

EDELSBERG LAW, P.A.

Scott Edelsberg, Esq. (CA Bar # 330090)

scott@edelsberglaw.com

1925 Century Park East, Suite 1700

Los Angeles, CA 90067

Telephone: (305) 975-3320

Counsel for Plaintiff

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
FRESNO DIVISION**

AQUELIA WALKER, *Individually and
On Behalf of All Others Similarly
Situated,*

Plaintiff,

v.

RADNET, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 **CLASS ACTION COMPLAINT**

2 Plaintiff Aquelia Walker, on behalf of herself and all others similarly situated,
3 files this Complaint against Defendant RadNet, Inc. (“RadNet” or “Defendant”).
4 Plaintiff’s allegations are made on personal knowledge as to Plaintiff and Plaintiff’s
5 own acts and upon information and belief as to all other matters.
6

7 **I. NATURE OF THE ACTION**

8
9 1. This is a medical privacy class action complaint against RadNet, Inc.,
10 as the owner of *radnet.com*, for knowingly and repeatedly intercepting, and
11 disclosing to a third party, Meta Platforms, Inc. (“Facebook”), confidential patient
12 communications and data from RadNet’s website containing its patients’ personally
13 identifiable information (“PII”) and/or statutorily-protected patient health
14 information (“PHI”) (together, “User Data”) without their knowledge, authorization,
15 or consent, in violation of various state laws, the California constitution, and as well
16 as Defendant’s privacy policy with its patients.
17
18

19
20 2. Like many other hospitals and healthcare providers, RadNet
21 encourages patients to use its website and “secure” online patient portal to
22 communicate with RadNet. Plaintiff and Class Members used *radnet.com* to
23 communicate with their doctors, view lab results, schedule medical appointments,
24 and find treatment options.
25

26
27 3. Patients who exchange communications with RadNet have a reasonable
28 expectation of privacy that their personally identifiable data and the content of their

1 communications will not be intercepted, transmitted, re-directed, or disclosed by
2 RadNet to third parties without the patient’s knowledge, consent, or authorization.

3 4. Defendant aids, employs, agrees, and conspires with Facebook, through
4 the use of the Facebook Pixel, to intercept communications sent and received by
5 Plaintiff and Class Members, including communications containing protected
6 medical information.
7

8 5. The Facebook Pixel is a code Defendant installed on its website and
9 patient portal allowing it to collect and transmit patients’ communications containing
10 personally identifiable, sensitive medical information. More specifically, it
11 automatically intercepts and transmits protected medical information, including, but
12 not limited to diagnoses, treatment information, lab results, medications, and
13 appointment times. This occurs even when the patient has not shared (nor consented
14 to share) such information.
15
16
17

18 6. Unbeknownst to Plaintiff and Class Members, and pursuant to the
19 systemic process described herein, whenever a patient uses RadNet’s website and
20 patient portal, patients’ private and protected communications with RadNet were
21 automatically transmitted and communicated to Facebook, alongside other
22 information—including diagnoses, treatment information, lab results, medications,
23 appointment times, and patients’ unique Facebook ID (“FID”)—as a result of
24 Defendant’s decision to install and use tracking pixels on its website.
25
26
27
28

1 7. Importantly, because the patient’s FID uniquely identifies an
2 individual’s Facebook user account, Facebook—or any other ordinary person—can
3 use it to quickly and easily locate, access, and view patients’ corresponding
4 Facebook profile. Put simply, Facebook Pixel grants Facebook knowledge of the
5 private medical information of RadNet’s patients communicated on the *Radnet.com*
6 site.
7

8
9 8. Defendant disregarded Plaintiff’s and hundreds of thousands of other
10 patients’ statutorily protected, constitutional, and common law privacy rights by
11 intercepting and releasing their sensitive personal medical information to Facebook.
12 As a result, Defendant violated state statutes, including the California Invasion of
13 Privacy Act, Cal. Penal Code §§ 630 *et seq.* (“CIPA”), and the California
14 Confidentiality of Medical Information Act, Cal. Civil Code §§ 56 *et seq.* (“CMIA”).
15 Defendant’s conduct also constitute an invasion of privacy under California’s
16 Constitution and the common law, and a breach of contract.
17
18

19
20 9. Accordingly, Plaintiff brings this class action for legal and equitable
21 remedies to redress and put a stop to Defendant’s practice of intentionally disclosing
22 its patients’ User Data to Facebook in knowing violation of state privacy laws, the
23 California constitution, and its privacy policy.
24

25 **II. JURISDICTION AND VENUE**

26 10. Court has jurisdiction over the subject matter of this action pursuant to
27 28 U.S.C. § 1332(d)(2), because the matter in controversy exceeds \$5,000,000,
28

1 exclusive of interest and costs, and is a class action in which at least one member of
2 the class is a citizen of a different State than Defendant. The number of members of
3 the proposed Classes in aggregate exceeds 100 users. 28 U.S.C. § 1332(d)(5)(B).
4

5 11. Venue is appropriate in this District pursuant to 28 U.S.C. § 1391
6 because Defendant resides in and is subject to personal jurisdiction in this District.
7 Venue is also proper because a substantial part of the events or omissions giving rise
8 to the claim occurred in or emanated from this District.
9

10 **III. DIVISIONAL ASSIGNMENT**

11 12. Assignment to the Fresno Division is appropriate because Plaintiff is
12 domiciled in Fresno County and a substantial part of the events or omissions giving
13 rise to this action occurred in Fresno County.
14

15 **IV. PARTIES**

16 13. Defendant RadNet, Inc., is a Delaware corporation with its principal
17 place of business in Los Angeles, California. RadNet is a provider of outpatient
18 diagnostic imaging services, with locations across California and in Arizona,
19 Florida, Delaware, Florida, Maryland, New Jersey, and New York. RadNet was
20 founded in 1984 as a small radiology imaging center in Los Angeles. Now, with over
21 332 imaging centers and thousands of patients, RadNet's estimated annual revenues
22 exceed \$1 billion.
23
24
25

26 14. Plaintiff Aquelia Walker is an adult citizen of California and is
27 domiciled in Clovis, California. Plaintiff has been a patient of RadNet since at least
28

1 2013 and continues to remain a patient to this day. At all relevant times, Plaintiff
2 has had a Facebook account.

