

CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Bryan P. Thompson (SBN 354683)
bthompson@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

SIMMONS HANLY CONROY LLP
Jason “Jay” Barnes (*Pro Hac Vice*)
jaybarnes@simmonsfirm.com
Eric S. Johnson (*Pro Hac Vice*)
ejohnson@simmonsfirm.com
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel: (212) 784-6400

**AHMAD, ZAVITSANOS,
& MENSING, PLLC**
Foster C. Johnson (SBN 289055)
fjohnson@azalaw.com
David Warden (*Pro Hac Vice*)
dwarden@azalaw.com
Nathan Campbell (*Pro Hac Vice*)
ncampbell@azalaw.com
1221 McKinney Street, Suite 3460
Houston, TX 77010
Tel: (713) 655-1101

Counsel for Plaintiffs and the Proposed Classes

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF MARIN

JOHN DOE I, JOHN DOE II, and JOHN
DOE III, individually, and on behalf of all
others similarly situated,

Plaintiffs,

vs.

MARINHEALTH MEDICAL CENTER

Defendant.

ELECTRONICALLY FILED
Superior Court of California
County of Marin
02/26/2025

James M. Kim, Clerk of the Court
By: N. Johnson, Deputy

ALMEIDA LAW GROUP LLC
Matthew J. Langley (SBN 342846)
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (773) 554-9354
matt@almeidawgroup.com

KIESEL LAW LLP
Jeffrey A. Koncius (SBN 189803)
koncius@kiesel.law
Nicole Ramirez Jones (SBN 279017)
ramirezjones@kiesel.law
Kaitlyn E. Fry (SBN 350768)
fry@kiesel.law
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel: (310) 854-4444

Case No.: CV0002218

*[Assigned for All Purposes to Hon. Stephen P.
Freccero in Courtroom A]*

**FIRST AMENDED CLASS ACTION
COMPLAINT FOR:**

- 1. VIOLATION OF CALIFORNIA
CONFIDENTIALITY OF MEDICAL
INFORMATION ACT, CAL. CIV.
CODE SECTION 56, et seq.**

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

- 2. VIOLATION OF CALIFORNIA
INVASION OF PRIVACY ACT,
CAL. PENAL CODE SECTION 630,
et seq.

- 3. VIOLATION OF CALIFORNIA
UNFAIR COMPETITION LAW,
CAL. BUS. & PROF. CODE
SECTION 17200, *et seq.*

- 4. INVASION OF PRIVACY UNDER
CALIFORNIA CONSTITUTION

- 5. INVASION OF PRIVACY -
INTRUSION UPON SECLUSION

- 6. BREACH OF IMPLIED
CONTRACT

- 7. LARCENY/RECEIPT OF STOLEN
PROPERTY, VIOLATION OF
CALIFORNIA PENAL CODE
SECTION 496(a) and (c)

- 8. QUASI-CONTRACT/
RESTITUTION/ UNJUST
ENRICHMENT

- 9. VIOLATION OF THE
COMPREHENSIVE COMPUTER
DATA ACCESS AND FRAUD ACT,
CAL. PENAL CODE SECTION 502;

- 10. VIOLATION OF CAL. CIVIL CODE
SECTION 1798.82; and

- 11. VIOLATIONS OF CAL. CIVIL
CODE SECTIONS 1709 and 1710

DEMAND FOR JURY TRIAL

Complaint Filed: March 7, 2024
Trial Date: None

1 Plaintiffs, individually and on behalf of all other California citizens similarly situated, bring
2 this action against Defendant MarinHealth Medical Center (“**Defendant**” or “**Marin**”).

3 Plaintiffs’ allegations are based upon personal knowledge as to Plaintiffs’ own acts, and
4 upon information and belief as to all other matters based on the investigation conducted by and
5 through Plaintiffs’ attorneys. Plaintiffs believe that substantial additional evidentiary support will
6 exist for the allegations set forth herein, after a reasonable opportunity for discovery.

7 INTRODUCTION

8 1. Defendant MarinHealth Medical Center is a full-service hospital comprised of expert
9 clinicians and physicians who practice at Marin clinics, including more than one hundred fifty (150)
10 providers in twenty (20) locations throughout Northern California.¹

11 2. Defendant has disregarded the privacy rights of millions of visitors to and users of its
12 websites (“**Users**” or “**Class Members**”) by intentionally, willfully, recklessly and/or negligently
13 failing to implement adequate and reasonable measures to ensure that that Users’ personally
14 identifiable information (“**PII**”) and protected health information (“**PHI**”) (collectively, “**Private**
15 **Information**”) was safeguarded. Instead, Defendant allowed unauthorized third parties, including
16 Meta Platforms, Inc. d/b/a Facebook (“**Facebook**”) to intercept Users’ clicks, communications on,
17 and visits of Defendant’s websites, including <https://www.mymarinhealth.org/> (the “**Site**”) and
18 <https://www.mymarinhealth.org/mychart> (the “**Portal**”) (collectively, the “**Websites**”).

19 3. Unbeknownst to Users and without Users’ authorization or informed consent,
20 Defendant installed Facebook’s Meta Pixel (“**Meta Pixel**” or “**Pixel**”) and other third-party tracking
21 technology, in its Websites in order to intercept and send Private Information to third parties such
22 as Facebook and/or Google LLC.

23 4. These Pixels collect Users’ confidential and private PHI—including but not limited
24 to details about their medical conditions, treatments and providers sought, and appointments—and
25 send it to Facebook without prior, informed consent. These Pixels are snippets of code that track
26 Users as they navigate through a website—logging which pages they visit, each button they click,
27

28 ¹*Marin Health Medical Network*, MARIN HEALTH, <https://www.mymarinhealth.org/career-opportunities/marinhealth-medical-network/> (last visited Aug. 8, 2023).

1 and what information they provide in online forms. More specifically, the Meta Pixel sends
2 information to Facebook via scripts running in a person's internet browser so each data packet
3 comes labeled with a specific internet protocol ("**IP**") address that can be used in combination with
4 other data to identify an individual or household. Additionally, if the person has an active Facebook
5 account, the IP address is paired with their personal unique Facebook ID ("**FID**"), which Facebook
6 uses to identify that individual.

7 5. Plaintiffs and Class Members who visited and used Defendant's Websites
8 understandably thought they were communicating with only their trusted healthcare providers, and
9 reasonably believed that their sensitive and private PHI would be guarded with the utmost care. In
10 browsing Defendant's Websites – be it to make an appointment, locate a doctor with a specific
11 specialty, find sensitive information about their diagnosis, or investigate treatment for their
12 diagnosis – Plaintiffs and Class Members did not expect that every search (including exact words
13 and phrases they typed into Defendant's website search bars), page visit, or even their
14 access/interactions on Defendant's online portals would be intercepted, captured, or otherwise
15 shared with Facebook in order to target Plaintiffs and Class Members, in conscious disregard of
16 their privacy rights.

17 6. Defendant encouraged Plaintiffs and Class Members to access and use various digital
18 tools via its Websites to, among other things, receive healthcare services, to gain additional insights
19 into its Users, improve its return on marketing dollars and, ultimately, increase its revenue.

20 7. In exchange for installing the Pixels, Facebook provides Defendant with analytics
21 about the advertisements they have placed as well as tools to target people who have visited
22 Defendant's Websites.

23 8. While the information captured and disclosed without permission may vary depending
24 on the Pixel(s) embedded, these "data packets" can be extensive, transmitting, for example, not just
25 the name of the physician and her field of medicine, but also the first name, last name, email address,
26 phone number, zip code, and city of residence entered in the booking form. That data is linked to a
27 specific IP address. The amalgamation of these data points and unique identifying information
28 results in an egregious, unauthorized dissemination of highly sensitive Private Information unique

1 to each individual User.

2 9. The Meta Pixel can track and log each page a user visits, what buttons they click, as
3 well as specific information they input into a website. In addition, if the person is (or recently has)
4 logged into Facebook when they visit a particular website when a Meta Pixel is installed, some
5 browsers will attach third-party cookies—another tracking mechanism—that allow Facebook to link
6 Pixel data to specific Facebook accounts.

7 10. Alarming, the use of Meta Pixels on Defendant's Websites tracks extremely
8 sensitive PHI such as health conditions (e.g., diabetes), diagnoses (e.g., COVID-19 or breast
9 cancer), procedures, test results, treatment status, the treating physician, allergies, and PII.

10 11. Plaintiffs had their Private Information, including sensitive medical information,
11 harvested by Facebook through the Meta Pixel tracking tool without their consent when they entered
12 their information into Defendant's Websites, and continued to have their privacy violated when his
13 Private Information was used to turn a profit by way of targeted advertising related to his respective
14 medical conditions and treatments sought.

15 12. Defendant knew that by embedding the Meta Pixel—a proprietary tracking and
16 advertising tool developed by Facebook—on its Websites, it was permitting Facebook to collect
17 and use Plaintiffs' and Class Members' Private Information, including sensitive medical
18 information.

19 13. Defendant (or any third parties) did not obtain Plaintiffs' and Class Members' prior
20 consent before sharing their sensitive, confidential communications and Private Information with
21 third parties such as Facebook.

22 14. Defendant's actions constitute an extreme invasion of Plaintiffs' and Class Members'
23 right to privacy and violate federal and state statutory and common law as well as Defendant's own
24 Privacy Policies that affirmatively and unequivocally state that any personal information provided
25 to Defendant will remain secure and protected.²

26
27 ² Marin's Privacy Policies (and other affirmative representations) represent to Users that it will not
28 share Private Information for marketing purposes unless patients provide written permission. *See*
<https://www.mymarinhealth.org/privacy-policy/> (last visited Aug. 4, 2023).

16. Plaintiff seeks, on behalf of himself and a class of similarly situated persons, to remedy these harms and therefore assert the following statutory and common law claims against Defendant: (i) Violation of the California Confidentiality of Medical Information Act (“**CMIA**”), Cal. Civ. Code § 56, *et seq.*; (ii) Violation of the California Invasion of Privacy Act (“**CIPA**”), Cal. Penal Code § 630, *et seq.*; Violation of the California Wiretapping Laws, Cal. Penal Code § 631, *et seq.*; (iii) Violation of California’s Unfair Competition Law (“**UCL**”), Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful and Unfair Business Practices; (iv) Invasion of Privacy under the California Constitution; (v) Common Law Invasion of Privacy; (vi) Common Law Breach of Implied Contract; (vii) Violation of California Penal Code § 496, *et seq.*; (viii) Quasi-Contract/Restitution/Unjust Enrichment; (ix) Violation of the Comprehensive Computer Data Access and Fraud Act (“**CDAFA**”), Cal. Penal Code § 502; (x) Violation of Cal. Civil Code § 1798.82; and (xi) Violations of Cal. Civil Code §§ 1709, 1710.

17. Plaintiff John Doe I is and at all relevant times was, a resident of Marin County, California.

3 20. Defendant MarinHealth Medical Center is a full-service hospital, located at 250 Bon
4 Air, Road, Greenbrae, CA 94904, comprised of expert clinicians and physicians who practice at
5 Marin clinics, including more than one hundred fifty (150) providers in twenty (20) locations
6 throughout Northern California.

21. This Court has jurisdiction over Defendant because it regularly conducts business in California, including in Marin County, and has its principal place of business in California.

22. Venue is appropriate in this Court because the injuries giving rise to the alleged causes of action occurred in Marin County, and because Plaintiffs resided in Marin County at the time the offer of services for personal use was made by Defendant. *See* Cal. Civ. Code §§ 395(a) & 395 (b). Venue is also appropriate in this Court because Marin County is the county in which the cause, or some part of the cause, arose for the recovery of a penalty imposed by statute. *See* Cal. Civ. Code § 393(a).

23. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to surreptitiously capture and to disclose their Users' Private Information. Specifically, and for example, The Markup reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person

27 ³ Plaintiff John Doe III, newly added into this amended complaint, is Plaintiff C.M. from *C.M. v.*
28 *Marinhealth Medical Group, Inc. et al*, Case No. 3:23-cv-04179-WHO (N.D. Cal.) The *C.M.* action
has been subsumed into this state action.

1 clicked a button to schedule a doctor's appointment.⁴ Estimates are that over 664 hospital systems
2 and providers utilize some form of tracking technology on their digital properties.⁵

3 24. Entities collecting and disclosing Users' Private Information face significant legal
4 exposure under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which
5 applies specifically to healthcare providers, health insurance providers and healthcare data
6 clearinghouses.⁶

7 25. The HIPAA privacy rule sets forth policies to protect all individually identifiable
8 health information that is held or transmitted.⁷ This is information that can be used to identify,
9 contact, or locate a single person or can be used with other sources to identify a single individual.
10 When PII is used in conjunction with one's physical or mental health or condition, health care, or
11 one's payment for that health care, it becomes PHI.

12 26. The unilateral disclosure of such Private Information is unquestionably a violation of
13 HIPAA, among other statutory and common laws. And, while some hospitals and other disclosing
14 entities attempt to seek refuge in the argument that these third parties allegedly do not store this
15 Private Information, that argument is unavailing as the violation lies in the unlawful transmission
16 of that data. As the Office for Civil Rights ("OCR") at the U.S. Department of Health and Human
17 Services ("HHS") reminded entities regulated under HIPAA in its recently issued *Use of Online*
18 *Tracking Technologies by HIPAA Covered Entities and Business Associates* bulletin:

19
20 ⁴ Todd Feathers, *et al.*, *Facebook Is Receiving Sensitive Medical Information from Hospital*
21 *Websites*, THE MARKUP (June 16, 2022), <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> (last visited Aug. 4, 2023).

22 ⁵ Dave Muoio & Annie Burky, *Advocate Aurora, WakeMed get served class action over Meta's*
23 *alleged patient data mining*, FIERCE HEALTHCARE (November 4, 2022),
24 <https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook> (last visited Aug. 4, 2023).

25 ⁶ Alfred Ng & Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids'*
26 *Information to Facebook*, THE MARKUP (June 21, 2022), <https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook>
27 (stating that "[w]hen you are going to a covered entity's website, and you're entering information
28 related to scheduling an appointment, including your actual name, and potentially other identifying
characteristics related to your medical condition, there's a strong possibility that HIPAA is going to
apply in those situations") (last visited Aug. 4, 2023).

⁷ The HIPAA Privacy Rule protects all electronically protected health information a covered entity
like Defendant "create, receive, maintain, or transmit" in electronic form. *See* 45 C.F.R. § 160.103.

*Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.*⁸

OCR makes it clear that information that is routinely collected by vendors on public-facing websites, apps and web-based assets may be PHI as well, including unique identifiers such as IP addresses, device IDs, or email addresses.⁹

Defendant's Method of Transmitting Plaintiffs' & Class Members' Private Information via the Meta Pixel.

27. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser and Microsoft's Edge browser).

28. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via web browsers.

29. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web

⁸ *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH AND HUM. SERVICES, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited Aug. 4, 2023) (emphasis added).

⁹ *See id.*; see also Mason Fitch, *HHS Bulletin Raises HIPAA Risks for Online Tracking Vendors*, LAW360 (December 13, 2022), <https://www.law360.com/articles/1557792/hhs-bulletin-raises-hipaa-risks-for-online-tracking-vendors?copied=1> (last visited Aug. 4, 2023).

address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.¹⁰

- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are “third-party cookies” which means they can store and communicate data when visiting one website to an entirely different website.¹¹
- **HTTP Response**: an electronic communication that is sent as a reply to the client device’s web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.¹²

30. A patient’s HTTP Request essentially asks the Defendant’s Website to retrieve certain information (such as a physician’s “Book an Appointment” page), and the HTTP Response renders or loads the requested information in the form of “Markup” (the pages, images, words, buttons, and other features that appear on the patient’s screen as they navigate Defendant’s Website).

31. Every website is comprised of Markup and “Source Code.” Source Code is a set of instructions that commands the website visitor’s browser to take certain actions when the web page first loads or when a specified event triggers the code.

32. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser’s User. The Pixel incorporated by Defendant uses Source Code that does just that. The Pixel acts much like a traditional wiretap.

¹⁰ *An overview of HTTP*, MDN WEB DOCS, <https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview> (last visited Aug. 4, 2023).

¹¹ *HTTP cookies*, MDN WEB DOCS, <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies> (last visited Aug. 4, 2023).

¹² *An overview of HTTP*, *supra* note 13. One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses. *HTTP Messages*, MDN WEB DOCS, <https://developer.mozilla.org/en-US/docs/Web/HTTP/Messages> (last visited Aug. 4, 2023).

33. When patients visit Defendant’s Websites via an HTTP Request to Defendant’s server, that server sends an HTTP Response including the Markup that displays the Webpage visible to the User and Source Code, including Defendant’s Pixel.

34. Thus, Defendant is, in essence, handing patients a tapped device and once the Webpage is loaded into the User’s browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications—intended only for Defendant—and transmits those communications to third parties, including Facebook. Such conduct occurs on a continuous, and not sporadic, basis.

35. Third parties, like Facebook, place third-party cookies in the web browsers of Users logged into their services.

36. These cookies uniquely identify the User and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the Private Information intercepted.

37. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that cannot be evaded by savvy users.

38. Facebook’s workaround, for example, is called CAPI, which is an “effective” workaround because it does not intercept data communicated from the User’s browser. Instead, CAPI “is designed to create a direct connection between [Web hosts’] marketing data and [Facebook].”¹³

39. Thus, the communications between patients and Defendant, which are necessary to use Defendant’s Websites, are actually received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook.

40. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

¹³ Michael Mata, *Stop Data Loss with Facebook Server-Side Tracking*, MADGICX (March 18, 2022), <https://madgicx.com/blog/facebook-server-side-tracking> (last visited Aug. 4, 2023).

41. While there is no way to confirm with certainty that a Web host like Defendant have implemented workarounds like CAPI without access to the host server, companies like Facebook instruct Defendant to “[u]se the CAPI in addition to the [] Pixel, and share the same events using both tools,” because such a “redundant event setup” allows Defendant “to share website events [with Facebook] that the pixel may lose.”¹⁴

42. The third parties to whom a website transmits data through Pixels and associated workarounds do not provide any substantive content relating to the User’s communications. Instead, these third parties are typically procured to track User data and communications for marketing purposes of the website owner (i.e., to bolster profits).

43. Thus, without any knowledge, authorization, or action by a User, website owners like Defendant can use its source code to commandeer the User’s computing device, causing the device to contemporaneously and invisibly redirect the Users’ communications to third parties.

44. In this case, Defendant employed the Tracking Pixel and CAPI to intercept, duplicate and re-direct Plaintiffs’ and Class Members’ Private Information to Facebook.

