

Hart L. Robinovitch (AZ SBN 020910)
ZIMMERMAN REED LLP
14648 N. Scottsdale Road, Suite 130
Scottsdale, AZ 85254
Telephone: (480) 348-6400
Facsimile: (480) 348-6415
Email: hart.robinovitch@zimmreed.com

(Additional Counsel listed below)

Attorneys for Plaintiffs

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA
PHOENIX DIVISION**

Cheryl McCulley, Rebecca Blount, Cindy
Freriks, Jill Schreidl, Demetria Ann Santiago-
Laboy, Oscar Irazaba, Dianna Williams, Faith
Robeson, and Tami Carroll,

*on behalf of themselves and all others
similarly situated,*

Plaintiffs,

v.

Banner Health,

Defendant.

Case No. CV-23-00985-PHX-SPL

No. CV-23-01054-PHX-ROS (cons.)

No. CV-23-01228-PHX-SPL (cons.)

REDACTED

**CONSOLIDATED CLASS ACTION
COMPLAINT**

1 Plaintiffs Cheryl McCulley, Rebecca Blount, Cindy Freriks, Jill Schreidl, Demetria
 2 Ann Santiago-Laboy, Oscar Irazaba, Dianna Williams, Faith Robeson, and Tami Carroll
 3 (“Plaintiffs”),¹ bring this Amended Class action Complaint on behalf of themselves, and
 4 all others similarly situated (the “Class Members”) against Banner Health (“Banner” or
 5 “Defendant”), which operates, controls, and manages 30 hospitals and several specialized
 6 care facilities across 6 different states.² Defendant owns and controls bannerhealth.com
 7 and its webpages (the “Website”), and it also owns and controls a mobile app (the “App”).
 8 The allegations contained in this Amended Class Action Complaint, which are based on
 9 Plaintiffs’ knowledge of facts pertaining to themselves and their own actions and counsels’
 10 investigations and upon information and belief as to all other matters are as follows:

11 1. Plaintiffs bring this class action lawsuit to address Banner Health’s
 12 outrageous, illegal, and widespread practice of disclosing its patients confidential
 13 personally identifiable information (“PII”) and protected health information (“PHI”)
 14 (collectively referred to as “Private Information”) to unauthorized third parties, including
 15 Meta Platforms, Inc. d/b/a Meta (“Facebook” or “Meta”) and Google LLC (“Google”).

16 2. This occurred and continues to occur because of the tracking technologies
 17 Defendant installed on its Website, App, and any corresponding patient portals it made
 18 available to its patients (collectively, the “Online Platforms”), including but not limited to
 19 the Facebook Pixel, Facebook SDK, Facebook Conversions API, Google Analytics,
 20 Google Tag Manager, DoubleClick (owned by Google), and related tools (collectively,
 21 “Tracking Technologies”).³

23 ¹ Plaintiffs file this Consolidated Complaint under seal out of a desire to protect their
 24 personal health information under the Health Insurance Portability and Accountability Act
 of 1996 (HIPAA) and Arizona law.

25 ² See <https://www.bannerhealth.com/about/glance> (last visited Nov. 21, 2023).

26 ³ This Complaint contains images and evidence demonstrating the Facebook Pixel was
 27 used on the Online Platforms, but Plaintiffs do not know every tracking and/or marketing
 28 tool that was previously installed on the Online Platforms during the relevant period, when
 they first began using Defendant’s Online Platforms.

1 3. The Tracking Technologies at-issue in the Complaint allow unauthorized
2 third parties to intercept the contents of patients' communications, receive and view
3 patients' Private Information, mine it for purposes unrelated to the provision of healthcare,
4 and further monetize it to deliver targeted advertisements to specific individuals.

5 4. Banner Health owns and controls the Website, which it encourages patients
6 to use for: (1) booking medical appointments; (2) locating physicians and treatment
7 facilities; (3) communicating medical symptom; (4) searching medical conditions and
8 treatment options; (5) signing up for events and classes; (6) registering for their Patient
9 Portal; and (7) utilizing their Symptom checker feature.⁴

10 5. In doing so, and by designing its Website in the manner described throughout
11 this complaint, Banner Health knew or should have known that its patients would use the
12 Online Platforms to communicate Private Information in conjunction with obtaining and
13 receiving medical services from it.

14 6. Unbeknownst to its Patients, however, Defendant's Online Platforms
15 contained Tracking Technologies within their source code that surreptitiously track and
16 transmit Plaintiffs' and Class Members' online activity and communications (including
17 intimate details about their medical treatment and appointments) to third parties without
18 first obtaining their permission, in violation of HIPAA, state laws, industry standards, and
19 patient expectations.

20 7. These Tracking Tools, including Meta Platforms, Inc.'s Tracking Pixel (the
21 "Meta Pixel" or "Pixel") and Google, Inc.'s Google Analytics tool, track and collect
22 communications with the Defendant via the Website and surreptitiously force the user's
23 web browser to send those communications to undisclosed third parties, such as Facebook
24 or Google.

25 8. Operating as designed and as implemented by Defendant, the Pixel allowed
26 the Private Information that Plaintiffs and Class Members submitted to Defendant to be

27 _____
28 ⁴ <https://www.bannerhealth.com/patients>

1 unlawfully disclosed to Facebook alongside their unique and persistent Facebook ID
2 (“FID”), IP address, and other static identifiers.

3 9. By installing Facebook Pixel, SDK, Google Analytics, and other Tracking
4 Technologies on its Online Platforms, Defendant effectively planted a bug on Plaintiffs’
5 and Class Members’ web browsers that caused their communications to be intercepted,
6 accessed, viewed, and captured by third parties in real time, as they were communicated
7 by patients, based on Defendant’s chosen parameters.

8 10. The Office for Civil Rights at HHS has issued a Bulletin to highlight the
9 obligations of HIPAA covered entities and business associates (“regulated entities”) under
10 the HIPAA Privacy, Security, and Breach Notification Rules (“HIPAA Rules”) when using
11 online tracking technologies (“tracking technologies”), such as the Tracking
12 Technologies.⁵ The Bulletin expressly provides (in bold type) that “[r]egulated entities
13 are not permitted to use tracking technologies in a manner that would result in
14 impermissible disclosures of PHI to tracking technology vendors or any other
15 violations of the HIPAA Rules.” In other words, HHS has expressly stated that
16 Defendant’s implementation of Tracking Technologies violates HIPAA Rules.

17 11. Plaintiffs and Class Members used Defendant’s Online Platforms to submit
18 information related to their past, present, or future health conditions, including, for
19 example, searches for specific health conditions and treatment and the booking of medical
20 appointments with a specific physician. Such Private Information would allow the third
21 party (e.g., Facebook or Google) to know that a specific patient was seeking confidential
22 medical care from Defendant, as well as the type of medical care being sought, such as
23 treatment for cancer, pregnancy, or addiction.

24
25
26 ⁵ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business*
27 *Associates*, [https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html)
28 [tracking/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html) (last visited Oct. 20, 2023).

1 12. Simply put, the health information disclosed through the tracking
2 technologies is personally identifiable.

3 13. Defendant is a healthcare entity and thus its disclosure of health and medical
4 communications is tightly regulated. The United States Department of Health and Human
5 Services (HHS) has established “Standards for Privacy of Individually Identifiable Health
6 Information” (also known as the “Privacy Rule”) governing how health care providers must
7 safeguard and protect Private Information. Under the Health Insurance Portability and
8 Accountability Act of 1996 (HIPAA) Privacy Rule, no health care provider can disclose a
9 person’s personally identifiable protected health information to a third party without
10 express written authorization.

11 14. Healthcare patients simply do not anticipate or expect that their trusted
12 healthcare provider will send personal health information or confidential medical
13 information collected via its webpages to a hidden third party – let alone Facebook and
14 Google, which both have a sordid history of privacy violations in pursuit of ever-increasing
15 advertising revenue – without the patients’ consent. Neither Plaintiffs nor any other Class
16 Member signed a written authorization permitting Defendant to send their Private
17 Information to Facebook or Google.