3 15. Plaintiff entrusted her User Data to Defendant as a condition of
4 receiving Defendant's healthcare services.
5

6 16. To receive healthcare services from Defendant, and at Defendant's
7 direction, Plaintiff accessed Defendant's website. From 2013 to the present, Plaintiff
8 used RadNet's website to manage her appointments, access testing and imaging
9 results, view doctor's notes, message healthcare providers, and review medications
10 and treatment information.
11

12 17. Plaintiff reasonably expected that her online communications with
13 Defendant were confidential, solely between herself and Defendant, and that such
14 communications would not be transmitted to or intercepted by a third party.
15

16 18. Plaintiff provided her User Data to RadNet and trusted that the
17 information would be safeguarded according to its privacy policy and state and
18 federal law.
19

20 19. To access RadNet's patient portal, Plaintiff provided, among other
21 information, her name, date of birth, full address, email address, phone number, IP
22 address (which informs RadNet as to the city and zip code she resides in as well as
23 her physical location), and any cookies associated with her device.
24

25 20. Plaintiff never consented, agreed, authorized, or otherwise permitted
26 RadNet to disclose her User Data to Facebook. Plaintiff has never been provided any
27
28

1 written notice that RadNet discloses its patients' User Data, or any means of opting
2 out of such disclosures of her User Data. Nonetheless, RadNet knowingly disclosed
3 Plaintiff's User Data to Facebook.
4

5 21. By law, Plaintiff is entitled to privacy in her User Data and confidential
6 electronic communications. RadNet deprived Plaintiff of her privacy rights when it:
7 (i) implemented a system that surreptitiously tracked, recorded, and disclosed
8 Plaintiff's and other and other online patients' confidential communications and
9 User Data; (2) disclosed patients' protected information to Facebook; and (3)
10 undertook this pattern of conduct without notifying Plaintiff and without obtaining
11 her express written consent.
12
13

14 22. Plaintiff has a continuing interest in ensuring that Plaintiff's User Data,
15 which, upon information and belief, remain backed up in RadNet's possession, is
16 protected, and safeguarded from future breaches.
17

18 **V. FACTUAL ALLEGATIONS**

19 **A. Radnet's Website and Privacy Policy**

20 23. Defendant operates a website in the U.S. accessible from a desktop and
21 mobile device at *radnet.com*.
22

23 24. Defendant provides its patients with a website, *radnet.com*, that
24 includes an online patient portal through which patients can manager their health
25 care needs. For example, through the online patient portal, patients can communicate
26 with their healthcare providers, schedule appointments, pay bills, and view
27
28

1 information about past and upcoming appointments. Patients can also view their
2 clinical notes, electronic health information, medical records, and test results, as
3 soon as they become available, and access other healthcare related services.
4

5 25. Defendant encourages its patients to use its online patient portal.

6 26. Patients access the patient portal through the *radnet.com* website by
7 logging in with their username and password.
8

9 27. RadNet’s Website Privacy Policy in effect prior to the 2023 update,
10 attached as **Exhibit 1**, represented that Defendant “respects the privacy of everyone
11 who uses our Web site.” Indeed, it touted RadNet’s “commitment to ensuring that
12 privacy.”
13

14 28. The Website Privacy Policy promises that “You may rest assured that
15 any further confidential information obtained, such as medical records and test
16 results, will not be shared with anyone other than the appropriate and authorized
17 RadNet staff, medical physicians, and payors.”
18

19 29. The Website Privacy Policy also indicates that “any information
20 [RadNet] obtained, which is limited to names and e-mail addresses, will be used
21 solely for internal objectives, such as creating user profiles and for other RadNet
22 marketing purposes.”
23
24

25 30. Further, RadNet’s Website Privacy Policy purports to include an opt-
26 out provision for “information used for purposes not directly related to the RadNet
27
28

1 Web site” and represents that “Users are also notified when their information is
2 being collected by any outside parties.”

3 31. Notwithstanding these promises, RadNet deployed Facebook’s Pixel on
4 its website and patient portal that caused the contemporaneous unauthorized
5 transmission of User Data and the precise content of patient communications with
6 RadNet’s patient portal to Facebook whenever a patient uses the patient portal.
7

8
9 **B. How RadNet Intercepts and Discloses Patients’ Personally Identifiable
10 Information and Protected Health Information**

11 **i. Tracking Pixels**

12 32. Websites and apps use Facebook’s Pixel and SDK to collect
13 information about user’s devices and activities and send that to Facebook. Facebook
14 then uses that information to show the user targeted ads.
15

16 33. The Facebook tracking Pixel, also known as a “tag” or “web beacon”
17 among other names, is an *invisible* tool that tracks consumers’ actions on Facebook
18 advertisers’ websites and reports them to Facebook. It is a version of the social
19 plugin that gets “rendered” with code from Facebook. To obtain the code for the
20 pixel, the website advertiser tells Facebook which website events it wants to track
21 (e.g., messaging a healthcare provider or scheduling appointments) and Facebook
22 returns corresponding Facebook Pixel code for the advertiser to incorporate into its
23 website.
24
25

26 34. Through this technology, Facebook intercepts each page a user visits,
27 what buttons they click, as well as specific information they input into the website
28

1 and what they searched. The Facebook Pixel sends each of these pieces of
2 information to Facebook with PII, such as the user’s IP address. Facebook stores this
3 data on its own server, and, in some instances, for years on end.¹
4

5 35. The Pixel harvests this data – even when a user is not logged into
6 Facebook.²
7

8 36. Unbeknownst to Plaintiff and Class Members, Defendant installed the
9 Facebook Pixel, not only on its website, but also on the portal that patients use to
10 communicate sensitive, non-public, personal and health information to Defendant.
11 As implemented by Defendant, the tracking Pixel was configured to collect and
12 transmit the User Data of Plaintiff and Class Members to Facebook without their
13 knowledge or consent.
14

15 37. Defendant installed the Facebook tracking Pixel, which enables it to
16 intercept and disclose Plaintiff’s and Class Members’ User Data to Facebook,
17 because it benefits financially from the advertising analytics and information
18 services that stem from use of the Pixel. For example, in exchange for installing the
19 pixel, Facebook provides Defendant with analytics about the ads they’ve placed on
20 Facebook and Instagram and insight on other tools to target people who’ve visited
21 their website.
22
23
24
25

26 ¹ Grace Oldham and Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting*
27 *Highly Sensitive Info on Would-Be Patients*, The Markup (June 15, 2022),
28 [https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-
highly-sensitive-info-on-would-be-patients](https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients) (last visited Feb. 14, 2023).