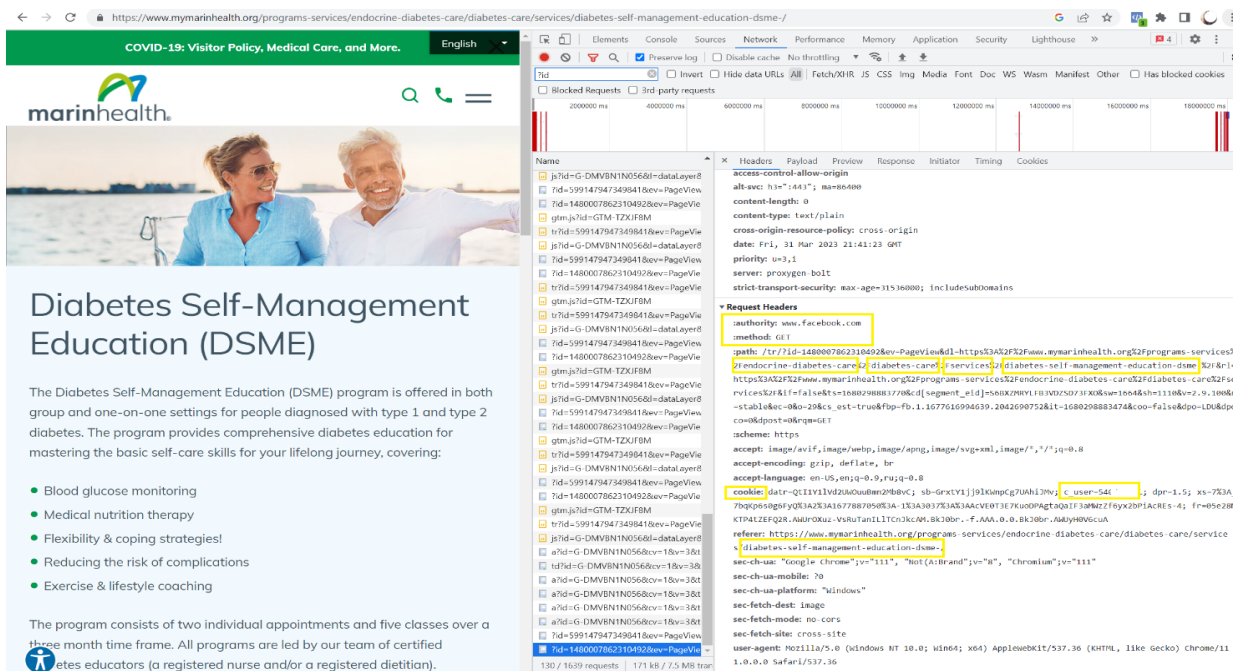
45. By way of example, Marin shared with third parties Plaintiffs’ and Class Members’ patient status, their medical conditions, the type of medical treatment or provider sought, names of specific providers, and the fact that the individual attempted to or did book a medical appointment. This Private Information was shared at the same time as certain HIPPA identifiers including patient’s IP address, and along with their unique Facebook ID. Such information was shared without a patient’s express consent even though it allows a third party (e.g., Facebook) to know that a specific patient was or is being treated for a specific type of medical condition.

46. For example, if a patient with diabetes researched their type of diabetes or looked up available care options when visiting www.mymarinhealth.org, including “Diabetes Self-management Education” program provided by Defendant, that information would have been shared with Facebook along with unique identifiers including the patient’s Facebook ID. Someone seeking gender-affirming surgery would have had their sensitive and private information shared in the same

¹⁴See *Best Practices for Conversions API*, META, <https://www.facebook.com/business/help/308855623839366?id=818859032317965> (last visited Aug. 4, 2023).

manner (see **Figure 1** below).

Figure 1: Image from <https://www.mymarinhealth.org/programs-services/endocrine-diabetes-care/diabetes-care/services/diabetes-self-management-education-dsme/>.



47. The patient visiting this particular web page only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses. In reality, Defendant's Source Code and underlying HTTP Requests and Responses share the patient's personal information with Facebook, including the fact that the patient is looking for treatment for his Diabetes diagnosis along with the patient's unique Facebook identifiers.

48. Defendant provides an option to click a dedicated phone number to call its specialized programs for patients, including the Diabetes Self-Management Education program, to learn more or enroll. If a User diagnosed with diabetes clicks on the phone button, this information, including the name of the program and the phone number clicked, is also shared with Facebook, via the "SubscribedButtonClicked" event (see **Figure 2** below)¹⁵:

¹⁵ The image in Figure 2 was taken from <https://www.mymarinhealth.org/programs-services/endocrine-diabetes-care/diabetes-care/services/diabetes-self-management-education-dsme/> after a User of Defendant's Website clicked the phone number for the Diabetes Self-Management Education Program.

1 52. This occurs because the Pixel embedded in Defendant's Source Code is programmed
2 to automatically track and transmit a patient's communications, and this occurs contemporaneously,
3 invisibly, and without the patient's knowledge.

4 53. Thus, without Users' consent, Defendant effectively uses this Source Code to
5 commandeer patients' computing devices, thereby re-directing their Private Information to
6 unauthorized third parties.

7 54. The information that Defendant's Pixel sends to Facebook may include, among other
8 things, patients' PII, PHI, and other confidential information.

9 55. Consequently, when Plaintiffs and Class Members visit Defendant's Websites and
10 communicate their Private Information, it is transmitted to Facebook, including, but not limited to,
11 patient status, health conditions experienced and treatments sought, physician selected,
12 appointments sought, specific button/menu selections, sensitive demographic information such as
13 sexual orientation, and exact words and phrases typed into the search bar. Additionally, this includes
14 instances when patients pay a bill, self-enroll in the patient portal, or access their portal via a
15 designated button (or link) on the website. Each of these activities involves the transmission of
16 sensitive information—such as payment details, personal identifiers required for portal enrollment,
17 and portal usage data—which is inevitably communicated to Facebook.

18 ***Defendant's Pixel Tracking Practices caused Plaintiffs' and Class Members' Private Information***
19 ***to be sent to Facebook.***

20 56. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel
21 and/or CAPI on its Websites to secretly track patients by recording their activity and experiences in
22 violation of its common law, contractual, statutory, and regulatory duties, and obligations.

23 57. Defendant's web pages contain a unique identifier which indicates that the Pixel is
24 being used on a particular webpage.

25 58. The Pixels allow Defendant to optimize the delivery of advertisements, measure
26 cross-device conversions, create custom audiences, and decrease advertising and marketing costs.

27 59. However, Defendant's Websites do not rely on the Pixel to function.
28

1 60. While seeking and using Defendant's services as a medical provider, Plaintiffs and
2 Class Members communicated their Private Information to Defendant via its Websites.

3 61. Defendant did not disclose to Plaintiffs and Class Members that their Private
4 Information would be shared with Facebook as it was communicated to Defendant. Rather,
5 Defendant represented the opposite. This prevents the provision of any informed consent by
6 Plaintiffs or Class Members to Defendant for the challenged conduct described herein.

7 62. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise
8 permitted Defendant to disclose their Private Information to Facebook (or any other third-party),
9 nor did they intend for Facebook to be a party to their communications with Defendant. Defendant
10 did not employ any form or click system whereby Plaintiffs and Class Members provide their
11 affirmative consent to Defendant agreeing, authorizing, or otherwise permitting Defendant to
12 disclose their Private Information to Facebook (or any other third-party).

13 63. Defendant's Pixels and CAPI sent sensitive Private Information to Facebook,
14 including but not limited to Plaintiffs' and Class Members': (i) status as medical patients; (ii) health
15 conditions; (iii) sought treatment or therapies; (iv) terms and phrases entered into Defendant's
16 search bar; (v) sought providers and their specialties; (vi) selected locations or facilities for
17 treatment; and (vii) web pages viewed.

18 64. Importantly, the Private Information Defendant's Pixels sent to Facebook was sent
19 alongside Plaintiffs' and Class Members' personal identifiers, including patients' IP address and
20 cookie values thereby allowing individual patients' communications with Defendant, and the
21 Private Information contained in those communications, to be linked to their unique Facebook
22 accounts.

23 65. IP addresses are used to identify and route communications on the internet. IP
24 addresses of individual users are used by internet service providers, websites, and tracking
25 companies to facilitate and track internet communications and content. IP addresses also offer
26
27
28

1 advertising companies like Facebook a unique and semi-persistent identifier across devices—one
2 that has limited privacy controls.¹⁸

3 66. Because of their uniquely identifying character, IP addresses are considered protected
4 personally identifiable information. 45 CFR § 164.514. Tracking pixels can (and typically do)
5 collect website visitors' IP addresses.

6 67. HIPAA further provides that information is personally identifiable where the covered
7 entity has “actual knowledge that the information could be used alone or in combination with other
8 information to identify an individual who is a subject of the information.” 45 C.F.R. §
9 164.514(2)(ii); *see also*, 45 C.F.R. § 164.514(b)(2)(i)(O

10 68. Through the Source Code deployed by Defendant, the cookies that they use to help
11 Facebook identify patients include but are not necessarily limited to cookies named: “c_user,”
12 “datr,” “fr,” and “fbp.”¹⁹

13 69. The “c_user” cookie or FID is a type of third-party cookie assigned to each person
14 who has a Facebook account, and it is composed of a unique and persistent set of numbers. Cookies
15 are considered personal identifiers. 45 CFR § 164.514.

16 70. The data supplied by the c_user cookie allows Facebook to identify the Facebook
17 account associated with the cookie. One simply needs to log into Facebook, and then type
18 www.facebook.com/#, with the c_user identifier in place of the “#.” For example, the c_user cookie
19 for Mark Zuckerberg is 4. Logging into Facebook and typing www.facebook.com/4 in the web
20 browser retrieves Mark Zuckerberg’s Facebook page: www.facebook.com/zuck.

21 71. A User’s FID is linked to their Facebook profile, which generally contains a wide
22 range of demographics and other information about the User, including pictures, personal interests,
23 work history, relationship status, and other details. Because the User’s Facebook Profile ID uniquely

24
25 ¹⁸*The future of IP address as an advertising identifier*, AD TECH EXPLAINED (May 16, 2022),
<https://www.adtechexplained.com/p/the-future-of-ip-address-as-an-advertising-identifier/>.

26 ¹⁹ Defendant’s Websites track and transmit data via first party and third-party cookies. C_user, datr,
27 and fr cookies are third-party cookies. The fbp cookie is a Facebook identifier that is set by Facebook
28 source code and associated with Defendant’s use of the Facebook Pixel. The fbp cookie emanates
from Defendant’s Website as a putative first-party cookie but is transmitted to Facebook through
cookie syncing technology that hacks around the same-origin policy.

identifies an individual’s Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly locate, access, and view the user’s corresponding Facebook profile.

72. The “*datr*” cookie identifies the patient’s specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient’s specific web browser and is therefore a means of identification for Facebook users. Facebook keeps a record of every *datr* cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all *datr* cookies associated with his or her Facebook account from Facebook.

73. The “*fr*” cookie is a Facebook identifier that is an encrypted combination of the *c_user* and *datr* cookies.²⁰

74. Defendant also discloses the same kind of patient data described above to other third parties involved in internet marketing, including Google Analytics, AudioEye, and Scorpion Internet Marketing via tracking software that Defendant has installed on its Web Properties. As with the Facebook Meta Pixel, Defendant provides patients and prospective patients with no notice that Defendant is disclosing the contents of their communications to these third parties. Likewise, Defendant does not obtain consent from patients and prospective patients before forwarding their communications to these companies.

75. These disclosures to third parties other than Facebook are equally disturbing. Google Analytics, for example, has been described by the Wall Street Journal as “far and away the web’s most dominant analytics platform,” which “tracks you whether or not you are logged in.”²¹ Like Facebook, Google tracks internet users with IP addresses, cookies, geolocation, and other unique device identifiers. Defendant routinely discloses patients’ Personal Health Information to such Google services as Google Analytics, Google DoubleClick, and Google AdWords.

²⁰ See Gunes Acar et al., *Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission* 16 (March 27, 2015), https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf (last visited Aug. 4, 2023).

²¹ Christopher Mims, *Who Has More of Your Personal Data Than Facebook? Try Google*, WALL STREET JOURNAL (Apr. 22, 2018), <https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401>.

1 76. Google cookies provide personally identifiable data about patients who visit
2 Defendant's website to Google. Defendant transmits personally identifiable Google cookie data to
3 Google.

4 77. Google warns web-developers that Google marketing tools are not appropriate for
5 health-related webpages and websites. Indeed, Google warns web developers that "Health" is a
6 prohibited category that should not be used by advertisers to target ads to users or promote
7 advertisers' products or services.

8 78. Defendant deployed Google tracking tools on nearly every page of its Web Properties,
9 resulting in the disclosure of communications exchanged with patients to be transmitted to Google.
10 These transmissions occurred simultaneously with patients' communications with Defendant and
11 include communications that Plaintiffs and Class Members made about specific medical providers,
12 treatments, conditions, appointments, payments, and registrations and logins to Defendant's patient
13 portal.

14 79. By compelling visitors to their websites to disclose personally identifying data and
15 sensitive medical information to Facebook, Defendant knowingly disclosed information that
16 allowed Facebook and other advertisers to link patients' and visitors' Personal Health Information
17 to their private identities and target them with advertising (or do whatever else Facebook may
18 choose to do with this data, including running "experiments" on its customers by manipulating the
19 information they are shown on their Facebook pages).²² Defendant intentionally shares the Personal
20 Health Information of its patients with Facebook in order to gain access to the benefits of the Meta
21 Pixel tool.

22 ***Defendant's Pixel Disseminates Patient Information Via Its Websites.***

23 80. By way of example, if a patient uses <https://www.mymarinhealth.org> to look for
24 medical treatments, they may select "Gender Affirmation" under the "Programs & Services" tab,
25 which takes them to the list of services offered by Defendant to Users in need of gender affirmation
26 surgery. On those pages the user can further narrow their search results by services offered by

27 ²²*Everything We Know About Facebook's Secret Mood-Manipulation Experiment*, THE ATLANTIC
28 (Jun. 28, 2014), <https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/>.

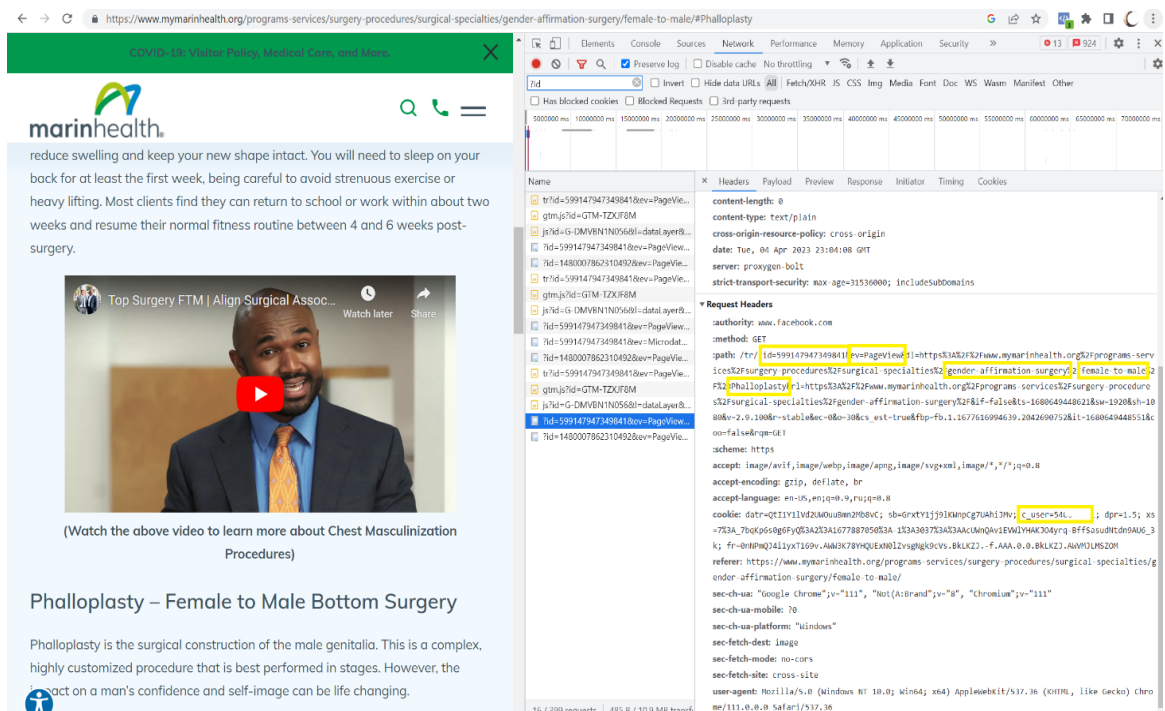
Defendant.

81. The User's selections and filters are transmitted to Facebook via the Meta Pixels, even if they contain the User's treatment, procedures, medical conditions, or related queries, without alerting the User, and the images below confirm that the communications Defendant sends to Facebook contain the User's Private Information and personal identifiers, including but not limited to their IP address, Facebook ID, and datr and fr cookies, along with the search filters the User selected.

82. For example, a patient in search for gender affirmation surgery can search for various surgery procedure options, from "top surgery" and "body contouring" to resources intended to help patients navigate their gender identity journey.²³

83. From the moment the patient begins searching for gender affirmation, their selections or search parameters are automatically transmitted by the Pixel to Facebook along with the User's unique personal identifiers, as evidenced by Figure 4 below.

Figure 4: Defendant's transmission to Facebook of User's search parameters showing treatment sought ("phalloplasty") and the User's unique Facebook ID.



²³ See *Gender Affirmation Surgery*, MARIN HEALTH, <https://www.mymarinhealth.org/programs-services/surgery-procedures/surgical-specialties/gender-affirmation-surgery/>.

1 84. The first line of highlighted text, “id = 599147947349841,” refers to the Defendant’s
2 Pixel ID for this particular Webpage and confirms that Defendant has downloaded the Pixel into its
3 Source Code on this particular Webpage.

4 85. In the second line of text, “ev:” is an abbreviation for event, and “PageView” is the
5 type of event. Here, this event means that Defendant’s Pixel is sending information about the
6 webpage the User is visiting, which can include information like page title, URL, and page
7 description.

8 86. The transmitted URLs contain both the “path” and the “query string” arising from
9 patients’ interactions with Defendant’s Web Properties. The path identifies where a file can be found
10 on a website. For example, a patient reviewing information about the “Services” that Defendant
11 offers patients such as information about “Cancer Care” will generate a URL with the path
12 <https://www.mymarinhealth.org/programs-services/cancer-care/>.