18 15. In response to the use of Tracking Technologies by HIPAA covered entities,
19 like Defendant, the recently issued HHS Bulletin warns that:

20 An impermissible disclosure of an individual’s PHI not only
21 violates the Privacy Rule but also may result in a wide range of
22 additional harms to the individual or others. For example, an
23 impermissible disclosure of PHI may result in identity theft,
24 financial loss, discrimination, stigma, mental anguish, or other
25 serious negative consequences to the reputation, health, or
26 physical safety of the individual or to others identified in the
27 individual’s PHI. Such disclosures can reveal incredibly
sensitive information about an individual, including diagnoses,
frequency of visits to a therapist or other health care
professionals, and where an individual seeks medical
treatment. While it has always been true that regulated entities
may not impermissibly disclose PHI to tracking technology
vendors, because of the proliferation of tracking technologies
collecting sensitive information, now more than ever, it is

critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.⁶

16. And as recently noted by the Hon. William J. Orrick in a decision concerning the use of the Facebook Pixel by healthcare organizations,

“[o]ur nation recognizes the importance of privacy in general and health information in particular: the safekeeping of this sensitive information is enshrined under state and federal law. The allegations against Meta are troubling: Plaintiff raise potentially strong claims on the merits and their alleged injury would be irreparable if proven.”⁷

17. Consequently, Plaintiffs bring this action for legal and equitable remedies to address and rectify the illegal conduct and actions described herein, to enjoin Defendant from making similar disclosure of its patients’ Private Information in the future, and to fully articulate, *inter alia*, the specific Private Information it disclosed to third parties and to identify the recipients of that information.

18. Defendant breached its statutory and common law obligations to Plaintiffs and Class Members by, *inter alia*,: (i) failing to remove or disengage technology that was known and designed to share web-users’ information; (ii) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook or others; (iii) failing to take steps to block the transmission of Plaintiffs’ and Class Members’ Private Information through Tracking Tools like the Facebook Pixel or Google Analytics; (iv) failing to warn Plaintiffs and Class Members; and (v) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

19. As a result of Defendant’s conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the

⁶ *Id.*

⁷ *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218, at *1 (N.D. Cal. Dec. 22, 2022).

bargain, (iii) diminution of value of their Private Information, (iv) statutory damages, (v) the continued and ongoing risk to their Private Information, and (vi) lost time.

20. Plaintiffs seek to remedy these harms and brings causes of action for (1) breach of confidence; (2) violation of the Electronics Communication Privacy Act (“ECPA”), 18 U.S.C. § 2511(1) – unauthorized interception, use, and disclosure; (3) invasion of privacy (intrusion upon seclusion); (4) breach of implied contract; (5) unjust enrichment; (6) negligence; (7) violation of the Arizona Consumer Fraud Act (“ACFA”), A.R.S. § 44-1521, *et seq.*; (8) violation of the California Invasion of Privacy Act (“CIPA”), Cal. Penal Code §§ 630, *et seq.*; (9) violation of the California Confidentiality of Medical Information Act (“CMIA”), Cal. Civ. Code §§ 56, *et seq.*; (10) violation of the California Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful Business Practices; (11) violation of the California UCL, Cal. Bus. & Prof. Code § 17200, *et seq.* – Unfair Prong; and (12) violation of the Colorado Consumer Protection Act, Colo. Rev. Stat. Section 6-1-101, *et seq.*

PARTIES

21. Plaintiff Cheryl McCulley is, and at all relevant times was, an individual residing in Susanville, Lassen County, in the State of California.

22. Plaintiff Cindy Freriks is, and has been since June 2022, an individual residing in Lehigh Acres, Lee County, in the State of Florida. Prior to moving to Lehigh Acres in June 2022, Ms. Freriks was a resident of Denver, Colorado.

23. Plaintiff Rebecca Blount is, and at all relevant times was, an individual residing in Casa Grande, Pinal County, in the State of Arizona.

24. Plaintiff Jill Schreidl is, and at all relevant times was, an individual residing in Loveland, Larimer County, in the State of Colorado.

25. Plaintiff Demetria Ann Santiago Laboy (Browning) is, and at all relevant times was, an individual residing in Peoria, Maricopa County, in the State of Arizona.

26. Plaintiff Oscar Irazaba is, and at all relevant times was, an individual residing

1 in Peoria, Arizona, where he intends to remain.

2 27. Plaintiff Dianna Williams is, and at all relevant times was, an individual
3 residing in Wyoming.

4 28. Plaintiff Faith Robeson is, and at all relevant times was, an individual
5 residing in Logan County, Colorado.

6 29. Plaintiff Tami Carroll is, and at all relevant times was, an individual residing
7 in Maricopa County, Arizona.

8 30. Defendant is one of the largest hospital systems in the country, operating 30
9 acute-care hospitals and a number of other service centers and clinics throughout the states
10 of Arizona, California, Colorado, Nebraska, Nevada, and Washington. As of 2021, Banner
11 Health is the largest private employer in Arizona with more than 50,000 employees across
12 its various locations. Defendant is based in Phoenix, Arizona.

13 31. Although Defendant operates under the name “Banner Health” it consists of
14 a network of services, hospitals, clinics, and programs known by various names including,
15 but not limited to: Banner – University Medical Center Tucson, Banner – University
16 Medical Center Phoenix, Banner – University Medical Center South, Banner Alzheimer’s
17 Institute, Banner Concussion Center, Banner Heart Hospital, Banner MD Anderson Cancer
18 Center, Banner Children’s, Banner Health network, Banner Medical Group, and Banner –
19 University Medicine.

20 32. According to its Website, Defendant was serving at least one million
21 members across its numerous locations and services as of 2021.

22 33. Defendant is a covered entity under the Health Insurance Portability and
23 Accountability Act of 1996.

24 **JURISDICTION & VENUE**

25 34. This Court has subject matter jurisdiction over this action under 28 U.S.C. §
26 1332(d) because this case is brought as a class action where the amount in controversy
27 exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than
28

100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant.

35. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (18 U.S.C. § 2511, *et seq.*).

36. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

37. Venue is proper under 28 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

A. Background

38. Facebook operates the world's largest social media company and generated \$117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.⁸

39. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

40. Facebook's Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of website visitors' activity.

41. One such Business Tool is the Pixel, which "tracks the people and type of actions they take."⁹ When a user accesses a webpage hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated

⁸*Facebook, Meta Reports Fourth Quarter and Full Year 2021 Results*, FACEBOOK, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited Nov. 19, 2023).

⁹ RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited Nov. 19, 2023).

1 and sent to Facebook's servers. Notably, this transmission does not occur unless the
2 webpage contains the Pixel. Stated differently, Plaintiffs' and Class Members' Private
3 Information would not have been disclosed to Facebook but for the Defendant's decisions
4 to install the Pixel on its webpage(s).

5 42. As explained in more detail below, this secret transmission to Facebook is
6 initiated by Defendant's source code concurrently with Plaintiffs' and Class Members'
7 communications to their intended recipient, Defendant.

8 **B. Banner Health Assisted Third Parties in Intercepting Patients'**
9 **Communications with its Online Platforms and Disclosed Plaintiffs' and Class**
10 **Members' Private Information to Third Parties.**

11 43. Defendant's Online Platforms are accessible on mobile devices and desktop
12 computers and allow patients to communicate with Defendant regarding the patients' past,
13 present, and future health, or medical care, as well as their past, present, and future medical
14 bills and payments.

15 44. Defendant encouraged patients to use the Online Platforms to communicate
16 their private medical information, schedule appointments and facility tours, access
17 information about their treatments, pay medical bills, view test results, and more.

18 45. Despite this, Defendant purposely installed Tracking Technologies on its
19 Online Platforms and programmed specific webpage(s) to surreptitiously share its patients'
20 private and protected communications, including Plaintiffs' and Class Members' PHI and
21 PII, which was sent to Facebook, Google, and additional third parties.

22 46. The Tracking Technologies followed, recorded, and disseminated patients'
23 information as they navigated and communicated with Defendant via the Online Platforms,
24 simultaneously transmitting the substance of those communications to unintended third
25 parties.

26 47. The information disseminated by the Tracking Technologies and/or
27 intercepted by third parties constitutes Private Information, including medical information
28 patients requested or viewed, the title of any buttons they clicked (such as the "Request

1 Treatment” button, which indicates the patients has requested treatment), the exact phrases
2 users typed into text boxes, selections they made from drop-down menus or while using
3 filtering tools, which indicates the exact treatment and therapy the user is seeking and also
4 reveals their medical symptoms and conditions), and other sensitive and confidential
5 information, the divulgence of which is and was highly offensive to Plaintiffs.

6 48. As described by the HHS Bulletin, this is protected health information (PHI)
7 because “the information connects the individual to the regulated entity (*i.e.*, it is indicative
8 that the individual has received or will receive health care services or benefits from the
9 covered entity), and thus relates to the individual’s past, present, or future health or health
10 care or payment for care.”¹⁰

11 49. The information collected and disclosed by Defendant’s Tracking Tools is
12 not anonymous and is viewed and categorized by the intercepting party on receipt.

13 50. The information Facebook received via the Tracking Tools was linked and
14 connected to patients’ Facebook profiles (via their Facebook ID or “c_user id”), which
15 includes other identifying information.

16 51. Similarly, Google stores users’ logged-in identifier on non-Google website
17 in its logs. Whenever a user logs-in on non-Google websites, whether in private browsing
18 mode or non-private browsing mode, the same identifier is associated with the data Google
19 collects from the user’s browsing activities on that website. Google further logs all such
20 data (private and non-private) within the same logs and uses these data for serving
21 personalized ads.