² *Id.*

1 38. When a RadNet patient uses its patient portal to schedule an
2 appointment, access test results, review diagnoses, or conducts any action, the
3 website sends certain information about the patient to Facebook, including, but not
4 limited to, their identity and specific communications and health procedures they
5 underwent. Accordingly, the Pixel allows RadNet to intercept and disclose sensitive
6 User Data.
7

8 **ii. Facebook ID (“FID”)**
9

10 39. An FID is a unique and persistent identifier that Facebook assigns to
11 each user. With it, anyone ordinary person can look up the user’s Facebook profile
12 and name. When a Facebook user with one or more personally identifiable FID
13 cookies on his or her browser uses RadNet’s patient portal, through its website code,
14 causes the patient’s User Data to be transmitted to Facebook by the user’s browser.
15 This transmission is not the patient’s decision, but results from Defendant’s
16 purposeful use of the Facebook tracking pixel by incorporation of that pixel and code
17 into the RadNet patient portal.
18
19

20 40. Defendant could easily program its website to prevent its patients’ User
21 Data from being automatically transmitted to Facebook when a patient logs in and
22 uses the portal. However, it is not in Defendant’s financial interest to do so because
23 it benefits financially by providing this highly sought-after information.
24
25

26 41. Notably, while Facebook can easily identify any individual on its
27 Facebook platform with only their unique FID, so too can any ordinary person who
28

1 comes into possession of an FID. Facebook admits as much on its website. Indeed,
2 ordinary persons who come into possession of the FID can connect to any Facebook
3 profile. Simply put, with only an FID and the sensitive User Data—all of which
4 Defendant knowingly and readily provides to Facebook without any consent from
5 patients—any ordinary person can connect the identity of the Facebook user profile
6 with the types of medical procedures the patient underwent, and even access the
7 patient’s doctor’s notes from Defendant.
8
9

10 42. At all relevant times, Defendant knew that the Facebook Pixel
11 intercepted and disclosed User Data to Facebook. This was evidenced from, among
12 other things, the functionality of the Pixel, i.e., sending all interactions and
13 communications on its website to Facebook.
14

15 **C. RadNet Health Unlawfully Discloses Its Patients’ Personally Identifiable**
16 **Patient Information and Protected Health Information to Facebook**

17 43. RadNet maintains a vast digital database comprised of its patients’ User
18 Data, including the names and e-mail addresses of each patient, and their
19 confidential medical records.
20

21 44. RadNet is not sharing anonymized, non-personally identifiable data
22 with Facebook. To the contrary, the data it discloses is tied to unique identifiers that
23 track specific Facebook users. Importantly, the recipient of the User Data—
24 Facebook—*receives the information as one data point*. Defendant has thus
25 monetized its database by disclosing its patients’ PHI to Facebook in a manner
26 allowing it to make a direct connection to patients’ personal identities—without the
27
28

1 consent of its patients and to the detriment of their legally protected privacy and
2 medical rights.

3 45. Critically, the User Data Defendant discloses to Facebook allows
4 Facebook to build from scratch or cross-reference and add to the data it already has
5 in their own detailed profiles for its own users, adding to its trove of personally
6 identifiable data.
7

8 46. In June 2022, an investigation by The Markup revealed that the
9 Facebook Pixel is embedded on the websites of 33 of the top 100 hospitals in the
10 nation, collecting User Data, and transmitting it to Facebook when a user interacts
11 with the website. For example, when a patient schedules an appointment online, the
12 pixel intercepted and transmitted the details of the patient's doctor appointment,
13 including the doctor's name, and search term used to find the doctor.³
14

15 47. Worse, this surveillance persisted even inside the password-protected
16 patient portals, like RadNet's portal, of at least seven health systems. When a user
17 navigates through their patient portal, the tracking Pixel collects intimate patient
18 details, such as prescriptions, sexual orientation, and health conditions, and sends
19 that data to Facebook.⁴
20

21 48. The 33 hospitals found to have the Facebook Pixel collecting and
22 sending patient appointment details to Facebook collectively reported more than 26
23
24
25
26
27

28 ³ *Id.*

⁴ *Id.*

1 million patient admissions and outpatient visits in 2020 alone. But the number of
2 impacted patients is likely higher as The Markup's investigation was limited to just
3 over 100 hospitals.

4
5 49. As a result of Defendant's data compiling and sharing practices,
6 Defendant has knowingly disclosed to Facebook (for its own personal profit) the
7 User Data of its patients.

8
9 50. Defendant does not seek its patients' prior written consent to the
10 disclosure of their User Data (in writing or otherwise) and its patients remain
11 unaware that their User Data is being disclosed to Facebook.

12
13 51. Plaintiff and Class Members had no way of knowing that Defendant
14 was disclosing, and Facebook was intercepting, their User Data, including sensitive
15 medical information, when they engaged with RadNet's website because the
16 software is inconspicuously incorporated in the background.

17
18 52. This undisclosed conduct is even more egregious given the nature of
19 the information entered in the RadNet patient portal, e.g., PII, test and lab results,
20 requests for appointments, messages to health care providers, and other health
21 information, among other things. Plaintiff and Class Members would not expect this
22 information would be disclosed or intercepted without their consent. This is
23 especially true given RadNet's consistent representations that this information
24 would remain private and confidential.
25
26
27
28

1 53. Plaintiff and Class Members could not consent to RadNet’s conduct
2 when they were never aware their sensitive medical information would be disclosed
3 to and intercepted by Facebook.
4

5 **D. Defendant Does Not Need to Disclose Personally Identifiable Patient**
6 **Information and Protected Health Information to Operate its Website**
7 **and App**

8 54. Tracking pixels are not necessary for Defendant to operate its website
9 and patient portal. They are deployed on Defendant’s website for the sole purpose
10 of enriching Defendant and Facebook.

11 55. Even if a healthcare provider found it useful to integrate Facebook
12 tracking pixels, Defendant is not required to disclose User Data to Facebook. In any
13 event, if Defendant wanted to do so, it must first comply with the federal and state
14 privacy laws described herein, which it failed to do.
15

16 **E. Defendant Had an Obligation to Protect its Patients’ Personally**
17 **Identifiable Patient Information and Protected Health Information**

18 56. Defendant has a legal duty to maintain its patient’s User Data as
19 confidential and to protect Plaintiff’s and Class Members’ User Data from disclosure
20 to third parties.
21

22 57. Defendant’s failure to adequately secure Plaintiff’s and Class
23 Members’ sensitive User Data breaches duties it owes Representative Plaintiff and
24 Class Members under statutory and common law.
25

26 58. Under the Health Insurance Portability and Accountability Act of 1996
27 (“HIPAA”), health insurance providers have an affirmative duty to keep patients’
28

1 User Data private. As a covered entity, Defendant has a statutory duty under HIPAA
2 and other federal and state statutes to safeguard Plaintiff’s and Class Members’ User
3 Data. Moreover, Plaintiff and Class Members surrendered their highly sensitive
4 personal data to Defendant under the implied condition that Defendant would keep
5 it private and secure. Accordingly, Defendant also has an implied duty to safeguard
6 their data, independent of any statute.
7