13 87. Likewise, a query string provides a list of parameters. An example of a URL that
14 provides a query string is <https://www.mymarinhealth.org/site-search/?C=pregnancy/>. The query
15 string parameters in this search indicate that a search was done at Defendant’s website for
16 information about pregnancy. In other words, the Meta Pixel captures information that connects a
17 particular user to a particular healthcare provider.

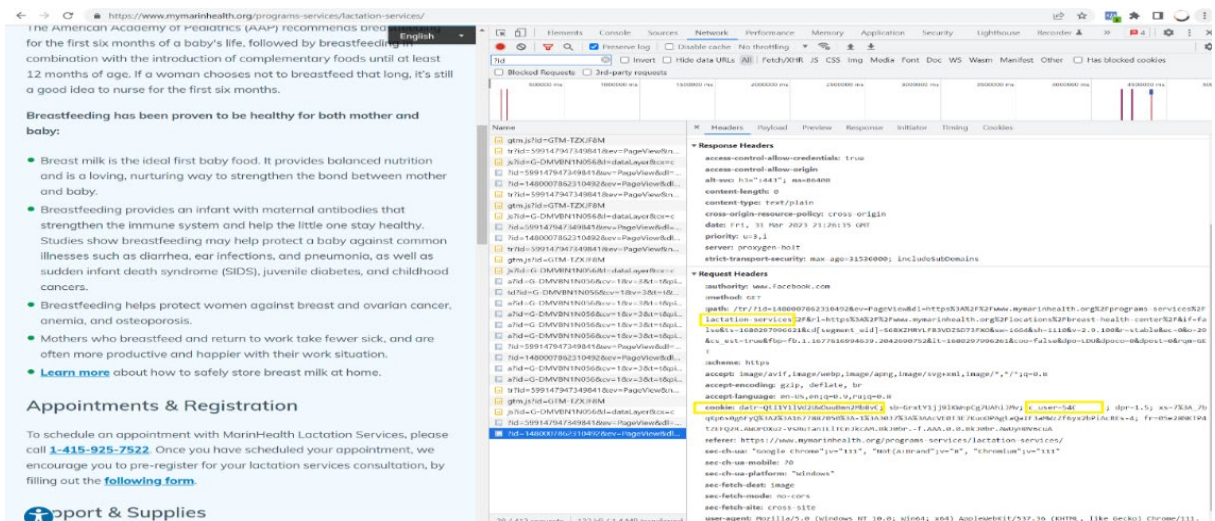
18 88. The remaining lines of text identify the User as a patient: (i) seeking medical care
19 from Defendant via www.mymarinhealth.org; (ii) who is seeking gender affirmation surgery; and
20 (iii) who is searching for phalloplasty.

21 89. Finally, the text (“GET”), demonstrates that Defendant’s Pixel sent the User’s
22 communications, and the Private Information contained therein, alongside the User’s personal
23 identifiers, including Facebook ID and other cookies.

24 90. Defendant offers many types of services and treatments, including options to schedule
25 certain types of treatments, on its Website. For example, under “Breast Health” services, a User can
26 select from various medical services including “Mammogram.”

27 91. This action takes the User to one of Defendant’s web pages for mammograms where
28 the User can click on the button “Schedule A Mammogram” and fill out a form to request an

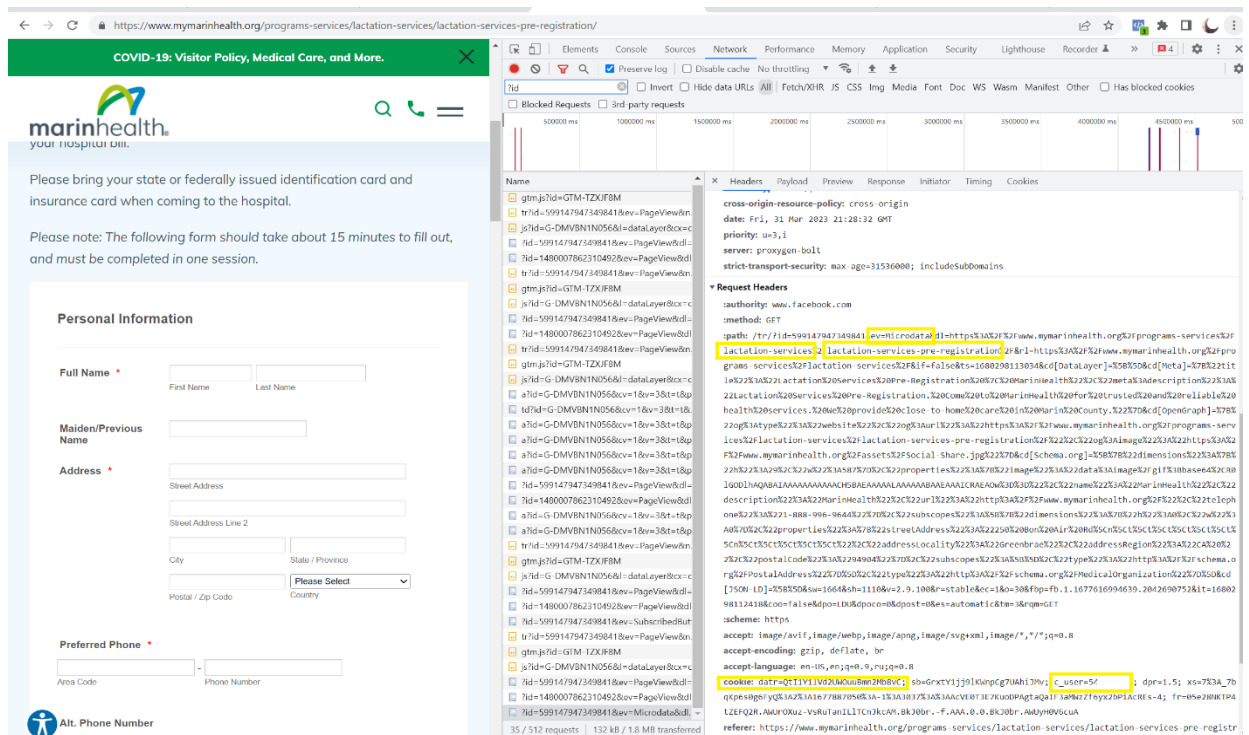
Figure 5: HTTP communication session sent from the User’s device to Facebook revealing the User is trying to schedule an appointment for a mammogram, and their personal identifiers.



21

these services. When a pregnant or new mother in search of lactation services visits these pages, Defendant transmits this information to Facebook:

Figures 6: HTTP communication sessions sent from the User's device to Facebook revealing the navigation path by the User interested in lactation services.



93. Additionally, a patient can use Defendant's website to search for a provider based on their name and/or specialty.

94. These search terms, including those disclosing the User's medical condition or treatment sought, are also transmitted via the Facebook Pixel:

///

///

///

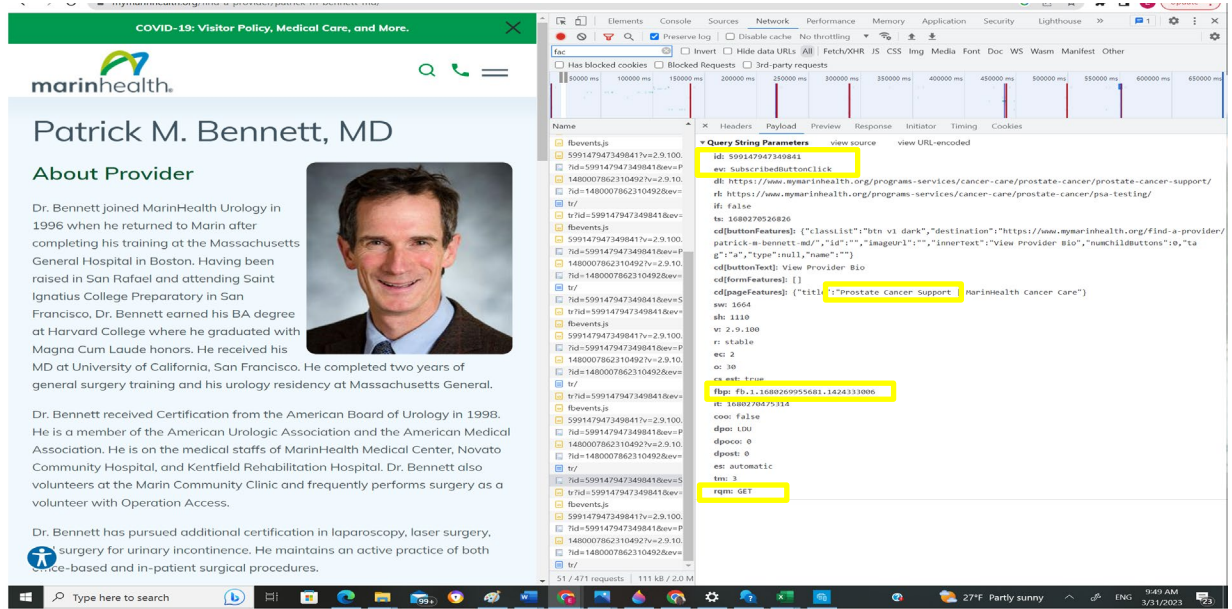
///

///

///

///

Figure 7: HTTP communication session sent from the User's device to Facebook disclosing that the User is looking for a prostate cancer specialist and the provider's name.



95. The Facebook Tracking Pixel uses both first- and third-party cookies. A first-party cookie is “created by the website the user is visiting”—i.e., Defendant.²⁴

96. A third-party cookie is “created by a website with a domain name other than the one the user is currently visiting”—i.e., Facebook.²⁵

97. The `_fbp` cookie is always transmitted as a first-party cookie. A duplicate `_fbp` cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

98. Facebook, at a minimum, uses the `fr`, `_fbp`, and `c_user` cookies to link to FIDs and corresponding Facebook profiles.

99. As shown in the figures above, Defendant sent these identifiers with the event data.

///

²⁴ *First-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/first-party-cookie> (last visited Aug. 4, 2023). This is confirmable by using developer tools to inspect a website’s cookies and track network activity.

²⁵ *Third-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/third-party-cookie> (last visited Aug. 4, 2023). This is also confirmable by tracking network activity.

100. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information, nor did he authorize any assistance with intercepting their communications.

101. Plaintiffs was never provided with any written notice that Defendant disclosed its Website Users' Private Information nor was he provided any means of opting out of such disclosures.

102. Despite this, Defendant knowingly and intentionally disclosed Plaintiffs' Private Information to Facebook.

Defendant Violated Its Promises to Users and Patients to Protect Their Confidentiality.

103. Defendant did not have the legal right to use or share Plaintiffs' and Class Members' data, as this information is protected by the HIPAA Privacy Rule. The Privacy Rule does not permit the use and disclosure of Private Information to Facebook for use in targeted advertising.²⁶

104. Beyond Defendant's legal obligations to protect the confidentiality of individuals' Private Information, Defendant's privacy policies and online representations affirmatively and unequivocally state that any personal information provided to Defendant will remain secure and protected.²⁷

105. Further, Defendant represents to Users that it will only disclose Private Information provided to them under certain circumstances, ***none of which apply here.***²⁸ Defendant's privacy policies do ***not*** permit Defendant to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes.

106. In fact, Defendant acknowledge in its Notice of Privacy Practices that it "...will not sell or otherwise provide the information [they] collect to outside third parties for the purpose of direct or indirect mass email marketing."²⁹

///

²⁶ See 45 C.F.R. § 164.502.

²⁷ *Privacy Policy*, MARINHEALTH, <https://www.mymarinhealth.org/privacy-policy/> (last visited Aug. 6, 2023).

²⁸ See *id.*

²⁹ See *id.*

1 107. Moreover, Defendant represents that it will disclose Users' PHI when required by
2 law or "in the good-faith belief that such action is necessary to: (i) Cooperate with the investigations
3 of purported unlawful activities and conform to the edicts of the law or comply with legal process
4 served on our company; (ii) Protect and defend the rights or property of our Website and related
5 properties; (iii) Identify persons who may be violating the law, the rights of third parties, or
6 otherwise misusing our Website or its related properties."³⁰

7 108. Further, Defendant's Privacy Policy represents:

8 "We follow generally accepted industry standards to protect the
9 information submitted to us, both during transmission and once we
10 receive it."³¹

11 "To make sure that your health information is protected in a way that
12 doesn't interfere with your health care, your information can be used
13 and shared:

- 14 ▪ For your treatment and care coordination
- 15 ▪ To pay doctors and hospitals for your health care and help run
16 their businesses
- 17 ▪ With your family, relatives, friends, or others you identify who
18 are involved with your health care or your health care bills,
19 unless you object
- 20 ▪ To make sure doctors give good care and nursing homes are
21 clean and safe
- 22 ▪ To protect the public's health, such as by reporting when the flu
23 is in your area
- 24 ▪ To make required reports to the police, such as reporting gunshot
25 wounds."

26 109. Upon information and belief, none of these circumstances listed above apply here.

27 110. Finally, in its privacy policy, Defendant acknowledges that, "[p]roviders and health
28 care insurers who are required to follow this law must comply with your right to...receive a notice
that tells you how your health information may be used and shared."³²

³⁰ See *id.*

³¹ See *id.*

³² See *id.*

111. Defendant failed to issue a notice that Plaintiffs and Class Members' Private Information had been impermissibly disclosed to an unauthorized third party. In fact, Defendant *never* disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications, data, and Private Information with Facebook and other third parties.³³

112. Defendant has unequivocally failed to adhere to a single promise vis-à-vis its duty to safeguard the Private Information of its Users. Defendant has made these privacy policies and commitments available on its websites. Defendant included these privacy policies and commitments to maintain the confidentiality of its Users' sensitive information as terms of its contracts with those Users, including contracts entered with Plaintiffs and the Class Members. In these contract terms and other representations to Plaintiffs and Class Members and the public, Defendant promised to take specific measures to protect Plaintiffs' and Class Members' Private Information, consistent with industry standards and federal and state law. However, it failed to do so.

113. Even non-Facebook users can be individually identified via the information gathered on the Digital Platforms, like an IP address or personal device identifying information. This is precisely the type of information for which HIPAA requires the use of de-identification techniques to protect patient privacy.³⁴

114. In fact, in an action currently pending against Facebook related to use of their Pixel on healthcare provider Websites, Facebook explicitly stated it requires Pixel users to "post a prominent notice on every page where the Pixel is embedded and to link from that notice to

³³ In contrast to Defendant, in recent months several medical providers which have installed the Meta Pixel on their Websites have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See, e.g., Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Aug. 4, 2023); Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies*, FIERCE HEALTHCARE (October 20, 2022), <https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3>; *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWswire (August 19, 2022), <https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html>.

³⁴ *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH AND HUM. SERVICES, <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Aug. 4, 2023).

1 information about exactly how the Pixel works and what is being collected through it, so it is not
2 invisible.”³⁵ Defendant did not post such a notice.

3 115. Facebook further stated that “most providers [...] will not be sending [patient
4 information] to Meta because it violates Meta’s contracts for them to be doing that.”³⁶

5 116. Despite a lack of disclosure, Defendant allowed third parties to “listen in” on patients’
6 confidential communications and to intercept and use for advertising purposes the very information
7 they promised to keep private, in order to bolster its profits.

8 ***Plaintiffs and Class Members Reasonably Believed That Their Confidential Medical Information***
9 ***Would Not Be Shared with Third Parties.***

10 117. Plaintiffs and Class Members were aware of Defendant’s duty of confidentiality when
11 they sought medical services from Defendant.

12 118. Indeed, at all times when Plaintiffs and Class Members provided their Private
13 Information to Defendant, they each had a reasonable expectation that the information would remain
14 confidential and that Defendant would not share the Private Information with third parties for a
15 commercial purpose, unrelated to patient care.

16 119. Personal data privacy and obtaining consent to share Private Information are material
17 to Plaintiffs and Class Members.

18 120. Plaintiffs and Class Members relied to their detriment on Defendant’s uniform
19 representations and omissions regarding protection privacy, limited uses, and lack of sharing of their
20 Private Information.

21 121. Now that their sensitive personal and medical information is in possession of third
22 parties, Plaintiffs and Class Members face a constant threat of continued harm – including
23 bombardment of targeted advertisements based on the unauthorized disclosure of their personal
24 data. Collection and sharing of such sensitive information without consent or notice poses a great
25 threat to individuals by subjecting them to the never-ending threat of identity theft, fraud, phishing
26 scams, and harassment.

27 ³⁵ See Transcript of the Argument on Plaintiff’s Motion for Preliminary Injunction in *In re Meta*
28 *Pixel Healthcare Litig.*, *supra* note 6, at 19:12-18.

³⁶ *Id.* at 7:20-8:11.

Plaintiffs and Class Members Have No Way of Determining Widespread Usage of Invisible Pixels.

122. Plaintiffs and Class Members have no idea that Defendant is collecting and utilizing their Private Information, including sensitive medical information, when they engage with Defendant's Websites which have Meta Pixels secretively incorporated in the background.

123. Plaintiffs and Class Members do not realize that tracking Pixels exist because they are invisibly embedded within Defendant's web pages that users might interact with.³⁷ Patients and users of Defendant's Websites do not receive any alerts during their uses of Defendant's Websites stating that Defendant tracks and shares sensitive medical data with Facebook, allowing Facebook and other third parties to subsequently target all users of Defendant's Websites for marketing purposes.

124. Plaintiffs and Class Members trusted Defendant's Websites when inputting sensitive and valuable Private Information. Had Defendant disclosed to Plaintiffs and Class Members that every click, every search, and every input of sensitive information was being tracked, recorded, collected, and **disclosed** to third parties, Plaintiffs and Class Members would not have trusted Defendant's Websites to input such sensitive information.

125. Defendant knew or should have known that Plaintiffs and Class Members would reasonably rely on and trust Defendant's promises regarding the tracking privacy and uses of their Private Information. Furthermore, any person visiting a health website has a reasonable understanding that medical providers must adhere to strict confidentiality protocols and are bound not to share any medical information without their consent.

126. By collecting and sharing Users' Private Information with Facebook and other unauthorized third parties, Defendant caused harm to Plaintiff, Class Members, and all affected individuals.

127. Furthermore, once Private Information is shared with Facebook, such information may not be effectively removed, even though it includes personal and private information.

³⁷ FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FED. TRADE COMM'N (March 16, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>.

128. Plaintiffs fell victim to Defendant's unlawful collection and sharing of their sensitive medical information using the Meta Pixel tracking code on its websites.

Facebook Use of Tracking Pixels in Advertising Business.