22
23
24
25
26
27
28

¹⁰ See HHS Bulletin *supra*, note 6.

52. Simply put, the health information that was disclosed via the Tracking Tools is personally identifiable and was sent alongside other persistent unique identifiers such as the patients' IP address, Facebook ID, and device identifiers.^{11,12}

53. As described by the HHS Bulletin, this is protected health information (PHI) even if the visitor has no previous relationship with Defendant because "the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care."¹³

i. Banner Health's Tracking Technologies, Source Code, Interception of HTTP Requests and Transmission of HTTP Requests.

54. Web browsers are software applications that allow consumers to navigate the internet and exchange electronic communications, and every "client device" (computer, tablet, or smart phone) has a web browser (e.g., Microsoft Edge, Google Chrome, Mozilla's Firefox, etc.).

55. Correspondingly, every website is hosted by a computer "server" which allows the website's owner (Defendant) to display the Website and exchange communications with the website's visitors (Plaintiffs and Class Members) via the visitors' web browser.

¹¹ See *Brown v. Google, Inc.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049 (N.D. Cal. 2021) (citing internal evidence from Google employees). Google also connects user data to IP addresses; IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifying information. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

¹² <https://developers.facebook.com/docs/meta-pixel/> (last accessed Nov. 5, 2023).

¹³ See HHS Bulletin *supra*, note 5.

1 56. When patients used the Online Platforms, they engaged in an ongoing back-
2 and-forth exchange of electronic communications with Defendant wherein their web
3 browser communicated with Defendant's computer server—like how two telephones
4 would communicate.

5 57. These communications are invisible to ordinary consumers¹⁴, but one
6 browsing session may consist of thousands of individual HTTP Requests and HTTP
7 Responses.

8 58. A patient's HTTP Request essentially asks the Defendant's Website to
9 retrieve certain information (such as a "Find a Doctor" page), and the HTTP Response
10 renders or loads the requested information in the form of "Markup" (the pages, images,
11 words, buttons, and other features that appear on the patient's screen as they navigate
12 Defendant's Webpage(s)).

13 59. Every webpage is comprised of both Markup and "Source Code." Source
14 Code is simply a set of instructions that commands the website visitor's browser to take
15 certain actions when the web page first loads or when a specified event triggers the code.

16 60. Defendant's Tracking Technologies were embedded in its Online Platforms'
17 Source Code, which is contained in its HTTP Response. The Tracking Technologies, which
18 were programmed to automatically track patients' communications and transmit them to
19 third parties, executed instructions that effectively opened a hidden spying window into
20 each patients' web browser, through which third parties intercepted patients'
21 communications and activity while using Defendant's Online Platforms.

22 61. For example, when a patient visits www.bannerhealth.com and selects the
23 "Get Care Now" button, the patient's browser automatically sends an HTTP Request to
24 Defendant's web server. Defendant's web server automatically returns an HTTP Response,
25

26
27 ¹⁴ See HHS Bulletin *supra*, note 5 ("Tracking technologies collect information and track
28 users in various ways, many of which are not apparent to the website or mobile app user.").

which loads the Markup for that particular webpage. As depicted below, the user only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

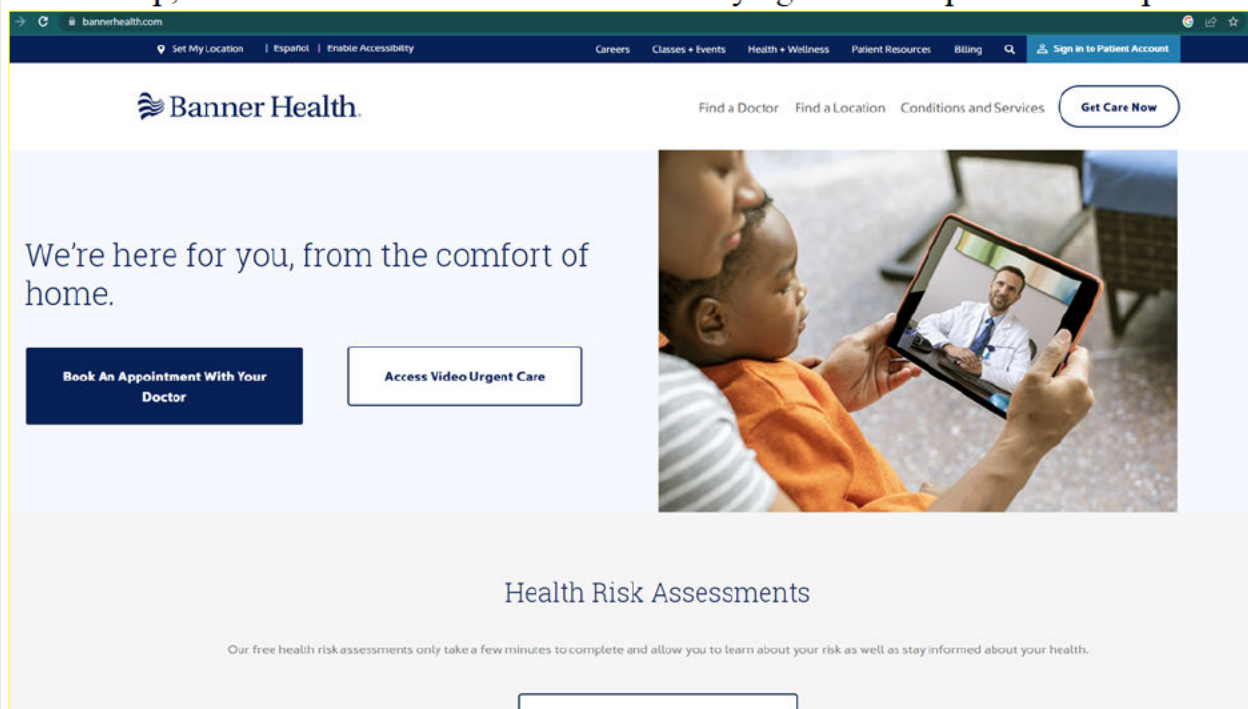


Figure 1. The image above is a screenshot taken from the user's web browser upon visiting <https://www.bannerhealth.com> (Last accessed June 7, 2023).

62. The image above displays the Markup of Defendant's Webpage. Behind the scenes, however, Tracking Tools like the Facebook Pixel and the Google Analytics are embedded in the source code, automatically transmitting everything the patient does on the webpage and effectively opening a hidden spy window into the patients' browser.¹⁵

C. Defendant Disclosed Plaintiffs' and Class Members' Private Information to Facebook and Google Using Tracking Tools

63. In this case, Defendant employed Tracking Tools, including the Facebook Pixel and Conversions API, as well as the Google Analytics tool, to intercept, duplicate,

¹⁵ When used in the context of a screen or visual display, a "pixel" is the smallest unit in such a digital display. An image or video on a device's screen can be made up of millions of individual pixels. For example, the Facebook Pixel is a tiny image file that is so small as to be invisible to website users. It is purposefully designed and camouflaged in this manner so that website users remain unaware of it.

1 and re-direct Plaintiffs' and Class Members' Private Information to Facebook and Google.

2 64. Defendant's Source Code manipulates the patient's browser by secretly
3 instructing it to duplicate the patient's communications (HTTP Requests) with Defendant
4 and to send those communications to Facebook and Google. These transmissions occur
5 contemporaneously, invisibly, and without the patient's knowledge.

6 65. Thus, without its patients' consent, Defendant has effectively used its source
7 code to commandeer and "bug" or "tap" its patients' computing devices, allowing
8 Facebook, Google, and other third parties to listen in on all of their communications with
9 Defendant and thereby intercept those communications, including Private Information.

10 66. The Tracking Tools allow Defendant to optimize the delivery of ads, measure
11 cross-device conversions, create custom audiences, and decrease advertising and
12 marketing costs. However, Defendant's Website does not rely on the Tracking Tools in
13 order to function.

14 67. While seeking and using Defendant's services as a medical provider,
15 Plaintiffs and Class Members communicated their Private Information to Defendant via its
16 Website.

17 68. Plaintiffs and Class Members were not aware that their Private Information
18 would be shared with third parties as it was communicated to Defendant because, amongst
19 other things, Defendant did not disclose this fact.

20 69. Plaintiffs and Class Members never consented, agreed, authorized, or
21 otherwise permitted Defendant to disclose their Private Information to third parties, nor did
22 they intend for anyone other than Defendant to be a party to their communications (many
23 of them highly sensitive and confidential) with Defendant.