8
9 59. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is
10 required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164,
11 Subparts A and E (“Standards for Privacy of Individually Identifiable Health
12 Information”), and Security Rule (“Security Standards for the Protection of
13 Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164,
14 Subparts A and C.
15

16
17 60. HIPAA’s Privacy Rule or Security Standards for Privacy of
18 Individually Identifiable Health Information establishes national standards for the
19 protection of health information, including health information that is kept or
20 transferred in electronic form.
21

22 61. HIPAA requires Defendant to “comply with the applicable standards,
23 implementation specifications, and requirements” of HIPAA “with respect to
24 electronic protected health information.” 45 C.F.R. § 164.302.
25
26
27
28

1 62. “Electronic protected health information” is “individually identifiable
2 health information ... that is (i) transmitted by electronic media; maintained in
3 electronic media.” 45 C.F.R. § 160.103.
4

5 63. HIPAA’s Security Rule requires Defendant to do the following:

6 a) Ensure the confidentiality, integrity, and availability of all
7 electronic protected health information the covered entity or business associate
8 creates, receives, maintains, or transmits;
9

10 b) Protect against any reasonably anticipated threats or hazards to
11 the security or integrity of such information;
12

13 c) Protect against any reasonably anticipated uses or disclosures of
14 such information that are not permitted; and
15

16 d) Ensure compliance by its workforce.

17 64. HIPAA also requires Defendant to “review and modify the security
18 measures implemented ... as needed to continue provision of reasonable and
19 appropriate protection of electronic protected health information” under 45 C.F.R. §
20 164.306(e), and to “[i]mplement technical policies and procedures for electronic
21 information systems that maintain electronic protected health information to allow
22 access only to those persons or software programs that have been granted access
23 rights.” 45 C.F.R. § 164.312(a)(1).
24
25

26 65. In addition to its obligations under federal and state laws, Defendant
27 owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining,
28

1 retaining, securing, safeguarding, deleting, and protecting the User Data in
2 Defendant's possession from being compromised, lost, stolen, accessed, and
3 misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class
4 Members to provide reasonable security, including consistency with industry
5 standards and requirements, and to ensure that its computer systems, networks, and
6 protocols adequately protected the User Data of Plaintiff and Class Members.
7

8
9 **F. Plaintiff and Class Members Have a Reasonable Expectation of Privacy
10 in Their User Data**

11 66. Plaintiff and Class Members have a reasonable expectation of privacy
12 in their User Data, including sensitive medical information.

13 67. Privacy polls and studies uniformly show that most Americans consider
14 one of the most important privacy rights to be the need for an individual's affirmative
15 consent before a company collects and shares its customers' personal data.
16

17 68. For example, a recent study by Consumer Reports shows that 92% of
18 Americans believe that internet companies and websites should be required to obtain
19 consent before selling or sharing consumers' data, and the same percentage believe
20 internet companies and websites should be required to provide consumers with a
21 complete list of the data that has been collected about them.
22

23
24 69. Moreover, according to a study by Pew Research Center, a majority of
25 Americans, approximately 79%, are concerned about how data is collected about
26 them by companies.
27
28

1 70. Users act consistent with these preferences. Following a new rollout of
2 the iPhone operating software—which asks users for clear, affirmative consent
3 before allowing companies to track users—85% of worldwide users and 94% of U.S.
4 users chose not to share data when prompted.
5

6 71. Another recent study by DataGrail revealed that 67% of people were
7 willing to pay \$100 or more annually to keep their information out of the hands of
8 companies and the government.
9

10 72. The same study revealed that 75% of people would abandon brands that
11 do not take care of their data.
12

13 73. Other privacy law experts have expressed concerns about the disclosure
14 to third parties of a user’s sensitive medical information. For example, Dena
15 Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current
16 Director of Health Policy and Data Governance at Elektra Labs—explained that
17 having your personal health information disseminated in ways you are unaware of
18 could have serious repercussions, including affecting your ability to obtain life
19 insurance and how much you pay for that coverage, increasing the rate you are
20 charged on loans, and leaving you vulnerable to workplace discrimination.
21
22

23 **G. The Data RadNet Intercepted is Plaintiff’s Property, Has Economic**
24 **Value, and its Unlawful Disclosure Caused Economic Harm**

25 74. There is an economic market for consumers’ personal data—including
26 the User Data RadNet allowed Facebook to intercept from Plaintiff and Class
27 Members.
28

1 75. For instance, according to Experian, health data is a “gold mine” for
2 health care companies and clinicians.

3 76. In 2013, the Financial Times reported that the data-broker industry
4 profits from the trade of thousands of details about individuals, and within that
5 context, “age, gender and location” information are sold for about “\$0.50 per 1,000
6 people.”⁵ This estimate was based upon “industry pricing data viewed by the
7 Financial Times,” at the time.⁶

8
9
10 77. In 2015, TechCrunch reported that “to obtain a list containing the
11 names of individuals suffering from a particular disease,” a market participant would
12 have to spend about “\$0.30 per name.”⁷ That same article noted that “Data has
13 become a strategic asset that allows companies to acquire or maintain a competitive
14 edge”⁸ and that the value of a single user’s data (within the corporate acquisition
15 context) can vary from \$15 to more than \$40 per user.⁹

16
17
18 78. Notably, a 2021 report from Invisibly found that personal medical
19 information is one of the most valuable pieces of data within this data-market. “It’s
20 worth acknowledging that because health care records often feature a more complete
21 collection of the patient’s identity, background, and PII, health care records have
22
23
24

25 ⁵ Emily Steel, et al., *How much is your personal data worth?*, Fin. Times (June 12, 2013),
26 <https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz3myQiw6u>.

27 ⁶ *Id.*

28 ⁷ Pauline Glickman and Nicolas Glady, *What’s the Value of Your Data?*, TechCrunch (October
13, 2015), <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>.

⁸ *Id.*

⁹ *Id.*

1 proven to be of particular value for data thieves. While a single social security
 2 number might go for \$0.53, a complete health care record sells for \$250 on average.
 3 For criminals, the more complete a dataset, the more potential value they can get out
 4 of it. As a result, healthcare breaches increased 55% in 2020.”¹⁰ The article noted
 5 the following breakdown in average price for record type:
 6

Record Type	Average Price
Health Care Record	\$250.15
Payment Card Details	\$5.40
Banking Records	\$4.12
Access Credentials	\$0.95
Social Security Number	\$0.53
Credit Record	\$0.31
Basic PII	\$0.03

7
 8
 9
 10
 11
 12
 13
 14
 15
 16
 17 79. The Federal Trade Commission has also confirmed the value of user
 18 data and, particularly, health information. In 2014, it found that data brokers sell data
 19 that categorize users into sensitive categories, such as “expectant parent.”¹¹ It
 20 recently sued one of these companies for selling location data on people who visit
 21 abortion clinics for approximately \$160 a week.
 22
 23
 24

25
 26 ¹⁰ *How Much is Your Data Worth? The Complete Breakdown for 2021*, Invisibly (July 13, 2021),
<https://www.invisibly.com/learn-blog/how-much-is-data-worth/>.