129. Facebook is one of the largest advertising companies in the country, with over 2.9 billion active users.³⁸

Realizing the value of having direct access to millions of consumers, in 2007, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming it to be a "completely new way of advertising online" that would allow "advertisers to deliver more tailored and relevant ads."³⁹ Facebook has since evolved into one of the leading digital advertising companies in the world.⁴⁰ Facebook can target users so effectively because it surveils user activity both on and off its website through the use of tracking pixels. This allows Facebook to make inferences about users based on their interests, behavior, and connections.⁴¹

130. Given the highly specific data used to target specific users, it is no surprise that millions of companies and individuals utilize Facebook's advertising services. Meta generates almost all of its revenue from selling advertisement placements:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2023 Q1	\$28.65 billion	\$28.101 billion	98.1%
2022	\$116.61 billion	\$113.64 billion	97.5%
2021	\$117.93 billion	\$114.93 billion	97.46%
2020	\$85.97 billion	\$84.17 billion	97.90%
2019	\$70.70 billion	\$69.66 billion	98.52%
2018	\$55.84 billion	\$55.01 billion	98.51%

³⁸ S. Dixon, *Facebook Users by Country 2023*, STATISTA (February 24, 2023), www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/.

³⁹ *Facebook Unveils Facebook Ads*, META (November 6, 2007), <https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/>.

⁴⁰ *Top 11 Facebook Ads Agencies for Expert Advertising Management in 2025*, NINJA (Jan. 3, 2025), <https://ninjapromo.io/top-facebook-ad-agencies-in-the-world#:~:text=Despite%20newcomers%2C%20Facebook%2C%20with%20over,businesses%20with%20multiple%20targeting%20options.>

⁴¹ *Audience and Targeting*, META ADS, <https://www.facebook.com/business/ads/ad-targeting> (last accessed Jan. 9, 2024).

131. Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications. These profiles are associated with personal identifiers, including IP addresses, cookies, and other device identifiers. Facebook also tracks non-users across the web through its internet marketing products and source code.

132. Tracking pixels can be placed directly on a web page by a developer, or they can be funneled through a "tag manager" service to make the invisible tracking run more smoothly. A tag manager further obscures the third parties to whom user data is transmitted.

133. These tracking pixels can collect dozens of data points about individual website users who interact with a website. One of the world's most prevalent tracking pixels, called the Meta Pixel, is provided by Facebook.

134. Launched in 2015, Meta Pixel, formerly known as Facebook Pixel, is one of its most powerful advertising tools.

135. Ad Targeting has been extremely successful due, in large part, to Facebook's ability to target people at a granular level. "Among many possible target audiences, Facebook offers advertisers, [for example,] 1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"⁴²

136. Acknowledging that micro-level targeting is highly problematic, in November of 2021 Facebook announced that it was removing options that "relate to topics people may perceive as sensitive," such as "Health causes (e.g., 'Lung cancer awareness', 'World Diabetes Day', 'Chemotherapy'), Sexual orientation (e.g., 'same-sex marriage' and 'LGBT culture')", "Religious practices and groups (e.g., 'Catholic Church' and 'Jewish holidays')," as well as "Political beliefs, social issues, causes, organizations, and figures."

137. For Facebook, Pixel acts as a conduit of information, sending the information it collects to Facebook through scripts running in the User's internet browser. The information is sent in data packets labeled with PII, including the User's IP address.

⁴² Natasha Singer, *What You Don't Know about How Facebook Uses Your Data*, N.Y. TIMES (April 11, 2018), <https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>.

138. If the User has a Facebook account, the Private Information collected is linked to the individual Users' Facebook account. For example, if the User is logged into their Facebook account when the User visits a website where the Meta Pixel is installed, many common browsers will attach third-party cookies allowing Facebook to link the data collected by the Pixel to the specific Facebook user.

139. Alternatively, Facebook can link the data to a users' Facebook account through the "Facebook Cookie." The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users.⁴³

140. Facebook can also link Private Information to Facebook accounts through identifying information collected via Meta Pixel through what Facebook calls "Advanced Matching."⁴⁴ There are two forms of Advanced Matching: manual matching and automatic matching. Using Manual Advanced Matching the website developer manually sends data to Facebook to link users. Using Automatic Advanced Matching, the Pixel scours the data it receives to search for recognizable fields, including name and email address to match users to their Facebook accounts.⁴⁵

141. While the Meta Pixel tool "hashes" personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent *Facebook* from using the data. In fact, Facebook explicitly uses the hashed information it gathers to link pixel data to Facebook profiles.⁴⁶

142. Facebook also uses browser-fingerprinting to uniquely identify individuals. A browser-fingerprint is information collected about a computing device that can be used to identify the specific device. Web browsers have several attributes that vary between users, like the browser

⁴³ Maciej Zawadziński & Michal Wlosik, *What Facebook's First-Party Cookie Means for AdTech*, CLEAR CODE (June 8, 2022), <https://clearcode.cc/blog/facebook-first-party-cookie-adtech/>.

⁴⁴ Illia Lahunou, *What is Advanced Matching in Facebook Pixel and How it Works*, VERFACTO, <https://www.verfacto.com/blog/ecommerce/advanced-matching-facebook-pixel/> (last visited Aug. 4, 2023); *see also About advanced matching for web*, META, <https://www.facebook.com/business/help/611774685654668?id=1205376682832142> (last visited Aug. 4, 2023).

⁴⁵ *Id.*

⁴⁶ *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (Jun. 16, 2022), <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.

1 software system, plugins that have been installed, fonts that are available on the system, the size of
2 the screen, color depth, and more. Together, these attributes create a fingerprint that is highly
3 distinctive. The likelihood that two browsers have the same fingerprint is at least as low as 1 in
4 286,777, and the accuracy of the fingerprint increases when combined with cookies and the user's
5 IP address. Facebook recognizes a visitor's browser fingerprint each time a Facebook button is
6 loaded on a third-party website page. Facebook can target users so effectively because it surveils
7 user activity both on and off its official website.

8 143. This allows Facebook to make inferences about users far beyond what they explicitly
9 disclose, like their "interests," "behavior," and "connections." Facebook compiles this information
10 into a generalized dataset called "Core Audiences," which advertisers use to create highly specific
11 targeted advertising.

12 144. Browser-fingerprints are personal identifiers, and tracking pixels can collect browser
13 fingerprints from website visitors.

14 145. The value of browser-fingerprinting to advertisers (and trackers who want to monetize
15 aggregated data) is that they can be used to track website users just as cookies do, but it employs
16 much more subtle techniques.⁴⁷ Additionally, unlike cookies, users cannot clear their fingerprint
17 and therefore cannot control how their personal information is collected.⁴⁸

18 146. A recent investigation revealed that the Meta Pixel was installed inside password-
19 protected patient portals of at least seven health systems.⁴⁹ When a User navigates through their
20 patient portal, the Meta Pixel sends Facebook sensitive data including but not limited to, the User's
21 medication information, prescriptions, descriptions of their issues, notes, test results, and details
22 about upcoming doctor's appointments.

26 ⁴⁷ Chris Hauk, *What Is Browser Fingerprinting? How It Works And How To Stop It*, PIXEL PRIVACY
27 (Updated April 11, 2024), <https://pixelprivacy.com/resources/browser-fingerprinting/>.

28 ⁴⁸ Justin Schuh, *Building a more private web*, GOOGLE (Aug. 22, 2019),
<https://www.blog.google/products/chrome/building-a-more-private-web/>.

⁴⁹ See Feathers, *et al.*, *supra* note 3.

1 147. David Holtzman, a health privacy consultant was “deeply troubled” by the results of
2 The Markup’s investigation and indicated “it is quite likely a HIPAA violation” by the hospitals,
3 such as Defendant.⁵⁰

4 148. Laura Lazaro Cabrera, a legal officer at Privacy International, indicated that
5 Facebook’s access to use even only some of these data points—such as just the URL—is
6 problematic. She explained, “Think about what you can learn from a URL that says something about
7 scheduling an abortion’ . . . ‘Facebook is in the business of developing algorithms. They know what
8 sorts of information can act as a proxy for personal data.”⁵¹

9 149. When Users visit websites that have incorporated the Meta Pixel, the Pixel collects
10 information about Users’ activity on that website. This information is then shared with Facebook
11 and, in tandem with data from the Users’ Facebook profile such as their age, gender, and interests,
12 can be used to target the user with advertisements on Facebook and other websites that use Pixel.

13 150. However, the collection and use of this data raises concerns about user privacy and
14 the potential misuse of personal information. For example, when Users browse Defendant’s
15 Websites, every bit of their activity is tracked and monitored. By analyzing this data using
16 algorithms and machine learning techniques, these entities tracking this information can learn a
17 chilling level of detail about Users’ behavioral patterns, preferences, and interests.

18 151. While this data can be used to provide personalized and targeted content and
19 advertising, it can also be used for more nefarious purposes, such as tracking and surveillance. For
20 example, if an advertiser or social media platform has access to a User’s browsing history, search
21 queries, and social media activity, they could potentially build a detailed profile of that User’s
22 behavior patterns, including where they go, what they do, and who they interact with.

23 152. This level of surveillance and monitoring raises important ethical and legal questions
24 about privacy, consent, and the use of personal data. It is important for Users to be aware of how
25

26 ⁵⁰ *Id.*

27 ⁵¹ Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly*
28 *Sensitive Info on Would-Be Patients*, THE MARKUP (Aug. 4, 2022), <https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients>.

1 their data is being collected and used, and to have control over how their information is shared and
2 used by advertisers and other entities.

3 153. Moreover, the misuse of this data could potentially lead to the spread of false or
4 misleading information, which could have serious consequences, particularly in the case of health-
5 related information. As an example, the Cambridge Analytica scandal revealed that personal data
6 was misused to target individuals with political propaganda and misinformation.⁵²

7 154. The Cambridge Analytica scandal involved the misuse of personal data collected from
8 Facebook users, which was then used to target individuals with political advertising and propaganda.
9 The scandal highlighted the potential dangers of using personal data for targeted advertising and the
10 need for greater transparency and accountability in the collection and use of personal information.⁵³
11 One of the ways that Cambridge Analytica was able to collect personal data was through the use of
12 third-party apps that collected data from users and their friends. This data was then used to build
13 detailed profiles of individuals, which were used to target them with personalized political ads and
14 propaganda.

15 155. The use of algorithms and machine learning techniques to analyze this data allowed
16 Cambridge Analytica to identify patterns in users' behavior and preferences, which were then used
17 to target them with specific messages and ads.

18 156. This highlights the potential dangers of using personal data to build detailed profiles
19 of individuals, particularly when that data is collected without their knowledge or consent. It also
20 raises important questions about the ethics of using personal data for political purposes and the need
21 for greater regulation and oversight of data collection and use.

22 157. Finally, as pointed out by the OCR, impermissible disclosures of such data in the
23 healthcare context "may result in identity theft, financial loss, discrimination, stigma, mental
24 anguish, or other serious negative consequences to the reputation, health, or physical safety of the
25

26
27 ⁵² Sam Meredith, *Here's Everything You Need to Know about the Cambridge Analytica Scandal*,
CNBC (March 23, 2018), <https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html>.
28 ⁵³ *Id.*

1 individual or to others identified in the individual’s PHI. . . . This tracking information could also
2 be misused to promote misinformation, identity theft, stalking, and harassment.”⁵⁴

3 158. In conclusion, as Judge Orrick pointed out in a recent decision allowing claims under
4 California and common law against Regents of the University of California for collecting personal
5 medical data via the Meta Pixel to go forward, “[p]ersonal medical information is understood to be
6 among the most sensitive information that could be collected about a person” and unauthorized
7 transmission or interception of such data by third parties may constitute a “highly offensive”
8 intrusion of privacy. *Doe v. Regents of Univ. of Cal.*, 23-cv-00598-WHO (N.D. Cal. May 6, 2023).
9 ***Defendant Knew Plaintiffs’ Private Information Included Sensitive Medical Information,***
10 ***Including Medical Records.***

11 159. Defendant’s websites are designed for interactive communication with patients,
12 including scheduling appointments, searching for physicians, paying bills, requesting medical
13 records, learning about medical issues and treatment options, and joining support groups

14 160. Defendant was aware that by incorporating the Meta Pixel onto its websites, this
15 would result in the disclosure and use of Plaintiffs’ and Class Members’ Private Information,
16 including sensitive medical information.

17 161. By virtue of how the Meta Pixel works, i.e., sending all interactions on a website to
18 Facebook, Defendant was aware that its Users’ Private Information would be sent to Facebook when
19 they researched specific medical conditions and/or treatments, looked up providers, made
20 appointments, typed specific medical queries into the search bar, and otherwise interacted with
21 Defendant’s Websites.

22 162. Indeed, software companies like MyChart that provide online access to medical
23 records utilized by Defendant have “specifically recommended heightened caution around the use
24 of custom analytics.” Despite this, Defendant continued to use Meta Pixel on its Websites.

25
26
27
28 ⁵⁴ *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, supra*
note 12.

1 **Facebook's History of Egregious Privacy Violations.**

2 163. Defendant knew or should have known that Facebook could not be trusted with its
3 patients' sensitive medical information.

4 164. Due to its ability to target individuals based on granular data, Facebook's ad-targeting
5 capabilities have frequently come under scrutiny. For example, in June 2022, Facebook entered into
6 a settlement with the Department of Justice regarding its Lookalike Ad service, which permitted
7 targeted advertising by landlords based on race and other demographics in a discriminatory manner.
8 That settlement, however, reflected only the latest in a long history of egregious privacy violations
9 by Facebook.

10 165. In 2007, when Facebook launched "Facebook Beacon," users were unaware that their
11 online activity was tracked, and that the privacy settings originally did not allow users to opt-out.
12 As a result of widespread criticism, Facebook Beacon was eventually shut down.

13 166. In 2011, Facebook settled charges with the Federal Trade Commission relating to its
14 sharing of Facebook user information with advertisers, as well as its false claim that third-party apps
15 were able to access only the data they needed to operate when—in fact—the apps could access
16 nearly all of a Facebook user's personal data. The resulting Consent Order prohibited Facebook
17 from misrepresenting the extent to which consumers can control the privacy of their information,
18 the steps that consumers must take to implement such controls, and the extent to which Facebook
19 makes user information available to third parties.⁵⁵

20 167. Facebook found itself in another privacy scandal in 2015 when it was revealed that
21 Facebook could not keep track of how many developers were using previously downloaded
22 Facebook user data. That same year, it was also revealed that Facebook had violated users' privacy
23 rights by harvesting and storing Illinois' users' facial data from photos without asking for their
24 consent or providing notice. Facebook ultimately settled claims related to this unlawful act for \$650
25 million.

26
27 ⁵⁵ *In the Matter of Facebook, Inc., a corporation*, FEDERAL TRADE COMMISSION (updated Nov. 7,
28 2024) <https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter>.

1 168. In 2018, Facebook was again in the spotlight for failing to protect users' privacy.
 2 Facebook representatives testified before Congress that a company called Cambridge Analytica may
 3 have harvested the data of up to 87 million users in connection with the 2016 election. This led to
 4 another FTC investigation in 2019 into Facebook's data collection and privacy practices, resulting
 5 in a record-breaking five-billion-dollar settlement.

6 169. Likewise, a different 2018 report revealed that Facebook had violated users' privacy
 7 by granting access to user information to over 150 companies.⁵⁶ Some companies were even able
 8 to read users' private messages.

9 170. In June 2020, after promising users that app developers would not have access to data
 10 if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party
 11 developers to access this data.⁵⁷ This failure to protect users' data enabled thousands of developers
 12 to see data on inactive users' accounts if those users were Facebook friends with someone who was
 13 an active user.

14 171. On February 18, 2021, the New York State Department of Financial Services released
 15 a report detailing the significant privacy concerns associated with Facebook's data collection
 16 practices, including the collection of health data. The report noted that while Facebook maintained
 17 a policy that instructed developers not to transmit sensitive medical information, Facebook received,
 18 stored, and analyzed this information anyway. The report concluded that "[t]he information
 19 provided by Facebook has made it clear that Facebook's internal controls on this issue have been
 20 very limited and were not effective ... at preventing the receipt of sensitive data."⁵⁸

21 172. The New York State Department of Financial Service's concern about Facebook's
 22 cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a
 23 different settlement involving Facebook's monetizing of sensitive medical data. In that case, the

24 ⁵⁶ *Facebook let tons of companies get info about you, including Amazon, Netflix, and Microsoft*,
 25 CNBC (Dec. 19, 2018), <https://www.cnbc.com/2018/12/19/facebook-gave-amazon-microsoft-netflix-special-access-to-data-nyt.html>.

26 ⁵⁷ Kurt Wagner, *Facebook admits another blunder with user data*, FORTUNE (Jul. 1, 2020),
 27 <https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/>.

28 ⁵⁸ *Report of Investigation of Facebook, Inc Data Privacy Concerns*, NEW YORK STATE DEPT. OF
 FINANCIAL SERVICES (Feb. 18, 2021),
https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.

1 more than 100 million users of Flo, a period and ovulation tracking app, learned something startling:
2 the company was sharing their data with Facebook.⁵⁹ When a user was having his period or informed
3 the app of his intention to get pregnant, Flo would tell Facebook, which could then use the data for
4 all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade
5 Commission for lying to its users about secretly sharing their data with Facebook, as well as with a
6 host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC
7 reported that Flo “took no action to limit what these companies could do with users’ information.”⁶⁰

8 173. More recently, Facebook employees admitted to lax protections for sensitive user
9 data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that
10 “We do not have an adequate level of control and explainability over how our systems use data, and
11 thus we can’t confidently make controlled policy changes or external commitments such as ‘we will
12 not use X data for Y purpose.’”⁶¹

13 174. These revelations were confirmed by an article published by the Markup in 2022,
14 which found during the course of its investigation that Facebook’s purported “filtering” failed to
15 discard even the most obvious forms of sexual health information. Worse, the article found that the
16 data that the Meta Pixel was sending Facebook from hospital websites not only included details
17 such as patients’ medications, descriptions of their allergic reactions, details about their upcoming
18 doctor’s appointments, but also included patients’ names, addresses, email addresses, and phone
19 numbers.⁶²

20 175. Despite knowing that the Meta Pixel code embedded in its websites was sending
21 patients’ Personal Health Information to Facebook, Defendant did nothing to protect patients and
22

23
24 ⁵⁹ Justin Sherman, *Your Health Data Might Be for Sale*, SLATE (Jun. 22, 2022),
<https://slate.com/technology/2022/06/health-data-brokers-privacy.html>.

25 ⁶⁰ *Id.*

26 ⁶¹ *Facebook Doesn’t Know What It Does With Your Data, Or Where It Goes: Leaked Document*,
VICE (Apr. 26, 2022), [https://www.vice.com/en/article/facebook-doesnt-know-what-it-does-with-](https://www.vice.com/en/article/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes/)
27 [your-data-or-where-it-goes/](https://www.vice.com/en/article/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes/).

28 ⁶² *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (Jul.
19, 2023), [https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-](https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites)
[information-from-hospital-websites](https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites).