24 70. Defendant's Tracking Tools sent non-public Private Information to third
25 parties like Facebook and Google, including but not limited to Plaintiffs' and Class
26 Members': (1) status as medical patients; (2) health conditions; (3) desired medical
27 treatment or therapies; (4) desired locations or facilities where treatment was sought; (5)

1 phrases and search queries (such as searches for symptoms, treatment options, or types of
2 providers); and (6) searched and selected physicians and their specialties conducted via the
3 general search bar.

4 71. Importantly, the Private Information Defendant's Tracking Tools sent to
5 third parties included personally identifying information that allowed those third parties to
6 connect the Private Information to a specific patient. Information sent to Facebook was
7 sent alongside the Plaintiffs' and Class Members' Facebook ID (c_user cookie or "FID"),
8 thereby allowing individual patients' communications with Defendant, and the Private
9 Information contained in those communications, to be linked to their unique Facebook
10 accounts and therefore their identity.¹⁶

11 72. A user's FID is linked to their Facebook profile, which generally contains a
12 wide range of demographic and other information about the user, including location,
13 pictures, personal interests, work history, relationship status, and other details. Because the
14 user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or
15 any ordinary person—can easily use the Facebook ID to locate, access, and view the user's
16 corresponding Facebook profile quickly and easily.

17 73. Similarly, Google users who are logged-in to their Google accounts also have
18 an identifier that is stored in Google's logs. Google logs a user's browsing activities on
19 non-Google websites and uses these data for serving personalized ads.¹⁷

20 74. Defendant deprived Plaintiffs and Class Members of their privacy rights
21 when it: (1) implemented Tracking Tools that surreptitiously tracked, recorded, and
22 disclosed Plaintiffs' and other online patients' confidential communications and Private
23 Information; (2) disclosed patients' protected information to unauthorized third parties; and
24

25 ¹⁶ Defendant's Website track and transmit data via first-party and third-party cookies. The
26 c_user cookie or FID is a type of third-party cookie assigned to each person who has a
Facebook account, and it is comprised by a unique and persistent set of numbers.

27 ¹⁷ *Brown v. Google LLC*, Case No. 4:20-cv-3664-YGR, FN11 (quoting Google employee
28 deposition testimony explaining how Google tracks user data).

1 (3) undertook this pattern of conduct without notifying Plaintiffs or Class Members and
2 without obtaining their express written consent.

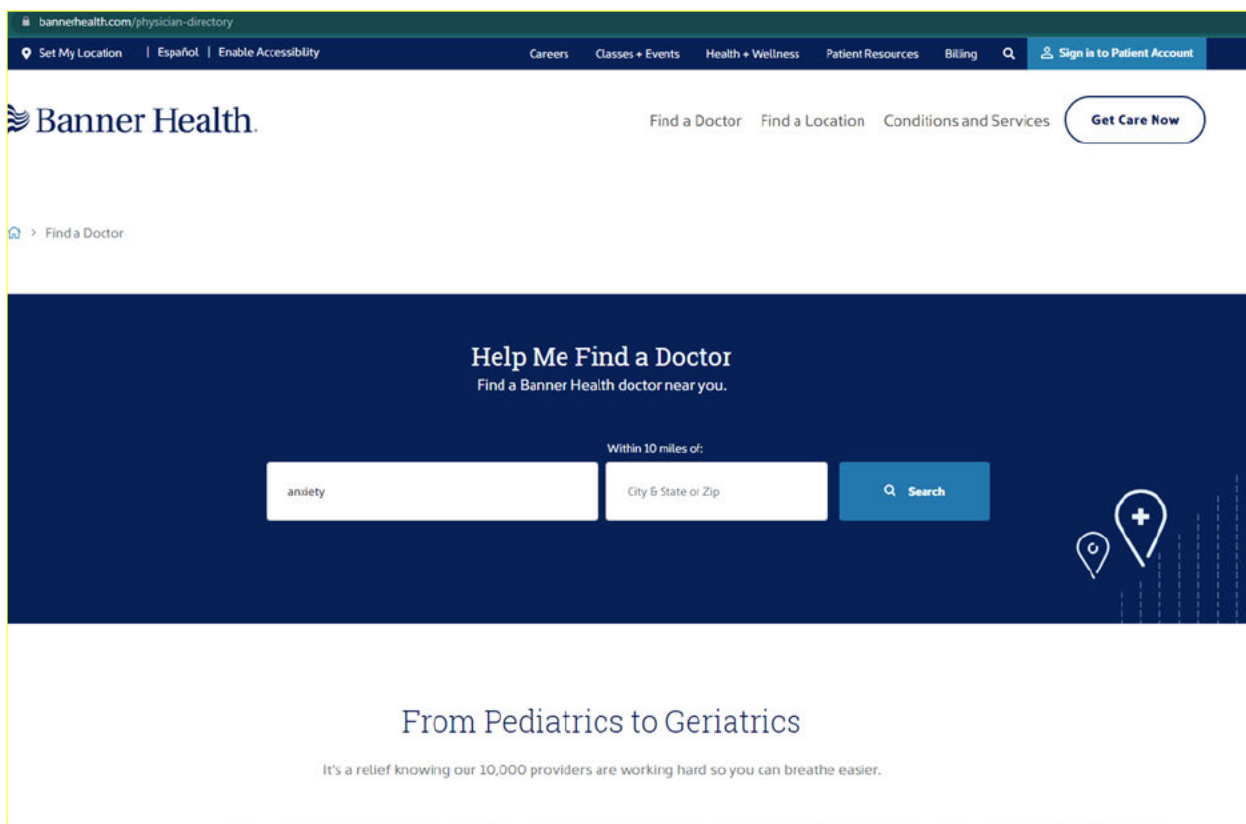
3 75. By installing and implementing both Facebook tools and Google Analytics,
4 Defendant caused Plaintiffs' and Class Member's communications to be intercepted by
5 and/or disclosed to Facebook and Google and for those communications to be personally
6 identifiable.

7 76. As explained below, these unlawful transmissions are initiated by
8 Defendant's source code concurrent with communications made via certain webpages.

9 **D. Defendant's Tracking Tools Disseminate Patient Information Via Its Website**

10 77. An example illustrates the point. If a patient uses the Website to find a
11 physician, Defendant's Website directs them to communicate Private Information,
12 including desired physician name, location, and specialty/area of practice. Unbeknownst
13 to the patient, this communication is sent to Facebook and other third-party entities via
14 Defendant's Pixel, including the terms searched in the search bar and the filters they select.

15 78. In the example below, the user navigated to the "Find a Doctor" page in
16 Defendant's Website where the user is prompted by Defendant's Website to find a doctor
17 by inputting personal information regarding their medical condition, including desired
18 specialty, or by using the search bar to search applicable terms:



bannerhealth.com/physician-directory

Set My Location | Español | Enable Accessibility | Careers | Classes + Events | Health + Wellness | Patient Resources | Billing | Sign in to Patient Account

Banner Health Find a Doctor Find a Location Conditions and Services **Get Care Now**

Find a Doctor

Help Me Find a Doctor
Find a Banner Health doctor near you.

Within 10 miles of:

anxiety City & State or Zip **Search**

From Pediatrics to Geriatrics

It's a relief knowing our 10,000 providers are working hard so you can breathe easier.

Figure 2. Screenshot taken from bannerhealth.com as the user searches for a specialist and communicates information via the search bar and filtering tools.

79. In this instance, the user searched for a physician specialized in treating “anxiety” who is currently offering local services.

80. Next, the user narrows their search results by typing “Phoenix, AZ” into the “City & State or Zip” search bar and set the location filters to physicians who are “within 10 miles” of the city.