27 ¹¹FTC, *Data Brokers: A Call for Transparency and Accountability* (May
 28 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

1 80. Indeed, even access to just prescription information is extremely
2 valuable. For instance, Datarade.ai advertises access to U.S. customers names,
3 addresses, email addresses, telephone numbers who bought brand name medicine.
4 The starting price for access to just some of this data was \$10,000. Other companies,
5 like Pfizer, spend \$12 million annually to purchase health data and the medical data
6 industry itself was valued at over \$2.6 billion back in 2014.
7

8
9 81. Furthermore, individuals can sell or monetize their own data if they so
10 choose. A myriad of other companies and apps such as Nielsen Data, Killi,
11 DataCoup, and AppOptix offer consumers money in exchange for their personal
12 data.
13

14 82. Moreover, “courts have recognized the ‘growing trend across courts . .
15 . to recognize the lost property value’ of personal information. *In re Marriott Int’l,*
16 *Inc., Cust. Data Sec. Breach Litig.*, 440 F.Supp.3d 447, 461 (D. Md. 2020) . . .; *see*
17 *also In re Facebook Privacy Litigation*, 557 F.App’x. 494, 494 [sic] (9th Cir. 2014).”
18 *Calhoun v. Google LLC*, 526 F.Supp.3d 605, 636 (N.D. Cal. 2021).”
19
20

21 83. Given the monetary value already assigned to personal information,
22 RadNet has deprived Plaintiff and Class Members of the economic value of their
23 sensitive medical information by acquiring such data without providing proper
24 consideration for Plaintiff’s and Class Members’ property.
25

26 **VI. TOLLING, CONCEALMENT, AND ESTOPPEL**
27
28

1 84. The applicable statutes of limitation have been tolled as a result of
2 RadNet's knowing and active concealment and denial of the facts alleged herein.

3 85. RadNet secretly incorporated the Facebook Pixel into its website and
4 patient portal, providing no indication to users that their User Data, including PII
5 and medical information, would be disclosed to Meta.
6

7 86. RadNet possessed exclusive knowledge that the Facebook Pixel was
8 incorporated on its website and patient portal, yet failed to disclose that fact to users,
9 or that by interacting with its website and patient portal Plaintiff's and Class
10 Members' User Data, including PII and health data, would be disclosed to Facebook.
11

12 87. Plaintiff and Class Members could not with due diligence have
13 discovered the full scope of RadNet's conduct, including because the incorporation
14 of the Facebook Pixel is surreptitious, highly technical and there were no disclosures
15 or other indication that would inform a reasonable consumer that RadNet was
16 disclosing to and allowing the interception of User Data, including PII and health
17 data, by Facebook.
18

19 88. The earliest Plaintiff and Class Members could have known about
20 Defendant's conduct was shortly before the filing of this Complaint.
21

22 89. RadNet was under a duty to disclose the nature and significance of its
23 data disclosure practices but did not do so. RadNet is therefore estopped from relying
24 on any statute of limitations under the discovery rule.
25
26
27
28

1 90. Additionally, RadNet engaged in fraudulent conduct to prevent
2 Plaintiff and Class Members from discovering the disclosure and interception of
3 their data. RadNet misled Plaintiff and Class Members to believe their User Data,
4 including health information and PII, would not be disclosed.
5

6 91. Plaintiff and Class Members were not aware that RadNet disclosed their
7 User Data, including PII and health information.
8

9 92. Plaintiff and Class Members exercised due diligence to uncover the
10 facts alleged herein and did not have actual or constructive knowledge of RadNet's
11 misconduct by virtue of their fraudulent concealment.
12

13 93. Accordingly, all statutes of limitations are tolled under the doctrine of
14 fraudulent concealment.
15

16 **VII. CLASS ACTION ALLEGATIONS**

17 94. Plaintiff brings this action on behalf of herself and all others similarly
18 situated as a class action under Rules 23(a) and (b)(3) of the Federal Rules of Civil
19 Procedure, on behalf of the following Classes (collectively, the "Class"):
20

21 **Nationwide Class:** All persons in the United States who
22 are, or were patients of Defendant, and accessed an online
23 website owned and/or operated by Defendant that caused
24 a transmission of personally identifiable information, PHI,
and other electronic communications to be made to
Facebook.

25 **California Subclass:** All California persons who are, or
26 were patients of Defendant, and accessed an online
27 website owned and/or operated by Defendant that caused
28 a transmission of personally identifiable information, PHI,

1 and other electronic communications to be made to
2 Facebook.

3 Excluded from the Classes are Defendant, their past or current officers, directors,
4 affiliates, legal representatives, predecessors, successors, assigns and any entity in
5 which any of them have a controlling interest, as well as all judicial officers assigned
6 to this case as defined in 28 USC § 455(b) and their immediate families.
7

8 95. Numerosity. Members of the Classes are so numerous that joinder of
9 all members of the Class is impracticable. The exact number of Class Members is
10 unknown to Plaintiff at this time; however, it is estimated that there are thousands of
11 individuals in the Classes. Class Members can be readily identified from
12 Defendant's records and non-party Facebook's records.
13

14 96. Typicality. Plaintiff's claims are typical of the claims of Members of
15 the Classes. Plaintiff and Members of the Classes were harmed by the same wrongful
16 conduct by Defendant in that they used Defendant's website and had their User Data
17 intercepted and disclosed to Facebook without Plaintiff's or Class Members'
18 knowledge, express written consent, or authorization. Plaintiff's claims are based on
19 the same legal theories as the claims of other Class Members.
20
21

22 97. Adequacy. Plaintiff will fairly and adequately protect and represent the
23 interests of the members of the Class. Plaintiff's interests are coincident with, and
24 not antagonistic to, those of the members of the Class. Plaintiff is represented by
25 counsel with experience in the prosecution of class action litigation generally and in
26 the emerging field of digital privacy litigation specifically.
27
28

1 98. Commonality. Questions of law and fact common to the Members of
2 the Classes predominate over questions that may affect only individual Members of
3 the Classes because Defendant has acted on grounds generally applicable to the
4 Classes. Such generally applicable conduct is inherent in Defendant's wrongful
5 conduct. Questions of law and fact common to the Classes include:
6

7 a) Whether Defendant had a duty to protect and refrain from
8 disclosing Plaintiff's and Class Members' User Data;
9