1 users from egregious intrusions into patient privacy, choosing instead to benefit at those patients'
2 and users' expense.

3 ***Defendant's interception and disclosure of patient communications permits Facebook, Google,***
4 ***and other third-party advertising companies to engage in cross-device targeting across multiple***
5 ***devices***

6 176. In addition to enabling Defendant to advertise to patients and potential patients on
7 non-Defendant websites, Defendant's misuse and exploitation of patient data and communications
8 also facilitates third parties' ability to target advertisements on other computing devices that a
9 patient uses. This is called cross-device targeting.

10 177. Third parties including Facebook and Google have established a unique ID for
11 individuals that tie together their desktop, laptop, and smartphone computing devices. For example,
12 even if a patient has never visited Defendant's website on their smartphone, cross-device tracking
13 and marketing allows Defendant and other third parties to target patients on that device. In other
14 words, a patient or potential patient who visited Defendant's website on his desktop, but never on
15 his smartphone, can nevertheless be targeted with advertisements by both Defendant and other third
16 parties on his smartphone.

17 178. Defendant's and other third parties' use of cross-device targeting demonstrates that
18 the data Defendant discloses to third parties is personally identifiable because it enables patients to
19 be tracked across multiple devices that patients own—even if a patient has never communicated
20 with Defendant on one or more of their devices.

21 179. Defendant has made the decision that access to the targeted advertising (including
22 retargeting and cross-device tracking) that is enabled by its disclosure of patient data and
23 communications is of commercial benefit to Defendant.

24 180. Defendant obtains additional revenue from its deployment of third-party tracking
25 tools through which it discloses personally identifying patient data and communications to third
26 parties, including Google and Facebook.

181. Any additional revenue that that Defendant obtained from its unauthorized misuse of its own patients' Personal Health Information is unearned and is the rightful property of the patients (including Plaintiffs and Class Members) from whom it was obtained.

182. Defendant's unauthorized disclosure and misuse of Plaintiffs' and Class Members' Personal Health Information is a form of theft, for which the victims are entitled to recover anything acquired with the stolen assets, even if the items acquired have a value that exceeds the value of that which was stolen.

Plaintiffs and Class Members Have a Reasonable Expectation of Privacy in Their Private Information, Especially with Respect to Sensitive Medical Information.

183. Plaintiffs and Class Members have a reasonable expectation of privacy in their Private Information, including personal information and sensitive medical information.

184. Patient PHI specifically is protected by federal law under HIPAA.

185. HIPAA sets national standards for safeguarding protected health information. For example, HIPAA limits the permissible uses of health information and prohibits the disclosure of this information without explicit authorization. *See* 45 C.F.R. § 164.502. HIPAA also requires that covered entities implement appropriate safeguards to protect this information. *See* 45 C.F.R. § 164.530(c)(1).

186. This federal legal framework applies to health care providers, including Defendant.

187. Given the application of HIPAA to Defendant, Plaintiffs and the members of the Class had a reasonable expectation of privacy over their PHI.

188. As patients, Plaintiffs had a reasonable expectation of privacy that their health care provider and its associates would not disclose their Personal Health Information to third parties without their express authorization.

189. The modern Hippocratic Oath provides, "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."⁶³ Likewise, the American Medical

⁶³ *The Hippocratic Oath: Modern Version*, PBS, https://www.pbs.org/wgbh/nova/doctors/oath_modern.html (last accessed Jan. 8, 2025).

1 Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of
2 patient data and communications.

3 190. For example, the AMA has issued medical ethics opinions providing that "[p]rotecting
4 information gathered in association with the care of a patient is a core value in health care. However,
5 respecting patient privacy in other forms is also fundamental, as an expression of respect for patient
6 autonomy and a prerequisite for trust....Physicians must seek to protect patient privacy in all settings
7 to the greatest extent possible and should ... [m]inimize intrusion on privacy when the patient's
8 privacy must be balanced against other factors [and inform] the patient when there has been a
9 significant infringement on privacy of which the patient would otherwise not be aware."⁶⁴

10 191. The AMA's ethics opinions have further cautioned physicians and hospitals that
11 "[d]isclosing information to third parties for commercial purposes without consent undermines trust,
12 violates principles of informed consent and confidentiality, and may harm the integrity of the
13 patient-physician relationship."⁶⁵

14 192. Plaintiffs' and Class Members' reasonable expectations of privacy in their Personal
15 Health Information are grounded in, among other things, Defendant's status as a health care
16 provider, Defendant's common law obligation to maintain the confidentiality of patients' Personal
17 Health Information, state and federal laws protecting the confidentiality of medical information,
18 state and federal laws protecting the confidentiality of communications and computer data, and state
19 laws prohibiting the unauthorized use and disclosure of personal means of identification.

20 193. Several studies examining the collection and disclosure of consumers' sensitive
21 medical information confirm that the collection and unauthorized disclosure of sensitive medical
22 information from millions of individuals, as Defendant has done here, violates expectations of
23 privacy that have been established as general societal norms.

24
25
26 ⁶⁴ *Privacy in Health Care*, AMA CODE OF ETHICS, <https://code-medical-ethics.ama-assn.org/ethics-opinions/privacy-health-care> (last accessed Jan. 8, 2025).

27 ⁶⁵ *Access to Medical Records by Data Collection Companies*, AMA CODE OF ETHICS, <https://code-medical-ethics.ama-assn.org/ethics-opinions/access-medical-records-data-collection-companies>
28 (last accessed Jan. 8, 2025).

1 194. Privacy polls and studies uniformly show that the overwhelming majority of
2 Americans consider one of the most important privacy rights to be the need for an individual's
3 affirmative consent before a company collects and shares its customers' data.

4 195. For example, a recent study by Consumer Reports shows that 92% of Americans
5 believe that internet companies and websites should be required to obtain consent before selling or
6 sharing consumers' data, and the same percentage believe internet companies and websites should
7 be required to provide consumers with a complete list of the data that has been collected about
8 them.⁶⁶ Moreover, according to a study by Pew Research Center, a majority of Americans,
9 approximately 79%, are concerned about how data is collected about them by companies.⁶⁷

10 196. Users act consistent with these preferences. Following a new rollout of the iPhone
11 operating software—which asks users for clear, affirmative consent before allowing companies to
12 track users—85% of worldwide users and 94% of U.S. users chose not to share data when
13 prompted.⁶⁸

14 197. Medical data is particularly even more valuable because unlike other personal
15 information, such as credit card numbers which can be quickly changed, medical data is static. This
16 is why companies possessing medical information, like Defendant, are intended targets of cyber-
17 criminals.⁶⁹

18 198. Patients using Defendant's Websites must be able to trust that the information they
19 input including their physicians, their health conditions and courses of treatment will be protected.
20 Indeed, numerous state and federal laws require this. And these laws are especially important when

21 ⁶⁶ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*,
22 CONSUMER REPORTS (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

23 ⁶⁷ *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal*
24 *Information*, PEW RESEARCH CENTER (November 15, 2019),
25 <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

26 ⁶⁸ Margaret Taylor, *How Apple Screwed Facebook*, WIRED (May 19, 2021),
<https://www.wired.co.uk/article/apple-ios14-facebook>.

27 ⁶⁹ Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit*
28 *card*, REUTERS (September 24, 2014), <https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924>.

protecting individuals with medical conditions such as HIV or AIDS that can and do subject them to regular discrimination. Furthermore, millions of Americans keep their health information private because it can become the cause of ridicule and discrimination. For instance, despite the anti-discrimination laws, persons living with HIV/AIDS are routinely subject to discrimination in healthcare, employment, and housing.⁷⁰

199. The concern about sharing medical information is compounded by the reality that advertisers view this type of information as particularly high value. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one article put it: “the datafication of family life can begin from the moment in which a parent thinks about having a baby.”⁷¹ The article continues, “[c]hildren today are the very first generation of citizens to be datafied from before birth, and we cannot foresee — as yet — the social and political consequences of this historical transformation. What is particularly worrying about this process of datafication of children is that companies like . . . Facebook . . . are harnessing and collecting multiple typologies of children’s data and have the potential to store a plurality of data traces under unique ID profiles.”⁷²

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

⁷⁰ Bebe J. Anderson, JD, *HIV Stigma and Discrimination Persist, Even in Health Care*, AMA J. ETHICS (December 2009), <https://journalofethics.ama-assn.org/article/hiv-stigma-and-discrimination-persist-even-health-care/2009-12>.

⁷¹ Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, MIT PRESS READER (January 14, 2021), <https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/>.

⁷² *Id.*

⁷³ Class Action Complaint, *Jane Doe v. Regents of the Univ. of Cal. d/b/a UCSF Medical Center*, CLASS ACTION (Feb. 9, 2023), <https://www.classaction.org/media/doe-v-regents-of-the-university-of-california.pdf>.

201. Defendant surreptitiously collected and used Plaintiffs’ and Class Members’ Private Information, including highly sensitive medical information, through Meta Pixel in violation of Plaintiffs’ and Class Members’ privacy interests.

Plaintiffs and Class Members’ Personal Health Information that Defendant collected, disclosed, and used has economic value, and its disclosure caused Plaintiffs and Class Members economic harm.

202. Plaintiffs’ Personal Health Information that Defendant collected, monitored, disclosed, and used is Plaintiffs’ property, it has economic value, and its illicit disclosure has caused Plaintiffs harm.

203. It is common knowledge that there is an economic market for consumers’ personal data—including the kind of data that Defendant has collected and disclosed from Plaintiffs and Class Members.

204. In 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals and that within that context, “age, gender and location information” were being sold for approximately “\$0.50 per 1,000 people.”⁷⁴

205. In 2015, *TechCrunch* reported that “to obtain a list containing the names of individuals suffering from a particular disease,” a market participant would have to spend about “\$0.30” per name.⁷⁵ That same article noted that “Data has become a strategic asset that allows companies to acquire or maintain a competitive edge” and that the value of a single user’s data can vary from \$15 to more than \$40 per user.⁷⁶

206. In a 2021 Washington Post article, the legal scholar Dina Srinivasan said that consumers “should think of Facebook’s cost as [their] data and scrutinize the power it has to set its own price.”⁷⁷ This price is only increasing. According to Facebook’s own financial statements, the

⁷⁴ *How much is your personal data worth?*, FINANCIAL TIMES, <https://ig.ft.com/how-much-is-your-personal-data-worth/> (last accessed Jan. 8, 2025).

⁷⁵ *What’s The Value Of Your Data?*, TECH CRUNCH (Oct. 13, 2015), <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>.

⁷⁶ *Id.*

⁷⁷ *There’s no escape from Facebook, even if you don’t use it*, WASHINGTON POST (Aug. 29, 2021), <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/>.

1 value of the average American's data in advertising sales rose from \$19 to \$164 per year between
2 2013 and 2020.⁷⁸

3 207. Despite the protections afforded by law, there is an active market for health
4 information. Medical information obtained from health providers garners substantial value because
5 of the fact that it is not generally available to third party data marketing companies because of the
6 strict restrictions on disclosure of such information by state laws and provider standards, including
7 the Hippocratic oath. Even with these restrictions, however, a multi-billion-dollar market exists for
8 the sale and purchase of such private medical information.⁷⁹

9 208. Further, individuals can sell or monetize their own data if they so choose. For
10 example, Facebook has offered to pay individuals for their voice recordings,⁸⁰ and it has paid
11 teenagers and adults up to \$20 per month plus referral fees to install an app that allows Facebook to
12 collect data on how individuals use their smart phones.⁸¹

13 209. A myriad of other companies and apps such as DataCoup, Nielsen Computer, Killi,
14 and UpVoice also offer consumers money in exchange for access to their personal data.⁸²

15 210. Further demonstrating the financial value of Class Members' medical data, CNBC has
16 reported that hospital executives have received a growing number of bids for user data.⁸³

17
18 ⁷⁸ *Id.*

19 ⁷⁹ *Your medical data is for sale, and there's nothing you can do about it*, REVEAL,
20 [https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-](https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it/)
21 [it/](https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it/); *see also* SLATE, <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>.

22 ⁸⁰ *Facebook will now pay you for your voice recordings*, THE VERGE (Feb. 20, 2020),
23 [https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-](https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-pronunciations-app)
24 [viewpoints-pronunciations-app](https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-pronunciations-app).

25 ⁸¹ *Facebook pays teens to install an app that could collect all kinds of data*, CNBC (Jan. 29 2019),
26 [https://www.cnbcm.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-](https://www.cnbcm.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html)
27 [techcrunch.html](https://www.cnbcm.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html).

28 ⁸² *Apps that Pay You for Data Collection*, CREDIT DONKEY (Jun. 12, 2021),
<https://www.creditdonkey.com/best-apps-data-collection.html>; *see also Can You Earn Money From Your Data? Yes, You Can. And Here's How!*, MONETHA (Apr. 28, 2022),
<https://www.monetha.io/blog/rewards/earn-money-from-your-data/>.

⁸³ Christina Farr, *Hospital execs say they are getting flooded with requests for your health data*, CNBC (Dec. 18, 2019), [https://www.cnbcm.com/2019/12/18/hospital-execs-say-theyre-flooded-](https://www.cnbcm.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html#:~:text=Hospitals%2C%20many%20of%20which%20are,health%20information%20to%20tech%20companies)
[with-requests-for-your-health-](https://www.cnbcm.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html#:~:text=Hospitals%2C%20many%20of%20which%20are,health%20information%20to%20tech%20companies)
[data.html#:~:text=Hospitals%2C%20many%20of%20which%20are,health%20information%20to%20tech%20companies](https://www.cnbcm.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html#:~:text=Hospitals%2C%20many%20of%20which%20are,health%20information%20to%20tech%20companies).

Hospitals, many of which are increasingly in dire financial straits, are weighing a lucrative new opportunity: selling patient health information to tech companies. Aaron Miri is chief information officer at Dell Medical School and University of Texas Health in Austin, so he gets plenty of tech start-ups approaching him to pitch deals and partnerships. Five years ago, he'd get about one pitch per quarter. But these days, with huge data-driven players like Amazon and Google making incursions into the health space, and venture money flooding into Silicon Valley start-ups aiming to bring machine learning to health care, the cadence is far more frequent. "It's all the time," he said via phone. "Often, once a day or more."

211. CNBC also explained:⁸⁴

[D]e-identified patient data has become its own small economy: This is a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers. Just one company alone, IQVIA, said on its website that it has access to more than 600 million patient records globally that are nonidentified, much of which it accesses through provider organizations. The buyers, which include pharma marketers, will often use it for things like clinical trial recruiting But hospital execs worry that this data may be used in unintended ways, and not always in the patient's best interest.

212. Given the monetary value that data companies like Facebook have already paid for personal information in the past, Defendant has deprived Plaintiffs and the Class Members of the economic value of their sensitive medical information by collecting, using, and disclosing that information to Facebook without consideration for Plaintiffs' and the Class Members' property. ***Defendant's failure to inform its patients and prospective patients that their Personal Health Information has been disclosed to Facebook or to take any steps to halt the continued disclosure of patients' Personal Health Information is malicious, oppressive, and in reckless disregard of Plaintiffs' and Class Members' rights.***

213. Hospital systems, like other businesses, have a legal obligation to disclose data breaches to their customers. *See, e.g.*, Cal. Civ. Code § 1798.82.

214. For example, in August 2022, Novant Health informed approximately 1.3 million patients that their medical data was disclosed to Facebook due to the installation of the Facebook

⁸⁴ *Id.*

Meta Pixel on the hospital system's websites.⁸⁵ Novant Health's data breach announcement conceded that the Meta Pixel tool installed on its websites "allowed certain private information to be transmitted to Meta from the Novant Health website."⁸⁶ Novant Health further admitted that the information about its patients that was disclosed to Facebook included "an impacted patient's: demographic information such as email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes."⁸⁷

215. Likewise, in October 2022, Advocate Aurora Health informed approximately 3 million patients that their Personal Health Information had been disclosed to Facebook via the Meta Pixel installed on Advocate Aurora Health's website.⁸⁸ Advocate Aurora Health's data breach notification conceded that patient information had been transmitted to third parties including Facebook and Google when patients used the hospital system's website.⁸⁹

216. Advocate Aurora Health further admitted that a substantial amount of its patients' Personal Health Information has been shared with Facebook and Google including patients' "IP address; dates, times, and/or locations of scheduled appointments; your proximity to an Advocate Aurora Health location; information about your provider; [and] type of appointment or procedure."⁹⁰ In conjunction with its data breach notice, Advocate Aurora Health claimed that the

⁸⁵ *1.3M Novant Health patients notified of 'unintended' disclosure via Facebook Pixel*, SC MEDIA (Aug. 16, 2022), <https://www.scmagazine.com/analysis/breach/1-3m-novant-health-patients-notified-of-unintended-disclosure-via-facebook-pixel>.

⁸⁶ *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWswire (Aug. 19, 2022), <https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html>.

⁸⁷ *Id.*

⁸⁸ *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies*, FIERCE HEALTHCARE (Oct. 20, 2022), <https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3>.

⁸⁹ ADVOCATE HEALTH, <https://www.advocateaurorahealth.org/>.

⁹⁰ *Advocate Aurora notifies patients of potential tracking pixel breach*, HEALTHCARE IT NEWS (Oct. 20, 2022), <https://www.healthcareitnews.com/news/advocate-aurora-notifies-patients-potential-tracking-pixel-breach>.

1 hospital system had “disabled and/or removed the pixels from our platforms and launched
2 an internal investigation to better understand what patient information was transmitted to our
3 vendors.”⁹¹

4 217. Similarly, in October 2022, WakeMed notified more than 495,000 patients that their
5 Personal Health Information had been transmitted to Facebook through the use of tracking pixels
6 installed on its websites.⁹² In announcing this data breach, WakeMed admitted that the Facebook
7 Meta Pixel tool had been installed on its website resulting in the transmission of patient
8 information.⁹³ WakeMed further admitted that “[d]epending on the user’s activity, the data that may
9 have been transmitted to Facebook could have included information such as: email address, phone
10 number, and other contact information; computer IP address; emergency contact information;
11 information provided during online check-in, such as allergy or medication information; COVID
12 vaccine status; and information about an upcoming appointment, such as appointment type and date,
13 physician selected, and button/menu selections.”⁹⁴ WakeMed also conceded that it had no idea what
14 Facebook had done with the Personal Health Information that WakeMed had disclosed about its
15 patients.⁹⁵ Like the other hospital systems who have come clean about their use of the Meta Pixel
16 tool, WakeMed promised its patients that it had “proactively disabled Facebook’s pixel” and had
17 “no plans to use it in the future without confirmation that the pixel no longer has the capacity to
18 transmit potentially sensitive or identifiable information.”⁹⁶

19 218. In November 2022, the fallout from hospital systems’ use of the Meta Pixel tool
20 expanded when Community Health Network informed 1.5 million of its patients that their Personal
21

22 ⁹¹ *Advocate Aurora Health Data Breach Could Impact Up to 3 Million Patients*, HEALTHCARE
23 INNOVATION (Oct. 21, 2022) <https://www.hcinnovationgroup.com/cybersecurity/data-breaches/news/21284747/advocate-aurora-health-data-breach-could-impact-up-to-3-million-patients> (last accessed Jan. 9, 2025).