81. Unbeknownst to ordinary patients, this webpage—which is undoubtedly used to communicate Private Information for the purpose of seeking medical treatment—contains Defendant’s Tracking Tools. The image below shows the “behind the scenes” portion of the website that is invisible to ordinary users:

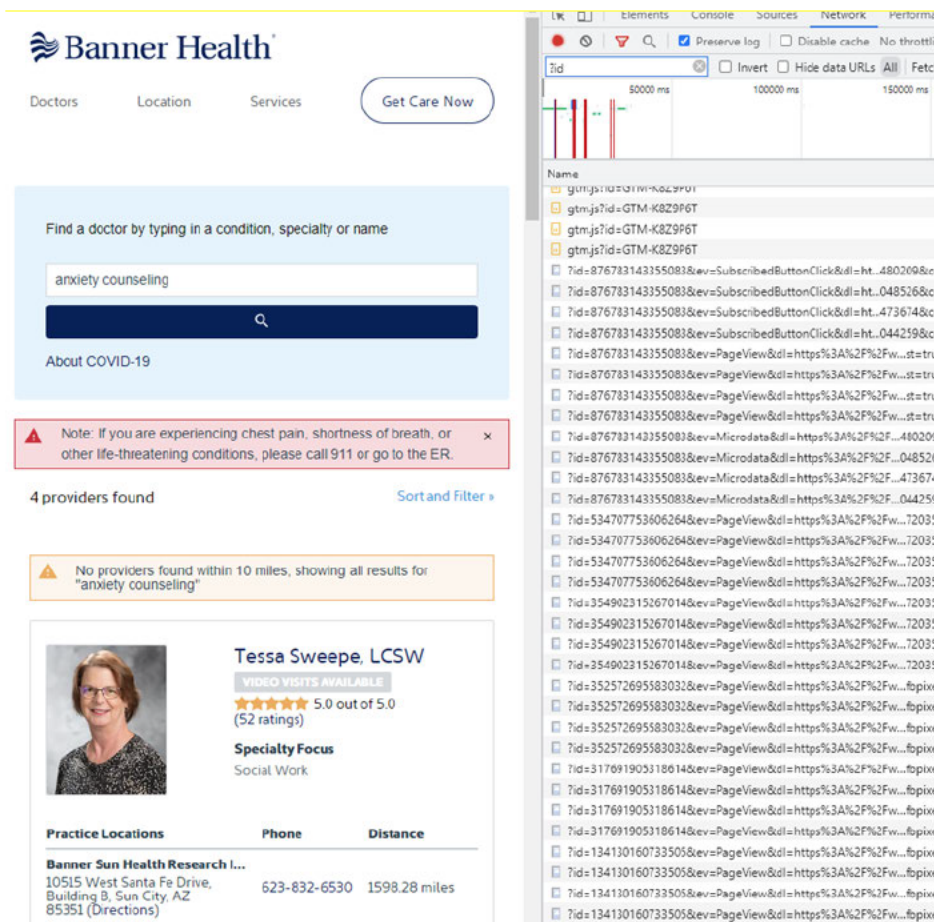


Figure 3. Screenshot from Defendant's website depicting back end network traffic.

82. Thus, without alerting the user, Defendant's Pixel sends the communications the user made via the webpage to Facebook, and the images below confirm that the communications Defendant sends to Facebook contain the user's Private Information.

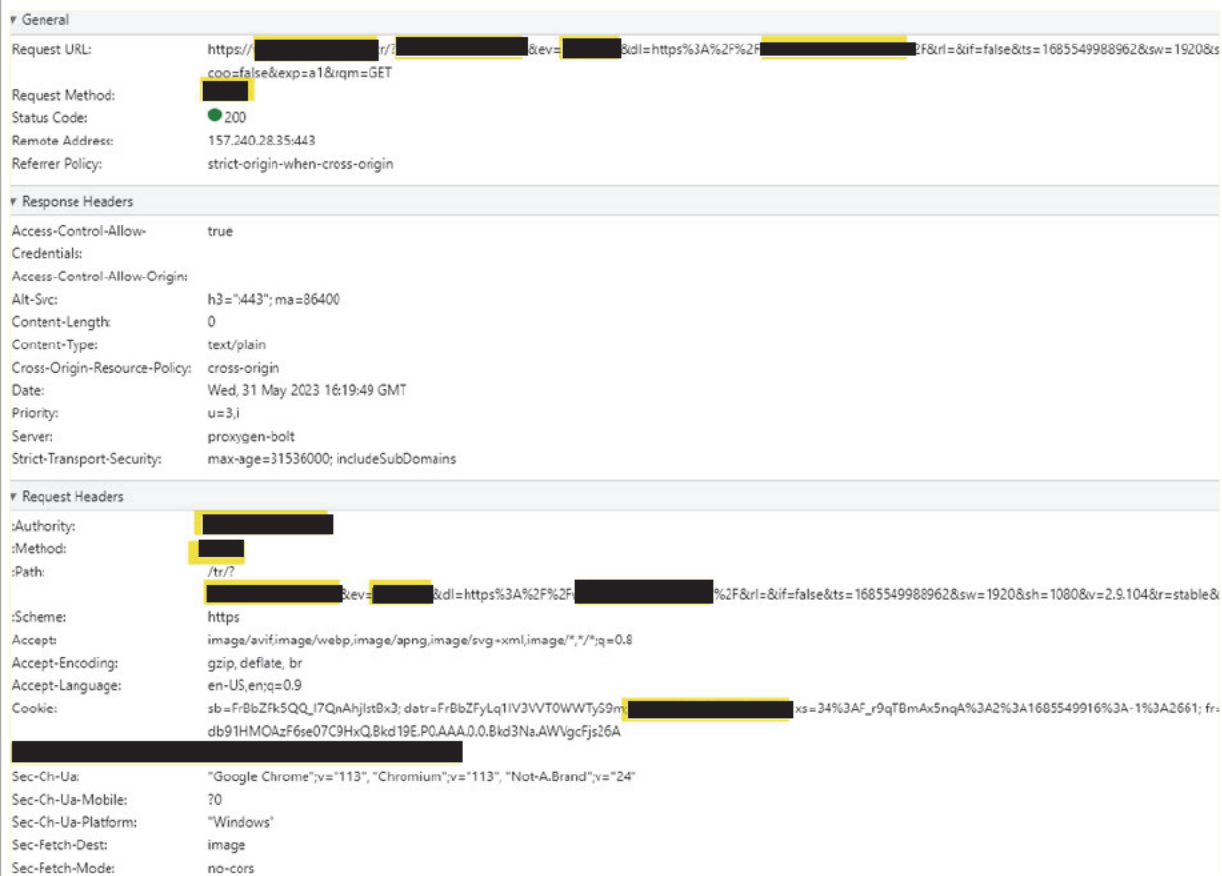


Figure 4: Screenshot from the Network traffic report depicting the payload that Facebook is sent including specific user identifiers.

83. The first line of highlighted text, “id=317691905318614” refers to Defendant’s Pixel ID and confirms that it implemented the Pixel into its Source Code for this webpage and transmitted info to Facebook from this webpage.

84. On the same line of text, “ev= PageView,” identifies and categorizes which actions the user took on the webpage (“ev=” is an abbreviation for event, and “PageView” is the type of event). Thus, this identifies the user as having navigated to the Website page.

85. Under request headers, the referrer is highlighted showing that Banner Health sent the information to Facebook.

86. Finally, the highlighted text (“GET”) demonstrates that Defendant’s Pixel sent the user’s communications, and the Private Information contained therein, alongside

the user's Facebook ID (c_user ID), thereby allowing the user's communications and actions on the website to be linked to their specific Facebook profile.¹⁸

87. The image demonstrates that the user's Facebook ID (highlighted as "c_user=" in the image above) was sent alongside the other data.¹⁹

88. To make matters worse, Defendant's Pixels even track and record the exact text and phrases that a user types into the general search bar located on Defendant's homepage. In the example below, the user typed "I have cancer" into the search bar.

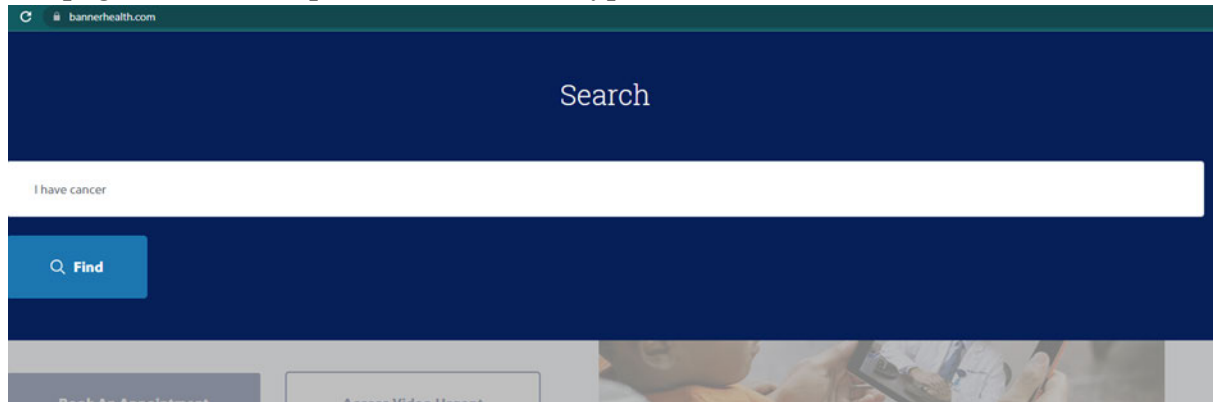


Figure 5. Screenshot from Defendant's website's search bar feature.

89. Resultantly, that exact phrase is sent to Facebook, thereby allowing the user's medical condition to be linked to their individual Facebook account for future retargeting and exploitation. This is simply unacceptable, and there is no legitimate reason for sending this information to Facebook.

¹⁸ The user's Facebook ID is represented as the c_user ID highlight in the image above, and Plaintiffs redacted the corresponding string of numbers to preserve the user's anonymity.