10 b) Whether Defendant knowingly intercepted and/or disclosed
11 Plaintiff and Class Members' User Data to Facebook;
12

13 c) Whether Defendant negligently maintained its records
14 containing Plaintiff and Class Members' User Data;
15

16 d) Whether Plaintiff and Class Members authorized or consented to
17 Defendant's disclosure of their User Data to Facebook;
18

19 e) Whether Defendant's acts and practices violated the CIPA;
20

21 f) Whether Defendant's acts and practices violated the CIMA;
22

23 g) Whether Defendant's actions violate Plaintiff's and Class
24 Members' privacy rights as provided by the California Constitution and the common
25 law;
26

27 h) Whether Defendant breached its contract with Plaintiff and Class
28 Members;
29

1 i) Whether Plaintiff and Class Members are entitled to equitable
2 relief, including but not limited to, injunctive relief, restitution, and disgorgement;
3 and

4
5 j) Whether Plaintiff and the Class Members are entitled to actual,
6 statutory, punitive or other forms of damages, and other monetary relief.

7
8 99. Superiority. Class action treatment is a superior method for the fair and
9 efficient adjudication of the controversy. Such treatment will permit a large number
10 of similarly situated persons to prosecute their common claims in a single forum
11 simultaneously, efficiently, and without the unnecessary duplication of evidence,
12 effort, or expense that numerous individual actions would engender. The benefits of
13 proceeding through the class mechanism, including providing injured persons or
14 entities a method for obtaining redress on claims that could not practicably be
15 pursued individually, substantially outweighs potential difficulties in management
16 of this class action. Plaintiff knows of no special difficulty to be encountered in
17 litigating this action that would preclude its maintenance as a class action.
18
19
20

21 100. Plaintiff reserves the right to revise the foregoing class allegations and
22 definitions based on facts learned and legal developments following additional
23 investigation, discovery, or otherwise.
24

25 **VIII. CLAIMS FOR RELIEF**

26 **FIRST CLAIM FOR RELIEF**

27 **Violation of the California Invasion of Privacy Act (“CIPA”)**

28 **Cal. Penal Code § 630, *et seq.***

(On Behalf of Plaintiff and the California Subclass)

1 101. Plaintiff incorporates paragraphs 1 through 100 by reference as if fully
2 set forth herein.
3

4 102. The CIPA was enacted to safeguard privacy from new technologies in
5 the ever-evolving digital age. The Act begins with its statement of purpose:
6

7 The Legislature hereby declares that advances in science and
8 technology have led to the development of new devices and techniques
9 for the purpose of eavesdropping upon private communications and that
10 the invasion of privacy resulting from the continual and increasing use
11 of such devices and techniques has created a serious threat to the free
exercise of personal liberties and cannot be tolerated in a free and
civilized society.”

12 Cal. Penal Code § 630.

13 103. To establish liability under Section 631(a), a plaintiff need only
14 establish that the Defendant, “by means of any machine, instrument, or contrivance,
15 or any other manner,” does any of the following:
16

17 *intentionally taps, or makes any unauthorized connection, whether*
18 *physically, electrically, acoustically, inductively, or otherwise, with*
19 *any telegraph or telephone wire, line, cable, or instrument, including*
20 *the wire, line, cable, or instrument of any internal telephonic*
communication system; or

21 *willfully and without the consent of all parties to the communication,*
22 *or in any unauthorized manner, reads, or attempts to read, or to learn*
23 *the contents or meaning of any message, report, or communication*
24 *while the same is in transit or passing over any wire, line, or cable, or*
is being sent from, or received at any place within this state; or

25 *uses, or attempts to use, in any manner, or for any purpose, or to*
26 *communicate in any way, any information so obtained, or who aids,*
27 *agrees with, employs, or conspires with any person or persons to*
28 *unlawfully do, or permit, or cause to be done any of the acts or things*
mentioned above in this section.

1 Cal. Penal Code § 631(a) (emphasis added).

2
3 104. Section 631(a) is not limited to phone lines, but also applies to “new
4 technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*,
5 No. 15-cv-4062-LHK, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA
6 applies to “new technologies” and must be construed broadly to effectuate its
7 remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, No. 06-cv- 5289-
8 WHA, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs
9 “electronic communications”); *In re Facebook, Inc. Internet Tracking Litigation*,
10 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy
11 claims based on Facebook’s collection of consumers’ internet browsing history).

12
13
14
15 105. To avoid liability under the CIPA, a Defendant must show it had the
16 consent of *all* parties to a confidential communication. Cal. Penal Code § 632.

17
18 106. As described in the statute, a “confidential communication” is “any
19 communication carried on in circumstances as may reasonably indicate that any
20 party to the communication desired it to be confided to the parties thereto[.]” *Id.*

21
22 107. Defendant aided, agreed with, employed, and conspired with Facebook
23 to track and intercept Plaintiff’s and Class Members’ internet communications while
24 accessing Defendant’s website—without their authorization and consent.

25
26 108. Defendant, in aiding and assisting Facebook’s eavesdropping of
27 Plaintiff and Class Members, intended to help Facebook learn or attempt to learn the
28 meaning of the contents of or record the confidential communications at issue.

1 109. The patient communication information that Defendant transmitted to
2 Facebook, through its Pixel, such as messages with healthcare providers,
3 appointment scheduling, constitutes protected health information.
4

5 110. As demonstrated herein, Defendant violated CIPA by aiding and
6 permitting third parties to receive its patients' online communication through its
7 website without their consent.
8

9 111. By disclosing Plaintiff's and the Class Members' User Data Defendant
10 violated Plaintiff's and Class Members' statutorily protected right to privacy.
11

12 112. As a result of the above violations, Defendant is liable to the Plaintiff
13 and Class Members for actual damages related to their loss of privacy in an amount
14 to be determined at trial or alternatively for "liquidated damages not less than \$2,500
15 per plaintiff." Pursuant to CIPA Section 637.2, any person who has been injured by
16 a violation of CIPA may recover \$5,000 dollars per violation or three times the
17 amount of actual damages (the greater of these two options). Additionally, Section
18 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant
19 to this section that the plaintiffs has suffered, or be threatened with, actual damages."
20
21

22 113. Under the CIPA, Defendant is also liable for reasonable attorney's fees,
23 and other litigation costs, injunctive and declaratory relief, and punitive damages in
24 an amount to be determined by a jury, but sufficient to prevent the same or similar
25 conduct by the Defendant in the future.
26

27
28 **SECOND CLAIM FOR RELIEF**

1 **Violation of the California Confidentiality of Medical Information Act**
2 **(“CMIA”)**
3 **Cal. Civ. Code §§ 56.10 & 56.35 – Disclosure of Medical Information**
4 **(On Behalf of Plaintiff and the California Subclass)**

5 114. Plaintiff incorporates the paragraphs 1 through 100 by reference as if
6 fully set forth herein.