24 ⁹² *WakeMed Faces Data Breach Lawsuit Over Meta Pixel Use*, TECH TARGET,
25 <https://healthitsecurity.com/news/wakemed-faces-data-breach-lawsuit-over-meta-pixel-use>.

26 ⁹³ *WakeMed Notifies Patients of Potential Data Privacy Incident*, WAKEMED (Oct. 14, 2022),
27 <https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident>.

28 ⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ *Id.*

1 Health Information had been routinely transmitted and disclosed to Facebook since at least April
2 2017.⁹⁷

3 219. In its data breach notice, Community Health informed patients that “third-party
4 tracking technologies were installed on Community’s website.”⁹⁸ Community Health further
5 admitted that it had discovered that the configuration of certain technologies allowed for a broader
6 scope of information to be collected and transmitted to each corresponding third-party tracking
7 technology vendor (e.g., Facebook and Google) than Community had ever intended. Community
8 Health—like WakeMed, Novant, and Advocate Aurora Health—also promised it will begin
9 “working with our service providers to disable and/or remove certain technologies from our
10 websites and application”⁹⁹ Community Health, however, also conceded that it had no idea how
11 Facebook or other third parties had exploited the patient Personal Health Information that had been
12 disclosed to them via the pixel technology.

13 220. Unlike Community Health, WakeMed, Novant, Advocate Aurora Health, and other
14 responsible hospital systems who have informed their patients of the serious privacy violations
15 resulting from the installation of Facebook’s Meta Pixel tool on their websites, Defendant has done
16 nothing. Indeed, not only has Defendant hidden these privacy violations from its patients, but
17 Defendant continues to collect, transmit, and disclose its patients’ Personal Health Information to
18 Facebook despite widespread knowledge in the health care community that such collection and
19 disclosure of patient Personal Health Information is patently illegal and in violation of patients’
20 fundamental privacy rights.

21 221. As these data breach announcements demonstrate, there is widespread knowledge
22 within the health care community that installation of the Meta Pixel tool on hospital websites results
23 in the disclosure of patients’ Personal Health Information to Facebook. This is also widespread
24

25 ⁹⁷ Andrea Fox, *Community Health Network reports online tracking data breach affecting 1.5*
26 *million*, HEALTHCARE IT NEWS (Dec. 5, 2022)
27 <https://www.healthcareitnews.com/news/community-health-network-reports-online-tracking-data-breach-affecting-15-million>.

28 ⁹⁸ *Id.*

⁹⁹ *Id.*

1 recognition that such disclosures are not only illegal but fundamentally unethical, given the privacy
2 rights involved.

3 222. Defendant's decision to hide its use of the Meta Pixel tool from its patients and its
4 refusal to remove such technologies from its websites after learning that its patients' Personal Health
5 Information was being routinely collected, transmitted, and exploited by Facebook is malicious,
6 oppressive, and in reckless disregard of Plaintiffs' and Class Members' rights. Defendant's conduct
7 in intentionally concealing its use of the Meta Pixel tool from patients was knowing, willful, and
8 malicious. Defendant was aware that installing the Meta Pixel would result in the unauthorized
9 disclosure of its patients' personal health information to Facebook. Defendant nevertheless chose to
10 install the Meta Pixel on its website, while leading its patients to believe that their privacy rights
11 would be respected. Defendant's deception, including the significant misrepresentations made to
12 the public in its Privacy Practices was also fraudulent and oppressive. Despite promising patients
13 that it would never disclose their personal health information for marketing purposes without their
14 consent, Defendant routinely bartered its patients' personal health information to Facebook and
15 Google in return for advertising benefits.

16 **REPRESENTATIVE PLAINTIFFS' EXPERIENCE**

17 **Plaintiff John Doe I:**

18 223. Plaintiff John Doe I has gastrointestinal issues and a urologic condition arising from
19 an enlarged prostate. After becoming a Marin patient in 2020, Plaintiff began using Marin's
20 Websites regularly, including as recently as January 2024, to search for information related to his
21 sensitive medical treatments. Plaintiff entered data, including sensitive medical information, such
22 as details about his medical condition and search for a doctor.

23 224. Plaintiff has used the Websites to search for Marin doctors, schedule appointments,
24 review test results, and research medical treatment relating to his condition. All this information
25 was shared with Facebook and Google by Marin as a result of tracking pixels that Marin installed
26 on its Websites, including information about his urological issues along with personally identifying
27 information such as his Facebook ID, his device identifiers, his IP address and his browser
28 fingerprint.

1 225. Plaintiff also used Marin’s Websites to research healthcare providers (including
2 specialists and primary care providers) and communicate with them, research particular medical
3 conditions and treatments, fill out forms and questionnaires, schedule and attend appointments, and
4 perform other tasks related to his specific medical inquiries and treatment.

5 226. While using Marin’s digital services, Plaintiff communicated and received
6 information regarding his appointments, treatments, medications, and clinical information,
7 including his surgeries, ER visits, lab work, and scans. As a result of the Meta Pixel Defendant
8 chose to install on its Websites, this information was intercepted, viewed analyzed, and used by
9 unauthorized third parties.

10 227. Plaintiff accessed Marin’s Websites in connection with receiving healthcare services
11 from Marin or Marin’s affiliates at Marin’s direction and with Marin’s encouragement.

12 228. Plaintiff has used and continues to use the same devices to maintain and to access an
13 active Facebook account throughout the relevant period in this case.

14 229. As a medical patient using Marin’s health services, Plaintiff reasonably expected that
15 his online communications with Marin were solely between himself and Marin, and that such
16 communications would not be transmitted or intercepted by a third party. Plaintiff also relied on
17 Marin’s Privacy Policies in reasonably expecting Marin would safeguard his Private Information.
18 But for his status as Marin’s patient and its representations via its Privacy Policies, Plaintiff would
19 not have disclosed his Private Information to Marin.

20 230. Plaintiff is also an active Facebook user and has had a Facebook account while being
21 a Marin patient.

22 **Plaintiff John Doe II:**

23 231. Plaintiff John Doe II has been a Marin patient for over a decade, who has had concerns
24 about knee replacement, Parkinson’s disease, and systemic infections. Over the last five years
25 Plaintiff has used the Websites regularly to search for information related to his sensitive medical
26 treatments. Plaintiff entered data, including sensitive medical information, such as details about his
27 medical condition and search for a doctor.

1 232. Plaintiff has used the Websites to search for Marin doctors, schedule appointments,
2 review test results, and research medical treatment relating to his condition. All this information
3 was shared with Facebook and Google by Marin as a result of tracking pixels that Marin installed
4 on its Websites, including information about his urological issues along with personally identifying
5 information such as his device identifiers, his IP address and his browser fingerprint.

6 233. Plaintiff also used Marin's Websites to research healthcare providers (including
7 specialists and primary care providers) and communicate with them, research particular medical
8 conditions and treatments, fill out forms and questionnaires, schedule and attend appointments, and
9 perform other tasks related to his specific medical inquiries and treatment.

10 234. While using Marin's digital services, Plaintiff communicated and received
11 information regarding his appointments, treatments, medications, and clinical information,
12 including his surgeries, ER visits, lab work, and scans. As a result of the Meta Pixel Defendant
13 chose to install on its Websites, this information was intercepted, viewed analyzed, and used by
14 unauthorized third parties.

15 235. Plaintiff accessed Marin's Websites in connection with receiving healthcare services
16 from Marin or Marin's affiliates at Marin's direction and with Marin's encouragement.

17 236. Plaintiff has used and continues to use the same devices to maintain and to access an
18 active Facebook account throughout the relevant period in this case.

19 237. As a medical patient using Marin's health services, Plaintiff reasonably expected that
20 his online communications with Marin were solely between himself and Marin, and that such
21 communications would not be transmitted or intercepted by a third party. Plaintiff also relied on
22 Marin's Privacy Policies in reasonably expecting Marin would safeguard his Private Information.
23 But for his status as Marin's patient and its representations via its Privacy Policies, Plaintiff would
24 not have disclosed his Private Information to Marin.

25 **Plaintiff John Doe III:**

26 238. Plaintiff has a rare autoimmune condition and has been a patient at Marin's Greenbrae,
27 California location for many years. Plaintiff started using Marin's website over three years ago,
28 utilizing the Patient Portal many times in the recent years. Plaintiff has had a Facebook account for

over a decade, and suddenly started to receive unsolicited advertisements relating to his medical conditions shortly after visiting Marin Health's Properties.

239. Defendant encouraged Plaintiff to utilize Marin's website and online portal in order to search for doctors, make appointments, review medical treatments, and to review charts from previous exams.¹⁰⁰

240. While using Defendant's Websites, Plaintiff communicated sensitive – and what he expected to be confidential – personal and medical information to Defendant.

241. Plaintiff used Marin's Websites to research healthcare providers (including specialists and primary care providers) and communicate with them, research particular medical conditions (such as his rare autoimmune disease) and treatments, fill out forms and questionnaires, schedule and attend appointments, and perform other tasks related to his specific medical inquiries and treatment.

242. Plaintiff also utilized Marin's Patient Portal to refill prescriptions, look at his bills and payments, to see his test results and notes from his appointments and from his visits to the ER.

243. While using Marin's digital services, Plaintiff communicated and received information regarding his appointments, treatments, medications, and clinical information, including his surgeries, ER visits, lab work, and scans. As a result of the Meta Pixel Defendant chose to install on its Websites, this information was intercepted, viewed analyzed, and used by unauthorized third parties.

244. Plaintiff accessed Marin's Websites in connection with receiving healthcare services from Marin or Marin's affiliates at Marin's direction and with Marin's encouragement.

¹⁰⁰See, e.g., *MyChart – MarinHealth's Patient Portal* MARINHEALTH, <https://www.mymarinhealth.org/mychart/> ("Marin Health Medical Center and MarinHealth Medical Network Clinics are on a single medical record system. This powerful technology creates a seamless experience throughout your entire health journey, whether you are being seen in a clinic or at the hospital. Your providers can immediately access all of your health information in one place, so they can more informed decisions about your diagnosis and treatment plan, resulting in more coordinated care. As part of this medical record system, you'll have access to your health information in **MyChart**, our patient portal. You can complete pre-visit tasks, view test results, medication lists, upcoming appointments, medical bills, price estimates, and more all in one place using the app on your phone or computer").

1 245. Plaintiff has used and continues to use the same devices to maintain and to access an
2 active Facebook account throughout the relevant period in this case.

3 246. As a medical patient using Marin's health services, Plaintiff reasonably expected that
4 his online communications with Marin were solely between himself and Marin, and that such
5 communications would not be transmitted or intercepted by a third party. Plaintiff also relied on
6 Marin's Privacy Policies in reasonably expecting Marin would safeguard his Private Information.
7 But for his status as Marin's patient and its representations via its Privacy Policies, Plaintiff would
8 not have disclosed his Private Information to Marin.

9 247. Plaintiff is also an active Facebook user and has had a Facebook account since at least
10 2008.

11 **TOLLING, CONCEALMENT & ESTOPPEL**

12 248. The applicable statutes of limitation have been tolled as a result of Defendant's
13 knowing and active concealment and denial of the facts alleged herein.

14 249. Defendant secretly incorporated Meta Pixel into its Websites and patient portals,
15 providing no indication to Users that their User Data, including their Private Information, would be
16 disclosed to unauthorized third parties.

17 250. Defendant had exclusive knowledge that the Meta Pixel was incorporated on its
18 Websites, yet failed to disclose that fact to Users, or inform them that by interacting with its
19 Websites Plaintiffs' and Class Members' User Data, including Private Information, would be
20 disclosed to third parties, including Facebook.

21 251. Plaintiffs and Class Members could not with due diligence have discovered the full
22 scope of Defendant's conduct because the incorporation of Meta Pixels is highly technical and there
23 were no disclosures or other indications that would inform a reasonable consumer that Defendant
24 was disclosing and allowing Facebook to intercept Users' Private Information.

25 252. The earliest Plaintiffs and Class Members could have known about Defendant's
26 conduct was shortly before the filing of this Complaint.

CLASS ALLEGATIONS

254. **Class Definition:** Plaintiffs brings this action on behalf of themselves and on behalf the class of persons similarly situated, as defined below, Cal. Code Civ. Proc. Rule 382.:

The MarinHealth Class: Defendant’s patients, California citizens, and other members of the public, who visited Defendant’s Websites between August 1, 2019, through the date of preliminary approval.

256. Plaintiffs and Class Members satisfy the numerosity commonality, typicality, adequacy, and predominance requirements for suing as representative parties.

258. **Commonality:** Commonality requires that the Class Members' claims depend upon a common contention such that determination of its truth or falsity will resolve an issue that is central to the validity of each claim in one stroke. Here, there is a common contention for all Class Members as to whether Defendant disclosed to third parties their Private Information without authorization or lawful authority.

1 259. **Typicality:** Plaintiffs' claims are typical of the claims of other Class Members in that
2 Plaintiffs and the Class Members sustained damages arising out of Defendant's uniform wrongful
3 conduct and data sharing practices.

4 260. **Adequate Representation:** Plaintiffs will fairly and adequately represent and protect
5 the interests of the Class Members. Plaintiffs' claims are made in a representative capacity on behalf
6 of the Class Members. Plaintiffs have no interests antagonistic to the interests of the other Class
7 Members. Plaintiffs have retained competent counsel to prosecute the case on behalf of Plaintiffs
8 and the Class. Plaintiffs and Plaintiffs' counsel are committed to vigorously prosecuting this action
9 on behalf of the Class members.

10 261. The declaratory and injunctive relief sought in this case includes, but is not limited to:

- 11 a. Entering a declaratory judgment against Defendant—declaring that Defendant's
12 interception of Plaintiffs' and Class Members' Private Information among themselves
13 and other third parties is in violation of the law;
- 14 b. Entering an injunction against Defendant:
- 15 i. preventing Defendant from sharing Plaintiffs' and Class Members' Private
16 Information among themselves and other third parties;
- 17 ii. requiring Defendant to alert and/or otherwise notify all users of its Websites
18 and portals of what information is being collected, used, and shared;
- 19 iii. requiring Defendant to provide clear information regarding its practices
20 concerning data collection from the users/patients of Defendant's Websites, as
21 well as uses of such data;
- 22 iv. requiring Defendant to establish protocols intended to remove all personal
23 information which has been leaked to Facebook and/or other third parties, and
24 request Facebook/third parties to remove such information;
- 25 v. and requiring Defendant to provide an opt out procedure for individuals who
26 do not wish for their information to be tracked while interacting with
27 Defendant's Websites.
- 28

262. **Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and Class Members, and those questions predominate over any questions that may affect individual Class Members. Common questions and/or issues for Class members include, but are not necessarily limited to the following:

- c. Whether Defendant's acts and practices violated California's Constitution, Art. 1, § 1;
- d. Whether Defendant's acts and practices violated California's Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*;
- e. Whether Defendant's acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;
- f. Whether Defendant's represented to Plaintiffs and the Class that it would protect Plaintiffs' and the Class Members' Private Information;
- g. Whether Defendant violated Plaintiffs' and Class Members' privacy rights;
- h. Whether Defendant's practices violated California's Confidentiality of Medical Information Act, Civ. Code §§ 56, *et seq.*;
- i. Whether Defendant's practices violated California's Constitution, Art. 1, § 1;
- j. Whether Plaintiffs and Class Members are entitled to actual damages, enhanced damages, statutory damages, and other monetary remedies provided by equity and law;
- k. Whether injunctive and declaratory relief, restitution, disgorgement, and other equitable relief is warranted.

263. **Superiority:** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by individual Class Members will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual Class Members to obtain effective relief from Defendant's misconduct. Even if Class Members could mount such individual litigation, it would still not be

1 preferable to a class action, because individual litigation would increase the delay and expense to
2 all parties due to the complex legal and factual controversies presented in this Complaint. By
3 contrast, a class action presents far fewer management difficulties and provides the benefits of single
4 adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of
5 time, effort and expense will be enhanced, and uniformity of decisions ensured.

6 264. Likewise, particular issues are appropriate for certification because such claims
7 present only particular, common issues, the resolution of which would advance the disposition of
8 this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- 9 a. Whether Defendant misrepresented that it would disclose personal information
10 only for limited purposes that did not include purposes of delivering
11 advertisements or collecting data for commercial use or supplementing
12 consumer profiles created by data aggregators and advertisers;
- 13 b. Whether Defendant's privacy policies misrepresented that it collected and
14 shared User information with third-party service providers only for the limited
15 purpose of providing access to its services;
- 16 c. Whether Defendant misrepresented that it had in place contractual and technical
17 protections that limit third-party use of User information and that it would seek
18 User consent prior to sharing Private Information with third parties for purposes
19 other than provision of its services;
- 20 d. Whether Defendant misrepresented that any information it receive is stored
21 under the same guidelines as any health entity that is subject to the strict patient
22 data sharing and protection practices set forth in the regulations propounded
23 under HIPAA;
- 24 e. Whether Defendant misrepresented that it complied with HIPAA's requirements
25 for protecting and handling Users' PHI;
- 26 f. Whether Defendant shared the Private Information that Users provided to
27 Defendant with advertising platforms, including Facebook, without adequate
28

notification or disclosure, and without Users' consent, in violation of health privacy laws and rules and its own privacy policy;

- g. Whether Defendant integrated third-party tracking tools, consisting of automated web beacons ("**Pixels**") in its Websites that shared Private Information and User activities with third parties for unrestricted purposes, which included advertising, data analytics, and other commercial purposes;
- h. Whether Defendant shared Private Information and activity information with Facebook using Facebook's tracking Pixels on its Websites without Users' consent;
- i. Whether Facebook used the information that Defendant shared with it for unrestricted purposes, such as selling targeted advertisements, data analytics, and other commercial purposes.

COUNT ONE

VIOLATION OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA"), CAL. CIV. CODE §§ 56, *et seq.*

265. Plaintiffs incorporate paragraphs and herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

266. Defendant is subject to the CMIA pursuant to California Civil Code § 56.10 because it is a "provider of health care" as defined by California Civil Code § 56.06(b); it operates hospitals, provides health care, maintains medical information, offers software to consumers designed to maintain medical information for the purposes of communications with doctors, receipt of diagnosis, treatment, or management of medical conditions.