¹⁹ The user's Facebook ID is represented as the c_user ID highlight in the image below, and Plaintiffs redacted the corresponding string of numbers to preserve the user's anonymity.

[REDACTED]
[REDACTED]
dl: https://www.bannerhealth.com/search?query [REDACTED]
rl: https://www.bannerhealth.com/
if: false
ts: 1685550505691
sw: 1920
sh: 1080
v: 2.9.104
r: stable
ec: 0
o: 28
fbp: fb.1.1685542516980.2007203529
it: 1685550505567
coo: false
exp: a1
rqm: GET

Figure 6. Screenshot of the Payload received by Facebook from the user's search of "I have cancer" from the Defendant's search bar.

90. In each of the examples above, the user's website activity and the contents of the user's communications are sent to Facebook alongside their personally identifiable information. Several different methods allow marketers and third-parties to identify individual website users, but the examples above demonstrate what happens when the website user is logged into Facebook on their web browser or device. When this happens, the website user's identity is revealed via third-party cookies that work in conjunction with the Pixels. For example, the Pixels transmit the user's c_user cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

91. Facebook receives at least six cookies when Defendant's website transmits information via the Pixels:

Request Cookies ☐ show filtered out request cookies

Name	Value	Domain
sb	uV1...	.facebook.com
datr	uV1...	.facebook.com
c_user	100...	.facebook.com
usida	eyJ...	.facebook.com
xs	16...	.facebook.com
fr	0hxl...	.facebook.com

Figure 8. Screenshot of network analysis showing cookies sent to Facebook when a user visits bannerhealth.com.

92. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies:²⁰

fr	00Zp...	.facebook.com
wd	1156...	.facebook.com
sb	qqAz...	.facebook.com
datr	Malz...	.facebook.com

Figure 9. Screenshot of Network traffic cookie report for a recently signed out facebook user.

93. The fr cookie contains an encrypted Facebook ID and browser identifier.²¹ Facebook, at a minimum, uses the fr cookie to identify users, and this cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.²²

²⁰ The screenshot below serves as example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

²¹ Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited Nov. 11, 2023).

²² *Cookies & other storage technologies*, <https://www.facebook.com/policy/cookies/> (last visited Nov. 11, 2023).

94. At each stage, Defendant also utilizes the `_fbp` cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user.

²³

<code>_fbp</code>	<code>fb.1.1686147863271.2049175303</code>	<code>.bannerhealth.com</code>
-------------------	--	--------------------------------

Figure 10. screenshot showing defendant's use of a first party cookie.

95. The Pixel uses both first- and third-party cookies, and both were used on the Website.²⁴

96. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but other evidence suggests Defendant is using additional tracking pixels and tools to transmit its patients' Private Information to additional third parties. For example, the image below indicates that Defendant is also sending its patients' protected health information to Google via Google Analytics:

²³ Defendant's Website tracks and transmits data via first-party and third-party cookies. The `c_user` cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

²⁴ A first-party cookie is "created by the website the user is visiting"—in this case, Defendant's Website. 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. The `_fbp` cookie is always transmitted as a first-party cookie. At a minimum, Facebook uses the `fr`, `_fbp`, and `c_user` cookies to link website visitors' data to their Facebook IDs and corresponding accounts.

▼ Request Headers

```

:method: POST
:path: /g/collect?v=2&[REDACTED]
[REDACTED]&gtm=45je3b81v893512385z8811848058&p=1700616266485&gcd=11111111&dma=0&cid=
2117730250.1700609170&ul=en-
us&sr=1680x1050&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B119.0.6045.123%7CChromium%3B
119.0.6045.123%7CNot%253FA_Brand%3B24.0.0.0&uamb=0&uam=&uap=macOS&uapv=12.6.3&uaw=0&
are=1&_s=1&dl=https%3A%2F%2Fwww.bannerhealth.com%2F[REDACTED]
[REDACTED]&dr=https%3A%2F%2Fwww.bannerhealth.com%2Fpatients%2Fsymptoms
checker&sid=1700616139&sct=2&seg=1&dt=Banner%20Health%20Search%20Results&en=page_view&tfd
=1951
:scheme: https
:Accept: */*
:Accept-Encoding: gzip, deflate, br
:Accept-Language: en-US,en;q=0.9
:Content-Length: 0
:Cookie: ar_debug=1
:Origin: https://www.bannerhealth.com
[REDACTED]
Sec-Ch-Ua: "Google Chrome";v="119", "Chromium";v="119", "Not?A_Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36

```

Figure 11. Screenshot showing the request headers from Google Analytics, that are sent by the Defendant's unique identifier ("tid=G-VTYKD8EHM8").²⁵

²⁵ See Google Analytics Dev Tools: Measurement Protocol Reference: Required Values for All Hits, <https://developers.google.com/analytics/devguides/collection/protocol/v1/reference> (last visited Nov. 21, 2023).

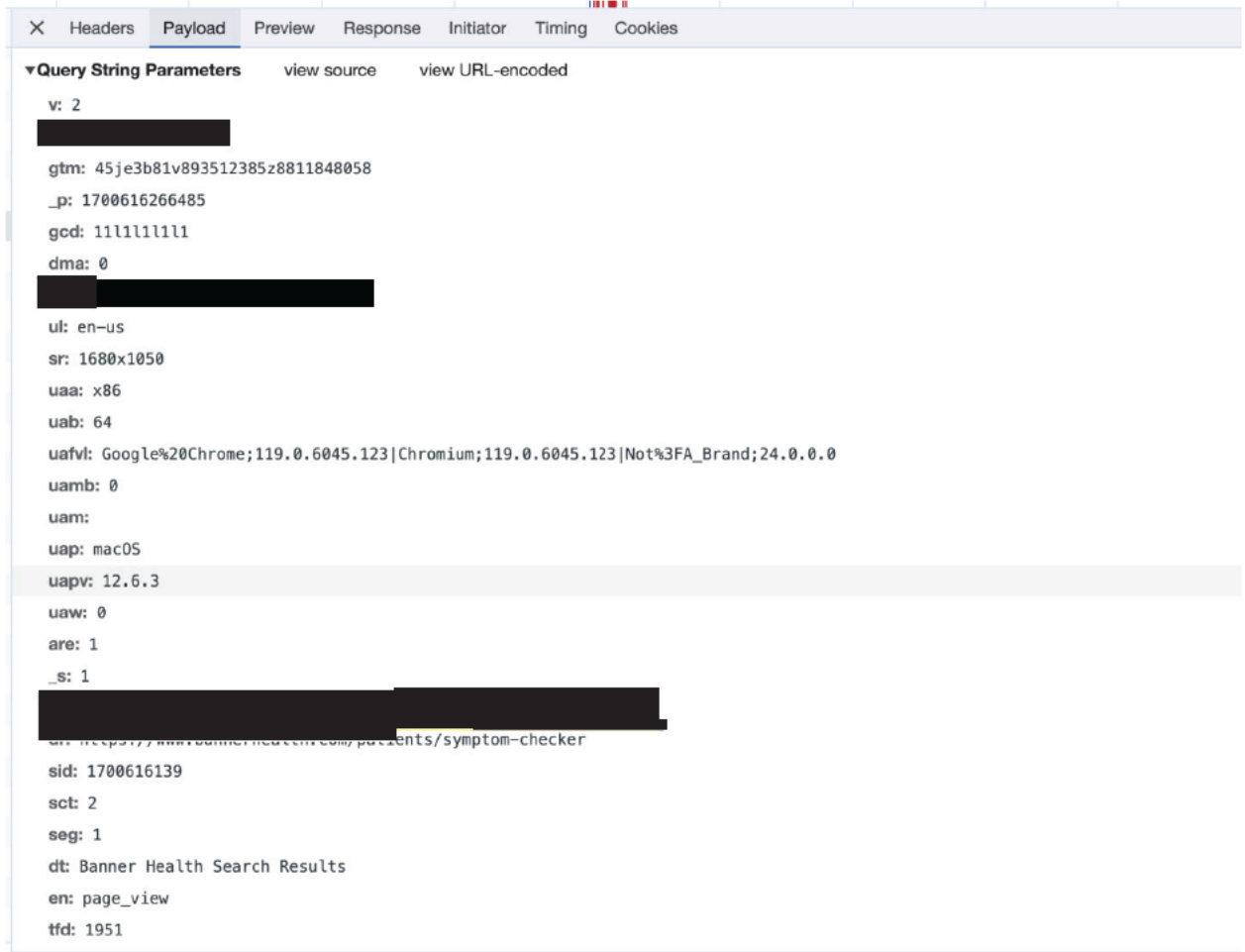


Figure 12. screenshot of Google Analytics Payload, depicting the Defendant's unique identifier ("tid=G-VTYKD8EHM8"), the user's unique identifier ("cid")²⁶, the referring site as the defendant and the specific search the user made on the Website.