7 115. Under the CMIA section 56.10, providers of health care are prohibited
8 from disclosing medical information relating to their patients, without a patient’s
9 authorization. Medical information refers to “any individually identifiable
10 information, in electronic or physical form, in possession of or derived from a
11 provider of health care . . . regarding a patient’s medical history, mental or physical
12 condition, or treatment. ‘Individually Identifiable’ means that the medical
13 information includes or contains any element of personal identifying information
14 sufficient to allow identification of the individual” Cal. Civ. Code § 56.05.
15

16 116. Defendant is deemed a provider of health care under Cal. Civ. Code.
17 Section 56.06, subdivision (a) and (b), because it “maintain[s] medical information”
18 of patients and makes it available for the “purposes of allowing its users to manage
19 his or her information” or for the diagnosis, treatment, or management of a medical
20 condition. Cal. Civ. Code. § 56.06.
21

22 117. Defendant is therefore subject to the requirements of the CMIA and
23 obligated under subdivision (b) to maintain the same standards of confidentiality
24 required of a provider of health care with respect to medical information that it
25 maintains on behalf of patients.
26
27
28

1 118. Plaintiff and Class Members are patients, and, as a health care provider,
2 Defendant has an ongoing obligation to comply with the CMIA's requirements.

3 119. As described herein, Facebook ID is an identifier sufficient to allow
4 identification of a specific individual. Along with patients' Facebook ID, Defendant
5 discloses to Facebook—without first obtaining authorization—several pieces of
6 information regarding its patients' use of its website, which includes, but is not
7 limited to: patient medical records, medical conditions, medical concerns, treatment
8 patients are seeking, email address, address, telephone number, etc. As a result,
9 Defendant violated Civil Code section 56.10, subdivision (a).
10
11

12 120. This patient information is derived from a provider of healthcare
13 regarding patients' medical treatment and physical condition. Accordingly, it
14 constitutes medical information pursuant to the CMIA.
15
16

17 121. As demonstrated herein, Defendant failed to obtain its patients'
18 authorization for the disclosure of medical information and failed to disclose in its
19 Privacy Policy that it shares protected health information for marketing purposes.
20

21 122. Pursuant to CMIA section 56.11, a valid authorization for disclosure of
22 medical information must, *inter alia*, be (1) "clearly separate from any other
23 language present on the same page and is executed by a signature which serves no
24 other purpose than to execute the authorization" (2) signed and dated by the patient
25 or their representative (3) state the name and function of the third party that receives
26 the information (4) state a specific date after which the authorization expires.
27
28

1 Accordingly, the information set forth in Defendant’s Privacy Policy does not
2 qualify as valid authorization.

3 123. Defendant knowingly and willfully disclosed medical information
4 without consent to Facebook for financial gain. Specifically, to market and advertise
5 its services, or to allow others to market and advertise their services, in violation of
6 Civil Code section 56.06 subdivisions (b) and (c).
7

8
9 124. California Civil Code § 56.35 provides that a patient who has sustained
10 economic loss or personal injury resulting from the disclosure of his or her
11 individually identifiable medical information, in violation of California Code §
12 56.10, may recover compensatory damages, punitive damages not to exceed \$3,000,
13 attorneys’ fees, and costs of litigation. Accordingly, Plaintiff and Class Members are
14 entitled to: (1) actual damages, in an amount to be determined at trial; (2) punitive
15 damages; and (3) attorneys’ fees and other litigation costs reasonably incurred.
16
17

18 **THIRD CLAIM FOR RELIEF**

19 **Violation of the California Confidentiality of Medical Information Act
20 (“CMIA”)**

21 **Cal. Civ. Code §§ 56.101 & 56.36 – Negligent Preservation of Medical Records
22 (On Behalf of Plaintiff and the California Subclass)**

23 125. Plaintiff incorporates the paragraphs 1 through 100 by reference as if
24 fully set forth herein.

25 126. The CMIA requires that every provider of health care who “creates,
26 maintains, preserves, stores, abandons, destroys, or disposes of medical information
27
28

1 shall do so in a manner that preserves the confidentiality of the information contained
2 therein.” Cal. Civ. Code § 56.101.

3 127. Any healthcare provider who “negligently creates, maintains,
4 preserves, stores, abandons, destroys, or disposes of medical information shall be
5 subject to the remedies and penalties provided under subdivisions (b) and (c) of
6 Section 56.36.”
7

8
9 128. Defendant failed to maintain, preserve, and store medical information
10 in a manner that preserves the confidentiality of the information contained therein
11 because it disclosed Plaintiff’s and Class Members’ sensitive medical information
12 without consent, including information concerning their medical condition,
13 diagnoses, treatment, appointment information, as well as personally identifiable
14 patient information, such as patients’ FID.
15

16
17 129. Defendant’s failure to maintain, preserve, and store medical
18 information in a manner that preserves the confidentiality of the information was, at
19 the least, negligent and violates California Civil Code section 56.06 subdivisions (b)
20 and (c).
21

22 130. Accordingly, Plaintiff and Class Members are entitled to the penalties
23 and remedies provided under subdivisions (b) and (c) of Section 56.35, including (1)
24 nominal damages of \$1,000 per violation; (2) actual damages, in an amount to be
25 determined at trial; and (3) reasonable attorneys’ fees and other litigation costs
26 reasonably incurred.
27
28

FOURTH CLAIM FOR RELIEF

**Invasion of Privacy Under the California Constitution and Common Law
(On Behalf of Plaintiff and the California Subclass)**

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

131. Plaintiff incorporates paragraphs 1 through 100 by reference as if fully set forth herein.

132. Plaintiff and Class Members have a legally protected privacy interest in the User Data that they enter into Defendant's Website and are entitled to the protection of their information and property against unauthorized access.

133. For reasons detailed above, Plaintiff and Class Members reasonably expected that their User Data would be protected and secure from unauthorized parties, and that it would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

134. Defendant unlawfully invaded the privacy rights of Plaintiff and Class Members by: (a) disclosing their private, and personal information to unauthorized parties in a manner that is highly offensive to a reasonable person; and (b) disclosing their private and personal information to unauthorized parties without the informed and clear consent of Plaintiff and Class Members, including but not limited to including the Facebook Pixel and other tracking code on its website that transfer information entered and records of actions taken by patients on Defendant's website to unrelated entities. This invasion into the privacy interest and seclusion of Plaintiff and Class Members is serious and substantial.