267. Section 56.10 states, in pertinent part, that "[n]o provider of health care . . . shall disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization"

268. Section 56.101 of the CMIA states, in pertinent part, that "[a]ny provider of health care . . . who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of

1 medical information shall be subject to the remedies and penalties . . .” Cal. Civ. Code §§ 56.10,
2 56.101.

3 269. Plaintiffs’ and Class Members’ Private Information constitutes “medical
4 information” under the CMIA because it consists of individually identifiable information in
5 possession of and derived from a provider of healthcare regarding Plaintiffs’ and Class Members’
6 medical history, test results, mental or physical condition, and/or treatment.

7 270. Defendant violated Cal. Civ. Code § 56.10 because it failed to maintain the
8 confidentiality of Users’ medical information, and instead “disclose[d] medical information
9 regarding a patient of the provider of health care or an enrollee or subscriber of a health care service
10 plan without first obtaining an authorization” by soliciting, intercepting, and receiving Plaintiffs’
11 and Class Members’ Private Information, and sharing it with advertisers and for advertising
12 purposes. Specifically, Defendant knowingly, or willfully, disclosed Plaintiffs’ and Class Members’
13 medical information to Facebook, allowing Facebook to now advertise and target Plaintiffs and
14 Class Members, misusing their extremely sensitive Private Information.

15 271. Defendant violated Cal. Civ. Code § 56.101 because it knowingly, or willfully, failed
16 to create, maintain, preserve, store, abandon, destroy, and dispose of medical information in a
17 manner that preserved its confidentiality by soliciting, intercepting, and receiving Plaintiffs’ and
18 Class Members’ Private Information, and sharing it with advertisers and for advertising purposes
19 for Facebook’s and Defendant’s financial gain.

20 272. Defendant intentionally embedded Facebook Pixels, which facilitates the
21 unauthorized sharing of Plaintiffs’ and Class Members’ medical information.

22 273. Defendant violated Cal Civ. Code § 56.36(b) because they released confidential
23 information and records concerning Plaintiffs and Class Members in violation of their rights under
24 the CMIA.

25 274. As a direct and proximate result of Defendant’s misconduct, Plaintiffs and Class
26 Members had their private communications containing information related to their sensitive and
27 confidential Private Information intercepted, disclosed, and used by third parties.
28

275. As a result of Defendant's unlawful conduct, Plaintiffs and Class Members suffered an injury, including violation to their rights of privacy, loss of the privacy of their Private Information, loss of control over their sensitive personal information, and suffered aggravation, inconvenience, and emotional distress.

276. Plaintiffs and Class Members are entitled to: (a) nominal damages of \$1,000 per violation; (b) actual damages, in an amount to be determined at trial; (c) reasonable attorneys' fees, and costs.

COUNT TWO

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ("CIPA"), CAL. PENAL CODE § 630, *et seq.*

277. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

278. Defendant is a person for purposes of Cal. Penal Code §631.

279. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, (1978) 22 Cal. 3d 187, 192-93. Thus, to establish liability under CIPA § 631(a), a Plaintiffs need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following: (1) "intentionally taps, or makes any unauthorized connection...with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system," (2) "willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication 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 [the state of California]," (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained," or (4) **aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section** (emphasis added).

280. Section 631(a) is not limited to phone lines, but also applies to “new technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic communications”); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook’s collection of consumers’ Internet browsing history).

281. Defendant’s Websites are a “machine, instrument, contrivance, or ... other manner” used to engage in the prohibited conduct at issue here.

282. At all relevant times, Defendant entered into contracts with Facebook, in order to track certain activities on its Websites. Defendant allowed Facebook to intercept and otherwise track Users’ clicks, communications, searches, and other User activities. Defendant’s activated Facebook Pixel tracking tools, allowing Facebook to intentionally tap, and make unauthorized connections with, the lines of internet communication between Plaintiffs and Class Members on the one hand, and Defendant’s Websites on the other hand, without consent of all parties to the communication.

283. At all relevant times, by using the Facebook Pixel, Facebook willfully and without the consent of Plaintiffs and Class Members, read or attempted to learn the contents or meaning of electronic communications of Plaintiffs and putative Class Members on Defendant’s Websites. This occurred while the electronic communications were in transit or passing over any wire, line, or cable, or were being sent from or received at any place within California. Facebook intercepted Plaintiffs’ and Class Members’ communications – including the very terms and phrases they typed into the search bar – without their authorization or consent.

284. By embedding Facebook Pixels on its websites, Defendant aided, agreed with, employed, and conspired with Facebook to wiretap consumers communications on Defendant’s Websites using the Facebook Pixel snipped codes and to accomplish the wrongful conduct at issue here.

285. Plaintiffs and Class Members did not consent to the interception, reading, learning, recording, and collection of their electronic communications with Defendant. Accordingly, the interception was unlawful and tortious.

286. The violation of section 631(a) constitutes an invasion of privacy sufficient to confer Article III standing.

287. Unless enjoined, Defendant will continue to commit the illegal acts alleged here. Plaintiffs continues to be at risk because he frequently uses Defendant's Websites to search for information about medical products, health conditions or services. Plaintiffs continues to desire to use the Defendant's Websites for that purpose, including but not limited to investigating health conditions (e.g., diabetes), diagnoses (e.g., COVID-19), procedures, test results, treatment status, the treating physician, medications, and/or allergies.

288. Plaintiffs and Class Members may or are likely to visit Defendant's Websites in the future but have no practical way of knowing whether their website communications will be collected, viewed, accessed, stored, and used by Facebook.

289. Plaintiffs and Class Members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of \$5,000 per violation.

COUNT THREE

VIOLATION OF THE UNFAIR COMPETITION LAW (“UCL”)

CALIFORNIA BUSINESS AND PROFESSIONS CODE § 17200, et seq.

290. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

A. Unlawful Prong

291. Defendant's conduct as alleged herein was unfair within the meaning of the UCL. The unfair prong of the UCL prohibits unfair business practices that either offend an established public policy or that are immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers.

292. Defendant's conduct, as alleged herein, was also fraudulent within the meaning of the UCL. Defendant made deceptive misrepresentations and omitted known material facts in connection

1 with the solicitation, interception, disclosure, and use of Plaintiffs' and Class Members' Private
2 Information. Defendant actively concealed and continued to assert misleading statements regarding
3 its protection and limitation on the use of Private Information. Meanwhile, Defendant was collecting
4 and sharing Plaintiffs' and Class Members' Private Information without their authorization or
5 knowledge to profit off of the information and deliver targeted advertisements to Plaintiffs and Class
6 Members, among other unlawful purposes.

7 293. Defendant's conduct, as alleged herein, was unlawful within the meaning of the UCL
8 because it violated regulations and laws as discussed herein, including but not limited to HIPAA,
9 Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the California
10 Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq.*

11 294. Had Plaintiffs and Class Members known Defendant would disclose and misuse their
12 Private Information in contravention of Defendant's representations, they would never have used
13 Defendant's website or its MyChart portal and would not have shared their Private Information.

14 295. Defendant's unlawful actions in violation of the UCL have caused and are likely to
15 cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that
16 is not outweighed by countervailing benefits to consumers or competition.

17 296. As a direct and proximate result of Defendant's misconduct, Plaintiffs and Class
18 Members had their private communications containing information related to their sensitive and
19 confidential Private Information intercepted, disclosed, and used by third parties, including but not
20 limited to Facebook.

21 297. As a result of Defendant's unlawful conduct, Plaintiffs and Class Members suffered
22 an injury, including violation to their rights of privacy, loss of value and privacy of their Private
23 Information, loss of control over their sensitive personal information, and suffered embarrassment
24 and emotional distress as a result of this unauthorized sharing of information.

25 **B. Unfair Prong**

26 298. Defendant engaged in unfair business practices by disclosing Plaintiffs' and Class
27 Members' Private Information to unrelated third parties, including Facebook, without prior consent
28 despite its promises to keep such information confidential.

1 299. Defendant's unfair business practices included widespread violations of Plaintiffs'
2 and Class Members' rights to privacy, including its failure to inform the public that using its
3 Websites would result in disclosure of highly private information to third parties.

4 300. Because Defendant is in the business of providing medical and mental healthcare
5 services, Plaintiffs and Class Members relied on Defendant to advise them of any potential
6 disclosure of their Private Information.

7 301. Plaintiffs and Class Members were entitled to assume, and did assume, that Defendant
8 would take appropriate measures to keep their Private Information secure and confidential. At no
9 point did Plaintiffs expect to become a commodity on which Defendant and Facebook would trade.

10 302. Plaintiffs and Class Members reasonably relied upon the representations Defendant
11 made in its Privacy Policy, including those representations concerning the confidentiality of Private
12 Information, such as patient health information.

13 303. Defendant was in sole possession of and had a duty to disclose the material
14 information that Plaintiffs and Class Members' private information was being shared with third
15 parties.

16 304. Had Defendant disclosed that it shared Private Information with third parties,
17 Plaintiffs and the Class would not have used Defendant's services at the level they did.

18 305. The harm caused by Defendant's conduct outweighs any potential benefits
19 attributable to such conduct and there were reasonably available alternatives to further Defendant's
20 legitimate business interests other than Defendant's conduct described herein.

21 306. Defendant's acts, omissions and conduct also violate the unfair prong of the UCL
22 because those acts, omissions and conduct offended public policy (including the aforementioned
23 federal and state privacy statutes and state consumer protection statutes, such as HIPAA), and
24 constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury,
25 including to Plaintiffs and Class Members.

26 307. As a direct result of Plaintiffs' and Class Members' reliance on Defendant's
27 representations that Defendant would keep their Private Information confidential and Defendant's
28 express representation that it would not share Private Information with third parties without the

1 Users' express consent, Plaintiffs and Class Members shared highly sensitive information through
2 their use of the Websites, causing them to suffer damages when Defendant disclosed said
3 information to a third party.

4 308. As a direct result of Defendant's violations of the UCL, Plaintiffs and Class Members
5 have suffered injury in fact and lost money or property, including but not limited to payments to
6 Defendant and/or other valuable consideration. The unauthorized access to Plaintiffs' and Class
7 Members' private and personal data also diminished the value of that Private Information.

8 309. As a direct result of its unfair practices, Defendant has been unjustly enriched and
9 should be required to make restitution to Plaintiffs and Class Members pursuant to §§ 17203 and
10 17204 of the California Business & Professions Code, disgorgement of all profits accruing to
11 Defendant because of its unlawful business practices, declaratory relief, attorney's fees and costs
12 (pursuant to Cal. Code Civ. Proc. §1021.5) and injunctive or other equitable relief.

13 **COUNT FOUR**

14 **INVASION OF PRIVACY UNDER CALIFORNIA CONSTITUTION, ART. I, § 1.**

15 310. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set
16 forth herein.

17 311. Art. I, § 1 of the California Constitution provides: "All people are by nature free and
18 independent and have inalienable rights. Among these are enjoying and defending life and liberty,
19 acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and
20 privacy." Cal. Const., Art. I, § 1.

21 312. The right to privacy in California's Constitution creates a private right of action
22 against private and government entities.

23 313. Plaintiffs and Class Members have and continue to have a reasonable expectation of
24 privacy and interest in: (1) precluding the dissemination and/or misuse of their sensitive,
25 confidential communications and protected health information; and (2) making personal decisions
26 and/or conducting personal activities without observation, intrusion or interference, including, but
27 not limited to, the right to visit and interact with various internet sites without being subjected to
28 wiretaps without their knowledge, authorization, or consent.

1 314. At all relevant times, by using Facebook’s Meta Pixel to record and communicate
2 patients’ FIDs and other individually identifying information alongside their confidential medical
3 communications, Defendant invaded Plaintiffs’ and Class Members’ privacy rights under the
4 California Constitution.

5 315. Plaintiffs and Class Members had a reasonable expectation that their
6 communications, identity, health information, and other data would remain confidential, and that
7 Defendant would not install wiretaps on its Websites to secretly transmit communications to a third
8 party.

9 316. Plaintiffs and Class Members did not authorize the Defendant to record and transmit
10 their Private Information – including private medical communications alongside their personally
11 identifiable health information – to a third party, Facebook. *See* Figures 2-9 of Defendant’s Websites
12 above.

13 317. This invasion of privacy is serious in nature, scope, and impact because it relates to
14 patients’ private medical communications. Moreover, it constitutes an egregious breach of the
15 societal norms underlying the privacy right.

16 318. As a result of the Defendant’s actions, Plaintiffs and Class Members have suffered
17 harm and injury, including but not limited to an invasion of their privacy rights.

18 319. Plaintiffs and Class Members have been damaged as a direct and proximate result of
19 the Defendant’s invasion of their privacy and are entitled to just compensation, including monetary
20 damages.

21 320. Plaintiffs and Class Members seek appropriate relief for their injuries, including but
22 not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm
23 to their privacy interests as a result of the intrusion(s) upon Plaintiffs’ and Class Members’ privacy.

24 321. Plaintiffs and Class Members are also entitled to punitive damages resulting from the
25 malicious, willful, and intentional nature of the Defendant’s conduct, injuring Plaintiffs and Class
26 Members in conscious disregard of their rights.

27 322. Plaintiffs seek all other relief as the Court may deem just, proper, and available for
28 invasion of privacy under the California Constitution, on behalf of the Class.

COUNT FIVE
INVASION OF PRIVACY
INTRUSION UPON SECLUSION

323. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

324. Plaintiffs and Class Members had a reasonable and legitimate expectation of privacy in the Private Information that Defendant failed to adequately protect against disclosure from unauthorized parties.

325. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

326. Defendant failed to protect, and instead released to unknown and unauthorized third parties, the Private Information of Plaintiffs and Class Members.

327. By failing to keep Plaintiffs' and Class Members' Private Information confidential and safe from misuse, Defendant knowingly shared highly sensitive Private Information with Facebook, Defendant unlawfully invaded Plaintiffs' and Class Members' privacy by, among others: (i) intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons; and (iii) enabling and facilitating the disclosure of Plaintiffs' and Class Members' Private Information without authorization or consent.

328. Plaintiffs' and Class Members' expectation of privacy was and is especially heightened given Defendant's consistent representations that Users' information would remain confidential and would not be disclosed to anyone without User consent.

329. Defendant's privacy policy specifically provides, "We will not sell or otherwise provide the information we collect to outside third parties for the purpose of direct or indirect mass email marketing."¹⁰¹

330. Defendant knew, or acted with reckless disregard, of the fact that a reasonable person in Plaintiffs' and Class Members' position would consider its actions highly offensive.

¹⁰¹ *Notice of Privacy Policy, supra* note 42.

334. Plaintiffs seek injunctive relief on behalf of the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiffs and Class Members. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

BREACH OF IMPLIED CONTRACT

338. Plaintiffs and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them that included Defendant's promise not to disclose Private Information without consent.

1 339. Defendant breached these implied contracts by disclosing Plaintiffs' and Class
2 Members' Private Information to third parties, including Facebook.

3 340. As a direct and proximate result of Defendant's breaches of these implied contracts,
4 Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members
5 would not have used Defendant's services, or would have paid substantially less for these services,
6 had they known their Private Information would be disclosed.

7 341. Plaintiffs and Class Members are entitled to compensatory and consequential damages
8 as a result of Defendant's breach of implied contract.

9 **COUNT SEVEN**

10 **LARCENY/RECEIPT OF STOLEN PROPERTY (VIOLATION OF CALIFORNIA**
11 **PENAL CODE § 496(a) and (c))**

12 342. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set
13 forth herein and bring this claim individually and on behalf of the proposed Class.

14 343. Courts recognize that internet users have a property interest in their personal
15 information and data. *See Calhoun v. Google, LLC*, (N.D. Cal. Mar. 17, 2021) 526 F. Supp. 3d 605,
16 at *21 (recognizing property interest in personal information and rejecting Google's argument that
17 "the personal information that Google allegedly stole is not property"); *In re Experian Data Breach*
18 *Litigation*, (C.D. Cal. Dec. 29, 2016) 2016 U.S. Dist. LEXIS 184500, at *5 (loss of value of PII is
19 a viable damages theory); *In re Marriott Int'l Inc. Customer Data Sec. Breach Litig.*, (D. Md. 2020)
20 440 F. Supp. 3d 447, 460 ("The growing trend across courts that have considered this issue is to
21 recognize the lost property value of this [personal] information."); *Simona Opris v. Sincera*, (E.D.
22 Pa. 2022) 2022 U.S. Dist. LEXIS 94192, at *20 (collecting cases).

23 344. Cal. Penal Code §496(c) permits "any" person who has been injured by a violation
24 of section 496(a) to recover three times the amount of actual damages, costs of suit and attorney's
25 fees in a civil suit.

26 345. Penal Code § 496(a) creates an action against "any" person who (1) receives "any"
27 property that has been stolen or obtained in any manner constituting theft, knowing the property to
28

1 be stolen or obtained, or (2) conceals, sells, withholds, or aids in concealing or withholding “any”
2 property from the owner, knowing the property to be so stolen or illegally obtained.

3 346. Under Penal Code § 1.07(a)(38), “person” means “an individual, corporation, or
4 association.” Thus, Defendant is a person under section 496(a).

5 347. As set forth herein, the Users’ Private Information was stolen or obtained by theft,
6 without limitation, under Penal Code §484, by false or fraudulent representations or pretenses. At
7 no point did the Defendant have Plaintiffs’ and Class Members’ consent to duplicate their searches
8 and send them to Facebook.

9 348. Defendant meets the grounds for liability of section 496(a) because they, and each of
10 them:

- 11 a. knew the Private Information was stolen or obtained by theft and/or false
12 pretenses; and, with such knowledge,
- 13 b. transmitted such information to unauthorized third parties, like Facebook.

14 349. Defendant violated the second ground for liability of section 496(a) because they, and
15 each of them:

- 16 a. knew the Private Information was stolen or obtained by theft; and, with such
17 knowledge,
- 18 b. concealed, withheld, or aided in concealing or withholding said data from their
19 rightful owners by unlawfully tracking the data and disclosing it to unauthorized
20 third parties, like Facebook.

21 350. As a direct and proximate result of the acts and omissions described above, Plaintiffs
22 and Class Members were injured by the Defendant’s violations of section 496(a).

23 351. Pursuant to California Penal Code § 496(c), the Plaintiffs and Class Members seek
24 actual damages, treble damages, costs of suit, and reasonable attorneys’ fees.

25 **COUNT EIGHT**

26 **QUASI-CONTRACT/RESTITUTION/UNJUST ENRICHMENT**

27 352. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.
28

1 353. “Common law principles of restitution require a party to return a benefit when the
2 retention of such benefit would unjustly enrich the recipient; a typical cause of action involving
3 such remedy is ‘quasi-contract.’” *Munoz v. MacMillan* (2011) 195 Cal. App. 4th 648, 661, 124 Cal.
4 Rptr. 3d 664; *see also City of Oakland v. Oakland Raiders* (2022) 83 Cal. App. 5th 458, 299 Cal. Rptr.
5 3d 463, 478.