97. The images above contain the user's search phrase ("I have cancer"), and Defendant does not appear to have enabled the anonymize feature provided by Google Analytics because the text "aip:" does not appear in the image, thereby revealing the user's status as a patient and that the patient is seeking treatment for cancer.

98. Accordingly, Google receives patients' communications alongside the patients' IP address, which is also impermissible under HIPAA.

²⁶ The cid has been redacted to protect the user's identity.

99. Defendant does not disclose that the Pixels, Google Analytics, or any other tracking tools embedded in the Website's source code track, record, and transmit Plaintiffs' and Class Members' Private Information to Facebook and Google. Moreover, Defendant never received consent or written authorization to disclose Plaintiffs' and Class Members' private communications to Facebook or Google.

E. Plaintiffs' Experiences with Banner

Plaintiff McCulley's Experience

100. As a condition of receiving Defendant's services, Plaintiff McCulley disclosed her Private Information to Defendant on numerous occasions, and most recently in March 2023.

101. Plaintiff McCulley has been a patient of Defendant for more than 15 years.

102. Plaintiff McCulley accessed Defendant's Website and Patient Portal on her phone and computer to receive healthcare services from Defendant and at Defendant's direction.

103. Plaintiff McCulley used Defendant's services to request and book doctor's appointments for herself, research specific health conditions and treatments, and complete patient web forms.

104. Specifically, Plaintiff McCulley utilized Defendant's services for all of her medical needs, including her [REDACTED]

105. Plaintiff McCulley also utilized Defendant's Patient Portal to refill prescriptions, look at her bills and payments and to see her test results.

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

107. Plaintiff McCulley reasonably expected that her communications with Defendant via the Web Properties were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

1 108. However, and as a result of the Meta Pixels Defendant chose to install on its
2 Website, Plaintiff McCulley's Private Information was intercepted, viewed, analyzed and
3 used by unauthorized third parties.

4 109. Defendant transmitted Plaintiff McCulley's Facebook ID, computer IP
5 address and other device and unique online identifiers to Facebook. Defendant also
6 transmitted information such as health and medical information including Plaintiff's
7 particular health condition, the type of medical treatment sought, patient status and the fact
8 that Plaintiff attempted to or did book a medical appointment.

9 110. Plaintiff McCulley never consented to the disclosure of or use of her Private
10 Information by third parties or to Defendant enabling third parties, including Facebook, to
11 access or interpret such information. Plaintiff McCulley never consented to any third
12 parties' receipt or use of her Private Information.

13 111. Notwithstanding, through the Meta Pixels and similar technologies
14 embedded on Defendant's Website, Defendant transmitted Plaintiff McCulley's Private
15 Information to, at a minimum, Facebook and likely many other third parties like Google,
16 Bing and others.

17 112. As a result, Plaintiff McCulley received targeted ads on Facebook or
18 Instagram related to her specific medical conditions and/or treatments, including but not
19 limited to medications, treatments, and specialized medical facilities [REDACTED]
20 [REDACTED]

21 113. By making these disclosures without her consent, Defendant breached
22 Plaintiff McCulley's privacy and unlawfully disclosed her Private Information.

23 114. Defendant did not inform Plaintiff McCulley that it had shared her Private
24 Information with Facebook.

25 115. Plaintiff McCulley used and continues to use the same devices to maintain
26 and to access an active Facebook account throughout the relevant period for this case.

1 116. Plaintiff McCulley has a continuing interest in ensuring that her Private
2 Information, which, upon information and belief, remains backed up in Defendant's
3 possession, is protected and safeguarded from future unauthorized disclosure(s).

4 117. Plaintiff McCulley would consider using Defendant's services again and/or
5 in greater frequency if she could be assured by Defendant that the violations set forth herein
6 were no longer occurring.

7 ***Plaintiff Blount's Experience***

8 118. As a condition of receiving Defendant's services, Plaintiff Blount disclosed
9 her Private Information to Defendant on numerous occasions, and most recently in April
10 2023.

11 119. Plaintiff Blount has been a patient of Defendant for approximately five years.

12 120. Plaintiff Blount accessed Defendant's Website and Patient Portal on her
13 phone and computer to receive healthcare services from Defendant and at Defendant's
14 direction.

15 121. Plaintiff Blount researched providers, specific health conditions and
16 treatments, looked for Defendant's locations close to her address, and scheduled doctor's
17 appointments for herself via the Defendant's Website and Patient Portal.

18 122. Specifically, Plaintiff Blount utilized Defendant's services for various types
19 of imaging (such as [REDACTED]), emergency room and urgent care
20 treatment (including [REDACTED])
21 appointments.

22 123. Plaintiff Blount also utilized Defendant's Patient Portal to complete patient
23 forms, refill prescriptions, look at her bills and payments and to see her test results.

24 124. Plaintiff Blount has used and continues to use the same devices to maintain
25 and access an active Facebook account throughout the relevant period in this case.

26 125. Plaintiff Blount reasonably expected that her communications with
27 Defendant via the Web Properties were confidential, solely between herself and Defendant,
28

1 and that such communications would not be transmitted to or intercepted by a third party.
2 However, and as a result of the Meta Pixels Defendant chose to install on its Website,
3 Plaintiff Blount's Private Information was intercepted, viewed, analyzed and used by
4 unauthorized third parties.

5 126. Defendant transmitted Plaintiff Blount's Facebook ID, computer IP address
6 and other device and unique online identifiers to Facebook. Defendant also transmitted
7 information such as health and medical information including Plaintiff's particular health
8 condition, the type of medical treatment sought, patient status and the fact that Plaintiff
9 attempted to or did book a medical appointment.

10 127. Plaintiff Blount never consented to the disclosure of or use of her Private
11 Information by third parties or to Defendant enabling third parties, including Facebook, to
12 access or interpret such information. Plaintiff Blount never consented to any third parties'
13 receipt or use of her Private Information.

14 128. Notwithstanding, through the Meta Pixels and similar technologies
15 embedded on Defendant's Web Properties, Defendant transmitted Plaintiff Blount's
16 Private Information to, at a minimum, Facebook and likely many other third parties like
17 Google, Bing, and others.

18 129. As a result, Plaintiff Blount received targeted ads on Facebook or Instagram
19 related to her specific medical conditions and/or treatments, including [REDACTED]
20 [REDACTED] medications, "alternative treatments," and clinical trials.

21 130. By making these disclosures without her consent, Defendant breached
22 Plaintiff Blount's privacy and unlawfully disclosed her Private Information.

23 131. Defendant did not inform Plaintiff Blount that it had shared her Private
24 Information with Facebook.

25 132. Plaintiff Blount used and continues to use the same devices to maintain and
26 to access an active Facebook account throughout the relevant period for this case.

1 133. Plaintiff Blount has a continuing interest in ensuring that her Private
2 Information, which, upon information and belief, remains backed up in Defendant's
3 possession, is protected and safeguarded from future unauthorized disclosure(s).

4 134. Plaintiff Blount would consider using Defendant's services again and/or in
5 greater frequency if she could be assured by Defendant that the violations set forth herein
6 were no longer occurring.

7 ***Plaintiff Freriks' Experience***

8 135. Plaintiff Freriks, was Defendant's patient, received healthcare services from
9 2014 through 2020 at hospitals and clinics in Defendant's network and has used
10 Defendant's Website to communicate Private Information to Defendant on numerous
11 occasions since she first engaged Defendant for healthcare services. She has used her
12 account to access the Website and use various digital services provided by Defendant since
13 at least 2015.

14 136. Plaintiff has been a Facebook user since at least 2008.

15 137. Plaintiff has had a Google account since at least 2015.

16 138. On numerous occasions, Plaintiff Freriks accessed Defendant's Website on
17 her iPad and mobile device to conduct the following activities: request and schedule
18 appointments, communicate with healthcare professionals, search for specialists, complete
19 medical forms, and request and review healthcare and billing records.

20 139. In particular, Plaintiff Freriks has used Defendant's Website to [REDACTED]
21 [REDACTED]
22 [REDACTED]

23 140. Plaintiff Freriks never consented to the disclosure of or use of her Private
24 Information. Plaintiff Freriks never consented to any third parties' receipt or use of her
25 Private Information.

26 141. Plaintiff communicated with Defendant about her past, present, and future
27 medical care and treatment via the Website. Because Defendant utilized the Facebook
28

Pixel, the Website's Source Code sent a secret set of instructions back to the individual's browser, causing the Pixel to send Plaintiff's FID, the Pixel ID, and both the webpage's and, upon information and belief, MyChart portal's URLs to Facebook.

142. Pursuant to the systematic process described in this Complaint, Plaintiff's Private Information thus was disclosed to Facebook, and this data included Plaintiff's PII, PHI, and related confidential information.