1 135. In willfully sharing Plaintiff's and Class Members' Personal
2 Information, Defendant acted in reckless disregard of their privacy rights.

3 136. Defendant violated Plaintiff's and Class Members' right to privacy
4 under California law, including, but not limited to California common law and
5 Article 1, Section 1 of the California Constitution and the California Consumer
6 Privacy Act.
7

8 137. As a direct and proximate result of Defendant's unlawful invasions of
9 privacy, Plaintiff's and Class Members' private, personal, and confidential
10 information has been accessed or is at imminent risk of being accessed, and their
11 reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff
12 and proposed Class Members have suffered injuries as a result of Defendant's
13 unlawful invasions of privacy and are entitled to appropriate relief.
14

15 138. Plaintiff and Class Members are entitled to injunctive relief as well as
16 actual damages, punitive damages, and damages for invasion of their privacy rights
17 in an amount to be determined by a jury without reference to specific economic
18 harm.
19
20
21

22 **FIFTH CLAIM FOR RELIEF**
23 **Breach of Contract**
24 **(On Behalf of Plaintiff and the Classes)**

25 139. Plaintiff incorporates the paragraphs 1 through 100 by reference as if
26 fully set forth herein.
27
28

1 140. As shown above, Defendant expressly promised to safeguard Plaintiff's
2 and Class Members' User Data, including their sensitive medical information, and
3 to not disclose that data to third parties without their consent.
4

5 141. In addition to the express contract provisions set forth above, implied
6 contracts existed between Defendant and Plaintiff that Defendant would not conspire
7 with others to violate Plaintiff's legal rights to privacy in their User Data.
8

9 142. Plaintiff and Class Members accepted Defendant's promises not to
10 disclose their User Data without explicit consent and/or authorization when they
11 entered into a contract with Defendant.
12

13 143. Plaintiff and Class Members fully performed their obligations under
14 their contract with Defendant, including by providing their User Data and paying for
15 medical services and/or treatment.
16

17 144. Defendant did not hold up its end of the bargain. Defendant secretly
18 disclosed Plaintiff and Class Members' User Data, including sensitive medical
19 information, to Facebook, without consent in violation of their agreement with
20 Plaintiff and Class Members.
21

22 145. Plaintiff and Class Members would not have entrusted Defendant with
23 their User Data in the absence of a contract between them and Defendant's express
24 promise not to disclose this information.
25

26 146. As a direct and proximate result of Defendant's breach of their contract,
27 Plaintiff and Class Members sustained damages as alleged herein. Plaintiff and Class
28

1 Members would not have used Defendant's services, or would have paid
2 substantially less for these services, had they known their User Data would be
3 disclosed.

4
5 147. Plaintiff and Class Members are entitled to the following damages: (a)
6 nominal damages for breach of contract; (b) general damages for invasion of their
7 privacy rights without reference to specific economic harm; (c) compensatory or
8 consequential damages caused by (i) the fact that sensitive and confidential health
9 and personal information that Plaintiffs and Class Members intended to keep private
10 are no longer private; (ii) Defendant's erosion of the essential confidential nature of
11 the patient-provider relationship; and (iii) the thing of value taken from Plaintiff and
12 Class Members, and benefits derived therefrom, without Plaintiff and Class
13 Members' knowledge or informed consent and without sharing the benefit of such
14 value.
15
16
17

18 **SIXTH CLAIM FOR RELIEF**
19 **Unjust Enrichment**
20 **(In the Alternative)**
21 **(On Behalf of Plaintiff and the Classes)**

22 148. Plaintiff incorporates the paragraphs 1 through 100 by reference as if
23 fully set forth herein.

24 149. Plaintiff and Class members conferred a benefit upon Defendant in the
25 form of valuable sensitive medical information that Defendant collected from
26 Plaintiff and Class members under the guise of keeping this information private.
27 Defendant collected and used this information for its own gain, including
28

1 advertisement purposes or sale. Additionally, Plaintiff and Class members
2 conferred a benefit upon Defendant in the form of monetary compensation.

3 150. Plaintiff and Class members would not have used Defendant's services,
4 or would have paid less for these services, if they had known Defendant would
5 use and disclose this information.
6

7 151. Defendant unjustly retained those benefits at the expense of Plaintiff
8 and Class members because Defendant's conduct damaged Plaintiff and Class
9 members, all without providing any commensurate compensation to Plaintiff and
10 Class members.
11

12 152. The benefits that Defendant derived from Plaintiff and Class
13 members rightly belong to Plaintiff and Class members. It would be inequitable
14 under unjust enrichment principles in California and every other state for Defendant
15 to be permitted to retain any of the profit or other benefits they derived from the
16 unfair and unconscionable methods, acts, and trade practices alleged in this
17 Complaint.
18
19

20 153. Defendant should be compelled to disgorge in a common fund for the
21 benefit of Plaintiff and Class members all unlawful or inequitable proceeds that
22 Defendant received, and such other relief as the Court may deem just and proper.
23
24

25 **IX. RELIEF REQUESTED**

26 154. Accordingly, Plaintiff, on behalf of herself and the proposed Classes,
27 respectfully requests that this Court:
28

1 a) Determine that this action may be maintained as a class action
2 pursuant to Rules 23(a), and (b)(3) of the Federal Rules of Civil Procedure, direct
3 that reasonable notice of this action, as provided by Rule 23(c)(2), be given to the
4 Classes, and declare Plaintiff as the representative of the Classes and her counsel as
5 Class Counsel;
6

7 b) Declare that Defendant's conduct, as set out above, violates the
8 laws cited herein;
9

10 c) Award damages, including nominal, statutory, and punitive
11 damages where applicable, to Plaintiff and the Classes in an amount to be determined
12 at trial;
13

14 d) Award Plaintiff and the Classes their reasonably litigation
15 expenses and attorneys' fees;
16

17 e) Awarding Plaintiff and the Classes pre-and post-judgment
18 interest, to the extent allowable;
19

20 f) Awarding such other further injunctive and declaratory relief
21 as is necessary to protect the interests of Plaintiff and the Classes; and
22

23 g) Awarding such other and further relief as the Court deems
24 reasonable and just.
25
26
27
28

JURY DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff, on behalf of herself and the proposed Class, demands a trial by jury on all issues so triable.

Dated: March 23, 2023

Respectfully submitted,

EDELSBERG LAW, P.A.

/s/ Scott Edelsberg, Esq.

Scott Edelsberg, Esq.

CA Bar No. 330090

scott@edelsberglaw.com

1925 Century Park East, Suite 1700

Los Angeles, CA 90067

Tel: 305-975-3320

Counsel for Plaintiff and the Proposed Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [RadNet Secretly Discloses Patient Health Information to Facebook, Class Action Claims](#)