6 354. By virtue of the unlawful, unfair and deceptive conduct alleged herein, Defendant
7 knowingly realized hundreds of millions of dollars in revenue from the use of the Private
8 Information of Plaintiffs and Classes Members for profit by way of targeted advertising related to
9 Users’ respective medical conditions and treatments sought.

10 355. This Private Information, the value of the Private Information, and/or the attendant
11 revenue, were monetary benefits conferred upon Defendant by Plaintiffs and Class Members.

12 356. As a result of Defendant’s conduct, Plaintiffs and Class Members suffered actual
13 damages in the loss of value of their Private Information and the lost profits from the use of their
14 Private Information.

15 357. It would be inequitable and unjust to permit Defendant to retain the enormous
16 economic benefits (financial and otherwise) it has obtained from and/or at the expense of Plaintiffs
17 and Class Members.

18 358. Defendant will be unjustly enriched if it is permitted to retain the economic benefits
19 conferred upon them by Plaintiffs and Class Members through Defendant’s obtaining the Private
20 Information and the value thereof, and profiting from the unlawful, unauthorized, and impermissible
21 use of the Private Information of Plaintiffs and Class Members.

22 359. Plaintiffs and Class Members are therefore entitled to recover the amounts realized by
23 Defendant at the expense of Plaintiffs and Class Members.

24 360. Plaintiffs and the Class Members have no adequate remedy at law and are therefore
25 entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the
26 amount of Defendant’s ill-gotten gains, and/or other sums as may be just and equitable.

27 ///

28 ///

COUNT NINE

VIOLATION OF THE COMPREHENSIVE COMPUTER

DATA ACCESS AND FRAUD ACT

(CAL. PENAL CODE § 502)

361. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein and bring this claim individually and on behalf of the proposed Class.

362. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502 (“CDAFA”) to “expand the degree of protection . . . from tampering, interference, damage, and unauthorized access to [including the extraction of data from] lawfully created computer data and computer systems,” finding and declaring that “the proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and computer data,” and that “protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals . . .” Cal. Penal Code§ 502(a).

363. Under CDAFA, any person who “[k]nowingly accesses and without permission . . . uses any data . . . or computer system in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data” is “guilty of a public offense.” Cal. Penal Code§ 502(c)(1).

364. Plaintiffs’ and the Class Members’ devices on which they accessed the hospital or patient portals, including their computers, smart phones, and tablets, constitute computers or “computer systems” within the meaning of CDAFA. Cal. Penal Code§ 502(b)(5).

365. Defendant violated section 502, subsection (c)(1)(A) by knowingly using data obtained from their patients as part of a scheme to defraud and deceive patients into surrendering their Personal Health Information so that Defendant could then barter that information to third parties like Facebook in return for economic benefits. Defendant violated section 502, subsection (c)(1)(B) by knowingly using data obtained from their patients to wrongfully obtain financial benefits from third parties like Facebook and Google by bartering patients’ Personal Health

1 Information to those companies. Neither Plaintiffs nor Class Members ever gave Defendant
2 permission to disclose their Personal Health Information to third parties like Facebook and Google.

3 366. Defendant also violated section 502, subsection (c)(1)(B), of CDAFA by knowingly
4 accessing without permission Plaintiffs' and Class Members' devices in order to wrongfully obtain
5 and use their personal data, including their sensitive medical information, in violation of Plaintiffs'
6 and Class Members' reasonable expectations of privacy in their devices and data. Defendant
7 achieved this by installing software code on its website that directed patients' browsers to send
8 copies of their communications to third parties like Facebook and Google without their consent.

9 367. Defendant violated California Penal Code section 502, subsection (c)(2), by
10 knowingly and without permission accessing, taking, copying, and making use of Plaintiffs and the
11 Class Members' personally identifiable information, including their sensitive medical information
12 as part of a scheme to barter patients' Personal Health Information to third parties like Facebook
13 and Google in return for advertising benefits.

14 368. Defendant violated California Penal Code section 502, subsection (c)(6) by
15 knowingly and without permission providing or assisting third parties like Facebook and Google
16 with a means of accessing Plaintiffs and Class Members' computer systems.

17 369. The computers that Plaintiffs and Class Members used when accessing Defendant's
18 website all have and operate "computer services" within the meaning of CDAFA. Defendant
19 violated §§ 502(c)(3) and (7) of CDAFA by knowingly and without permission accessing and using
20 those devices and computer services, and/or causing them to be accessed and used, *inter alia*, in
21 connection with Facebook's wrongful collection of such data.

22 370. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any set
23 of computer instructions that are designed to . . . record, or transmit information within a computer,
24 computer system, or computer network without the intent or permission of the owner of the
25 information." Defendant violated § 502(c)(8) by knowingly and without permission introducing a
26 computer contaminant via Meta Pixel embedded into the hospital website which intercepted
27 Plaintiff's and the Class Members' private and sensitive medical information.
28

1 371. Defendant's breach caused Plaintiffs and Class Members, at minimum, the following
2 damages:

- 3 a. Sensitive and confidential information that Plaintiffs and Class Members
4 intended to remain private is no longer private;
- 5 b. Defendant eroded the essential confidential nature of the doctor-patient
6 relationship;
- 7 c. Defendant took something of value from Plaintiffs and Class Members and
8 derived benefit therefrom without Plaintiffs' and Class Members' knowledge or
9 informed consent and without sharing the benefit of such value;
- 10 d. Plaintiffs and Class Members did not get the full value of the medical services
11 for which they paid, which included Defendant's duty to maintain
12 confidentiality; and
- 13 e. Defendant's actions diminished the value of Plaintiffs and Class Members'
14 personal information

15 372. Plaintiffs and Class Members also seek such other relief as the Court may deem
16 equitable, legal, and proper.

17 373. Plaintiffs and the Class Members seek compensatory damages in accordance with Cal.
18 Penal Code § 502(e)(1), in an amount to be proved at trial, and injunctive or other equitable relief.
19 Plaintiffs continue to desire to search for health information on Marin Health's website. They will
20 continue to suffer harm if the website is not redesigned. If the website were redesigned to comply
21 with applicable laws, Plaintiffs would use the Marin Health's website to search for health
22 information in the future.

23 374. Plaintiffs and Class Members are entitled to punitive or exemplary damages pursuant
24 to Cal. Penal Code§ 502(e)(4) because Defendant's violations were willful and, upon information
25 and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294

26 375. Plaintiffs and the Class Members are also entitled to recover their reasonable
27 attorney's fees under§ 502(e)(2).

28 ///

COUNT TEN

VIOLATION OF CAL. CIVIL CODE § 1798.82

376. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein and bring this claim individually and on behalf of the proposed Class.

377. California Civil Code § 1798.82(a) provides that “[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California . . . whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

378. For purposes of the statute, “personal information” means “[a]n individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: . . . (D) Medical information.” Cal. Civil Code § 1798.82.

379. For purposes of the statute, “medical information” means “any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.”

380. Any customer who is injured by a violation of the statute may institute a civil action to recover damages. Cal. Civil Code § 1798.84(b). Further, any business that violates, proposes to violate, or has violated this statute may be enjoined. Cal. Civ. Code § 1798.84(e).

381. Defendant failed to disclose to Plaintiffs and the Class that it was regularly collecting, transmitting, and sharing patients’ unencrypted medical information with Facebook and other third parties so that these third parties could target them with advertising. Along with its patients’ medical information, Defendant also disclosed its patients’ first names (or first initial and last name) to, for example, Facebook via encrypted data transmissions, including the unauthorized transmission of patients’ Facebook IDs to Facebook, which permitted Facebook to link the medical information provided with the personal identities of Plaintiffs and the Class Members.

382. Defendant willfully, intentionally, and/or recklessly failed to provide the disclosures required by California Civil Code section 1798.82 as part of a scheme to barter Plaintiffs’ and Class

Members' Personal Health Information to Facebook and other third parties in return for access to tracking tools like the Meta Pixel tool.

383. Plaintiffs and Class Members conferred a benefit on Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from Facebook and other third parties. Defendant had knowledge that Plaintiffs and Class Members had conferred this benefit on Defendant by interacting with their website, and Defendant intentionally installed the Meta Pixel tool on its website to capture and monetize this benefit conferred by Plaintiffs and Class Members.

384. Plaintiffs and Class Members also conferred a benefit on Defendant by paying Defendant for health care services, which included Defendant's obligation to protect Plaintiffs and Class Members' Personal Health Information. Defendant was aware of receiving these payments from Plaintiffs and Class Members and demanded such payments as a condition of providing treatment.

385. Plaintiffs and Class Members would not have used the Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to Facebook. The services that Plaintiffs and Class Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide.

386. The medical services that Defendant offers are available from many other healthcare systems who do protect the confidentiality of patient communications. Had Defendant disclosed that it would allow third parties to secretly collect Plaintiffs' and Class Members' medical information without consent, neither Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or their affiliated healthcare providers.

387. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class Members because Defendant's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs and Class Members.

1 388. Plaintiffs and Class Members were damaged by Defendant's failure to inform them
2 that their Personal Health Information was being shared with Facebook, resulting in, at minimum,
3 the following damages:

- 4 a. Sensitive and confidential information that Plaintiffs and Class Members
5 intended to remain private is no longer private;
- 6 b. Defendant eroded the essential confidential nature of the doctor-patient
7 relationship;
- 8 c. Defendant took something of value from Plaintiffs and Class Members and
9 derived benefit therefrom without Plaintiffs' and Class Members' knowledge
10 or informed consent and without sharing the benefit of such value;
- 11 d. Plaintiffs and Class Members did not get the full value of the medical services
12 for which they paid, which included Defendant's duty to maintain
13 confidentiality; and
- 14 e. Defendant's actions diminished the value of Plaintiffs and Class Members'
15 personal information

16 389. Plaintiffs also continue to desire to search for health information on Marin Health's
17 website. They will continue to suffer harm if Defendant does not make adequate disclosures regarding
18 which third party marketing companies are receiving Plaintiffs' and Class Members' protected
19 health information. Plaintiffs and the Class Members are therefore also entitled to injunctive relief
20 requiring Defendant to comply with Cal. Civ. Code § 1798.82.

21 **COUNT ELEVEN**

22 **VIOLATIONS OF CAL. CIVIL CODE §§ 1709 & 1710**

23 390. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set
24 forth herein and bring this claim individually and on behalf of the proposed Class.

25 391. California Civil Code § 1709 provides that "[o]ne who willfully deceives another with
26 intent to induce him to alter his position to his injury or risk, is liable for any damage which he
27 thereby suffers."

28 ///

1 392. California Civil Code§ 1710 defines “deceit” as (1) the suggestion, as a fact, of that
2 which is not true, by one who does not believe it to be true; (2) the assertion, as a fact, of that which
3 is not true, by one who has no reasonable ground for believing it to be true; (3) the suppression of a
4 fact, by one who is bound to disclose it, or who gives information of other facts which are likely to
5 mislead for want of communication of that fact; or (4) a promise, made without any intention of
6 performing it.

7 393. Throughout the class period, Marin Health engaged in deceit by intentionally
8 concealing and failing to disclose the true nature of its Web Properties and conduct to patients and
9 prospective patients. Marin Health knew that representations made within its privacy notices were
10 misleading and material and that the facts Marin Health failed to disclose were material.

11 394. Marin Health owed a duty to Plaintiffs and the Class to provide them material
12 information about its acquisition and use of the Personal Health Information that Marin Health
13 invited them to share through its website and patient portal. Marin Health’s omissions and
14 nondisclosures described herein were likely to deceive reasonable consumers, and have deceived
15 Plaintiffs and the Class. Marin Health’s acts of deceit include without limitation the following:
16 Marin Health installed source code on its website and patient portal that surreptitiously captured and
17 transmitted patients’ communications to third party tech companies, including Facebook and
18 Google. Marin Health suppressed these facts while under a duty to disclose them.

19 395. Marin Health’s omissions and nondisclosures were pervasive. Plaintiffs and Class
20 Members reasonably relied on the material omissions and nondisclosures by Marin Health.

21 396. Marin Health’s misconduct alleged herein was intentional, deliberate, and willful, and
22 was perpetrated with the intent to, inter alia, cause Plaintiffs and the California Class members
23 unknowingly to divulge confidential login credentials that could be and were used by Plaid to access
24 and collect private information stored within their financial accounts. Plaid thereby willfully
25 deceived Plaintiffs and California Class members with the intent to induce them to alter their
26 position to their injury or risk under Cal. Civ. Code § 1709.

27 397. Plaintiffs seek recovery of their and the Class Members’ resulting damages, including
28 economic damages, restitution, and disgorgement, as well as punitive damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and the Proposed Classes defined herein, respectfully request:

A. That this Action be maintained as a Class Action, that Plaintiffs be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order:

- a. Preventing Defendant from sharing Plaintiffs' and Class Members' Private Information among themselves and other third parties;
- b. Requiring Defendant to alert and/or otherwise notify all users of its Websites and portals of what information is being collected, used, and shared;
- c. Requiring Defendant to provide clear information regarding its practices concerning data collection from the users/patients of Defendant's Websites, as well as uses of such data;
- d. Requiring Defendant to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information;
- e. Requiring Defendant to provide an opt out procedures for individuals who do not wish for their information to be tracked while interacting with Defendant's Websites;
- f. Mandating the proper notice be sent to all affected individuals, and posted publicly;
- g. Requiring Defendant to delete, destroy, and purge the Private Information of Users unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Users;

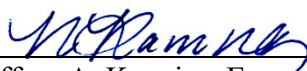
- 1 h. Requiring all further and just corrective action, consistent with
2 permissible law and pursuant to only those causes of action so permitted.
- 3 C. That the Court award Plaintiffs and the Class Members damages (both actual
4 damages for economic and non-economic harm and statutory damages) in an amount
5 to be determined at trial;
- 6 D. That the Court issue appropriate equitable and any other relief (including monetary
7 damages, restitution, and/or disgorgement) against Defendant to which Plaintiffs and
8 the Class are entitled, including but not limited to restitution and an Order requiring
9 Defendant to cooperate and financially support civil and/or criminal asset recovery
10 efforts;
- 11 E. Plaintiffs and the Class be awarded with pre- and post-judgment interest (including
12 pursuant to statutory rates of interest set under State law);
- 13 F. Plaintiffs and the Class be awarded with the reasonable attorneys' fees and costs of
14 suit incurred by their attorneys;
- 15 G. Plaintiffs and the Class be awarded with treble and/or punitive damages insofar as
16 they are allowed by applicable laws; and
- 17 H. Any and all other such relief as the Court may deem just and proper under the
18 circumstances.

19 **JURY TRIAL DEMANDED**

20 Plaintiffs demand a jury trial on all triable issues.

21
22 DATED: February 26, 2025

KIESEL LAW LLP

23
24 
25 Jeffrey A. Koncius, Esq.
26 Nicole Ramirez Jones, Esq.
27 Kaitlyn E. Fry, Esq.
28 8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel.: 310-854-4444

CLARKSON LAW FIRM, P.C.

Ryan Clarkson, Esq.
Yana Hart, Esq.
Bryan P. Thompson, Esq.
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

ALMEIDA LAW GROUP LLC

Matthew J. Langley, Esq.
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (773) 554-9354
matt@almeidalawgroup.com

SIMMONS HANLY CONROY LLP

Jason “Jay” Barnes, Esq.
Eric S. Johnson, Esq.
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: (212) 784-6400

**AHMAD, ZAVITSANOS,
& MENSING, PLLC**

Foster C. Johnson, Esq.
David Warden, Esq.
Nathan Campbell, Esq.
1221 McKinney Street, Suite 3460
Houston, TX 77010
Tel.: (713) 655-1101

Attorneys for Plaintiffs and the Proposed Class

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

PROOF OF SERVICE

STATE OF CALIFORNIA, COUNTY OF LOS ANGELES

At the time of service, I was over 18 years of age and not a party to this action. I am employed in the County of Los Angeles, State of California. My business address is 8648 Wilshire Boulevard, Beverly Hills, CA 90211-2910.

On February 26, 2025, I served true copies of the following document(s) described as **FIRST AMENDED CLASS ACTION COMPLAINT** on the interested parties in this action as follows:

SEE ATTACHED SERVICE LIST

BY E-MAIL OR ELECTRONIC TRANSMISSION: I caused a copy of the document(s) to be sent from e-mail address jmendez@kiesel.law to the persons at the e-mail addresses listed in the Service List. I did not receive, within a reasonable time after the transmission, any electronic message or other indication that the transmission was unsuccessful.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on February 26, 2025, at Beverly Hills, California.



Jessica Mendez

SERVICE LIST

CONSTANGY, BROOKS, SMITH & PROPHETE, LLP David A. Yudelson <i>dyudelson@constangy.com</i> Sydney M. Wright <i>smwright@constangy.com</i> Scott L. Satkin <i>ssatkin@constangy.com</i> 2029 Century Park East, Suite 1100 Los Angeles, CA 90067 Tel.: (310) 909-7775	Attorneys for Defendant MARIN HEALTH MEDICAL CENTER
SIMMONS HANLY CONROY LLP Jason “Jay” Barnes <i>jaybarnes@simmonsfirm.com</i> Eric S. Johnson <i>ejohnson@simmonsfirm.com</i> 112 Madison Avenue, 7th Floor New York, NY 10016 Tel.: (212) 784-6400	<i>Attorneys for Plaintiffs</i>
CLARKSON LAW FIRM, P.C. Ryan J. Clarkson <i>rclarkson@clarksonlawfirm.com</i> Yana Hart <i>yhart@clarksonlawfirm.com</i> Bryan P. Thompson <i>bthompson@clarksonlawfirm.com</i> 22525 Pacific Coast Highway Malibu, CA 90265 Tel: (213) 788-4050	<i>Attorneys for Plaintiffs</i>
ALMEIDA LAW GROUP LLC Matthew J. Langley <i>matt@almeidalawgroup.com</i> 849 W. Webster Avenue Chicago, Illinois 60614 Tel: (773) 554-9354	<i>Attorneys for Plaintiffs</i>
AHMAD, ZAVITSANOS, & MENSING, PLLC Foster C. Johnson <i>fjohnson@azalaw.com</i> David Warden <i>dwarden@azalaw.com</i> Nathan Campbell <i>ncampbell@azalaw.com</i> 1221 McKinney Street, Suite 3460 Houston, TX 77010 Tel: (713) 655-1101	<i>Attorneys for Plaintiffs</i>