Civil Code § 56.05(j), of Plaintiff and the Class.

20 67. Plaintiff and the Class are "patients" within the meaning of Civil Code § 56.05(k)
21 because they are natural persons, who received health care services from a provider of health care
22 and to whom medical information pertains. Plaintiff and the Class are "Endanger" within the
23 meaning of Civil Code § 56.05(e) because they fear that disclosure and/or release of their medical
24 information could subject them to harassment or abuse.

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

1 confidentiality of the information, and negligently failed to protect and preserve confidentiality of
2 electronic medical information of Plaintiff and the Class in its possession, as required by the Act,
3 and specifically, under Civil Code §§ 56.06(d), 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a),
4 56.101(b)(1)(A), and 56.36(e)(2)(E).

5 69. Due to HCP's negligent creation, maintenance, preservation and/or storage of
6 Plaintiff's and the Class members' medical and personal identifying information on HCP's
7 computer networks and NETGAIN's computer server, HCP allowed Plaintiff's and the Class'
8 medical information, including Plaintiff's and the Class' names, addresses, dates of birth,
9 diagnosis/treatment information and treatment cost information, in electronic form, to be accessed
10 and actually viewed by at least one unauthorized third party, without first obtaining an
11 authorization, constituting a disclosure in violation of Civil Code §§ 56.06(d), 56.10, 56.13, 56.245,
12 and 56.26(a).

13 70. 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 HCP's
15 computer networks and NETGAIN's computer server, HCP allowed Plaintiff's and the Class'
16 medical information, including Plaintiff's and the Class' names, addresses, dates of birth,
17 diagnosis/treatment information and treatment cost information, in electronic form, to be accessed
18 and actually viewed by at least one unauthorized third party, constituting a release in violation of
19 Civil Code § 56.101(a).

20 71. 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 HCP's
22 computer networks and NETGAIN's computer server, HCP allowed Plaintiff's and the Class'
23 medical information, including Plaintiff's and the Class' names, addresses, dates of birth,
24 diagnosis/treatment information and treatment cost information, in electronic form, to be accessed
25 and actually viewed by at least one unauthorized third party, constituting a release in violation of
26 Civil Code § 56.101(b)(1)(A).

27

28

1 76. 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 77. 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 78. HCP was aware that Plaintiff’s and the Class’ unencrypted personal information on
18 NETGAIN’s computer server was, or is reasonably believed to have been, acquired by an
19 unauthorized person no later than December 3, 2020, but did not begin to mail notification letters to
20 Plaintiff and the Class until April 12, 2021. Thus, HCP waited at least 131 days before *beginning* to
21 inform Plaintiff and the Class of this incident and the subsequent threat to Plaintiff’s and the Class’
22 personal information. As a result, HCP did not disclose to Plaintiff and the Class that their personal
23 information was, or was reasonably believed to have been, acquired by an unauthorized person, in
24 the most expedient time possible and without reasonable delay in violation of Civil Code §
25 1798.82(a). Given the example of the Legislature finding that a delay of 21 days to be “late notice”
26 under the statute, HCP’s delay of 131 days before *beginning* to inform Plaintiff and the Class that
27 their personal information was, or was reasonably believed to have been, acquired by an
28

1 unauthorized person by mailing HCP's form letter to Plaintiff and the Class is presumptively
2 unreasonable notice in violation of Civil Code § 1798.82(a).

3 79. 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 80. 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) from Defendants.

13 **THIRD 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 and the Class Against All Defendants)**

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

19 82. 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 83. 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 84. 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 and the Class in their possession, and
8 failing to protect and preserve confidentiality of electronic medical information of Plaintiff and the
9 Class in their possession against disclosure and/or release, outweighs the utility of such conduct and
10 such conduct offends public policy, is immoral, unscrupulous, unethical, deceitful and offensive,
11 and causes substantial injury to Plaintiff and the Class.

12 85. Defendants have obtain money and property from Plaintiff and the Class because of
13 the payment of the services and products they received from Defendants. Plaintiff and the Class
14 have suffered an injury in fact by acquiring less in their transactions with Defendants for the
15 services and products they received from Defendants than they otherwise would have if Defendants
16 would had adequately protected the confidentiality of their medical and personal identifying
17 information.

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

24 87. The aforementioned unlawful, fraudulent and unfair business acts or practices
25 conducted by Defendants have been committed in the past and continues to this day. Defendants
26 have failed to acknowledge the wrongful nature of their actions. Defendants have not corrected or
27 publicly issued comprehensive corrective notices to Plaintiff and the Class, and have not corrected
28

1 or enacted adequate privacy policies and procedures to protect and preserve confidentiality of
2 medical and personal identifying information of Plaintiff and the Class in their possession.

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

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

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

20 **PRAYER FOR RELIEF**

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

23 **As for the First Cause of Action**

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

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

As for the Second Cause of Action

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

As for the Third Cause of Action

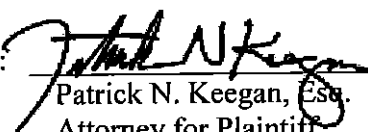
- 5. For an order awarding Plaintiff and the Class restitution of all monies wrongfully acquired by Defendants by means of such unlawful, fraudulent and unfair business acts and practices;
- 6. For injunctive relief in the form of an order instructing Defendants to prohibit the unauthorized release of medical and personal identifying information of Plaintiff and the Class, and to adequately maintain the confidentiality of the medical and personal identifying information of Plaintiff and the Class;
- 7. For injunctive relief in the form of an order enjoining Defendants from disclosing the medical and personal identifying information of Plaintiff and the Class without the prior written authorization of each Plaintiff and the Class member;

As to All Causes of Action

- 8. That the Court issue an Order certifying this action be certified as a class action on behalf of the proposed Class, appointing Plaintiff as representative of the proposed Class, and appointing Plaintiff's attorneys, as counsel for members of the proposed Class;
- 9. For an award of attorneys' fees as authorized by statute, including, but not limited to, the provisions of California Code of Civil Procedure § 1021.5, and as authorized under the "common fund" doctrine, and as authorized by the "substantial benefit" doctrine;
- 10. For costs of the suit;
- 11. For prejudgment interest at the legal rate; and
- 12. Any such further relief as this Court deems necessary, just, and proper.

Dated: September 13, 2021

KEEGAN & BAKER LLP

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

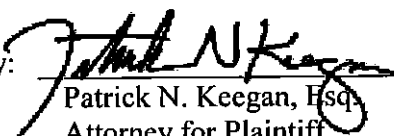
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

Plaintiff 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 13, 2021

KEEGAN & BAKER LLP

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

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Health Center Partners of Southern California, IT Provider Facing Class Action Over Cyberattack Affecting 293K](#)