143. After searching for symptoms, specialists, and treatments on Defendant's Website, Plaintiff observed advertisements on her Facebook account related to her medical conditions and treatments sought through Banner Health.

144. Plaintiff Freriks has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future unauthorized disclosure.

Plaintiff Schreidl's Experience

145. As a condition of receiving Defendant's services, Plaintiff Schreidl disclosed her Private Information to Defendant on numerous occasions, and most recently in November 2023.

146. Plaintiff Schreidl has been a patient of Defendant since October 2022.

147. Plaintiff Schreidl accessed Defendant's Website and Patient Portal on her phone and laptop to receive healthcare services from Defendant and at Defendant's direction.

148. Plaintiff Schreidl used Defendant's services to request and book doctor's appointments for herself, research specific health conditions and treatments, and complete patient web forms.

149. Specifically, Plaintiff Schreidl utilized Defendant's services for many of her medical needs, including her visits to her primary doctor and specialists (including her [REDACTED]), diagnostic tests (such as [REDACTED]), and treatments for her medical conditions, such as [REDACTED].

150. Plaintiff Schreidl also utilized Defendant's Patient Portal to request appointments, complete patient web forms, pay medical bills, refill prescriptions and to see her test results.

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

152. Plaintiff Schreidl reasonably expected that her communications with Defendant via the Web Properties were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

153. However, and as a result of the Meta Pixels Defendant chose to install on its Website, Plaintiff Schreidl's Private Information was intercepted, viewed, analyzed and used by unauthorized third parties.

154. Defendant transmitted Plaintiff Schreidl's Facebook ID, computer IP address and other device and unique online identifiers to Facebook. Defendant also transmitted information such as health and medical information including Plaintiff's particular health condition, the type of medical treatment sought, patient status and the fact that Plaintiff attempted to or did book a medical appointment.

155. Plaintiff Schreidl never consented to the disclosure of or use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information. Plaintiff Schreidl never consented to any third parties' receipt or use of her Private Information.

156. Notwithstanding, through the Meta Pixels and similar technologies embedded on Defendant's Website, Defendant transmitted Plaintiff Schreidl's Private Information to, at a minimum, Facebook and likely many other third parties like Google, Bing and others.

157. As a result, Plaintiff Schreidl received targeted ads on Facebook or Instagram related to her specific medical conditions and/or treatments, such as ads for [REDACTED]

1 158. By making these disclosures without her consent, Defendant breached
2 Plaintiff Schreidl's privacy and unlawfully disclosed her Private Information.

3 159. Defendant did not inform Plaintiff Schreidl that it had shared her Private
4 Information with Facebook.

5 160. Plaintiff Schreidl used and continues to use the same devices to maintain and
6 to access an active Facebook account throughout the relevant period for this case.

7 161. Plaintiff Schreidl has a continuing interest in ensuring that her Private
8 Information, which, upon information and belief, remains backed up in Defendant's
9 possession, is protected and safeguarded from future unauthorized disclosure(s).

10 162. Plaintiff Schreidl would consider using Defendant's services again and/or in
11 greater frequency if she could be assured by Defendant that the violations set forth herein
12 were no longer occurring.

13 ***Plaintiff Santiago-Laboy's Experience***

14 163. Plaintiff Santiago-Laboy, is Defendant's patient, has received healthcare
15 services since before 2013 through the present at hospitals and clinics in Defendant's
16 network and has used Defendant's Website to communicate Private Information to
17 Defendant on numerous occasions since he first engaged Defendant for healthcare services.
18 She has used her account to access the Website and use various digital services provided
19 by Defendant since at least 2019.

20 164. Plaintiff has been a Facebook user since at least 2007.

21 165. Plaintiff has had a Google account since at least 2017.

22 166. On numerous occasions, Plaintiff accessed Defendant's Website on her
23 computer and mobile device to conduct the following activities: request and schedule
24 appointments, communicate with healthcare professionals, search for specialists, complete
25 medical forms, and request and review healthcare and billing records.

1 167. In particular, Plaintiff has used Defendant's Website to research and find

2 [REDACTED]
3 [REDACTED]
4 168. Plaintiff Santiago-Laboy never consented to the disclosure of or use of her
5 Private Information. Plaintiff Santiago-Laboy never consented to any third parties' receipt
6 or use of her Private Information.

7 169. Plaintiff communicated with Defendant about her past, present, and future
8 medical care and treatment via the Website. Because Defendant utilized the Facebook
9 Pixel, the Website's Source Code sent a secret set of instructions back to the individual's
10 browser, causing the Pixel to send Plaintiff's FID, the Pixel ID, and both the webpage's
11 and, upon information and belief, MyChart portal's URLs to Facebook.

12 170. Pursuant to the systematic process described in this Complaint, Plaintiff's
13 Private Information thus was disclosed to Facebook, and this data included Plaintiff's PII,
14 PHI, and related confidential information.

15 171. After searching for [REDACTED] on Defendant's
16 Website, Plaintiff observed advertisements on her Facebook account related to her medical
17 conditions and treatments sought through Banner Health, [REDACTED]
18 [REDACTED].

19 172. Plaintiff Santiago-Laboy has a continuing interest in ensuring that her Private
20 Information, which, upon information and belief, remains backed up in Defendant's
21 possession, is protected and safeguarded from future unauthorized disclosure.

22 ***Plaintiff Irazaba's Experience***

23 173. Plaintiff Irazaba, as Defendant's patient, has received healthcare services
24 from 2010 through the present at hospitals and clinics in Defendant's network and has used
25 Defendant's Website to communicate Private Information to Defendant on numerous
26 occasions since he first engaged Defendant for healthcare services. He has used his account
27
28

1 to access the Website and use various digital services provided by Defendant since at least
2 2019 at Defendant's direction.

3 174. Plaintiff Irazaba has been a Facebook user since at least 2013.

4 175. Plaintiff Irazaba has had a Google account since at least 2018.

5 176. On numerous occasions, Plaintiff accessed Defendant's Website on his
6 mobile device to conduct the following activities: request and schedule appointments,
7 complete medical forms, and request and review healthcare and billing records.

8 177. In particular, Plaintiff has used Defendant's Website to search for [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED].

12 178. Plaintiff Irazaba never consented to the disclosure of or use of his Private
13 Information. Plaintiff Irazaba never consented to any third parties' receipt or use of his
14 Private Information.

15 179. Plaintiff Irazaba communicated with Defendant about his past, present, and
16 future medical care and treatment via the Website. Because Defendant utilized the
17 Facebook Pixel, the Website's Source Code sent a secret set of instructions back to the
18 individual's browser, causing the Pixel to send Plaintiff's FID, the Pixel ID, and both the
19 webpage's and, upon information and belief, MyChart portal's URLs to Facebook.

20 180. Pursuant to the systematic process described in this Complaint, Plaintiff's
21 Private Information thus was disclosed to Facebook, and this data included Plaintiff's PII,
22 PHI, and related confidential information.

23 181. After searching for [REDACTED]
24 [REDACTED] on Defendant's Website, Plaintiff observed advertisements on his Facebook
25 account related to his specific medical conditions and treatments sought through Banner
26 Health, such as ads [REDACTED].
27
28

1 182. Plaintiff Irzaba has a continuing interest in ensuring that his Private
2 Information, which, upon information and belief, remains backed up in Defendant's
3 possession, is protected and safeguarded from future unauthorized disclosure.

4 ***Plaintiff Williams' Experience***

5 183. Plaintiff has a Facebook account and has been a user of Facebook since 2009
6 Plaintiff has been using the Website since 2021 to search for medical information related
7 to her health conditions, to assess her [REDACTED] through the Website's [REDACTED]
8 assessment, and to assess her health needs and access other information related to her health
9 conditions. Ms. Williams similarly used the Website's search function to search for
10 information related to [REDACTED]. Ms. Williams was
11 encouraged to utilize the Website for these functions as one of the first results that popped
12 up when Ms. Williams searched for "health assessments" online was the Website's health
13 assessment function. Ms. William's Facebook profile contains information like her name,
14 occupation, place of residence, and other personal information.

15 184. After utilizing the Website to search for information related to her health
16 condition, Ms. Williams received various targeted advertisements on her Facebook page
17 related to her use of the Website.

18 ***Plaintiff Robeson's Experience***

19 185. As a condition of receiving Defendant's services, Plaintiff Robeson disclosed
20 her Private Information to Defendant on numerous occasions, and most recently in July or
21 August of 2023.

22 186. Plaintiff Robeson has been a patient of Defendant since approximately 2018.

23 187. Plaintiff Robeson accessed Defendant's Website and Patient Portal on her
24 phone, laptop, tablet and computer to receive healthcare services from Defendant and at
25 Defendant's direction.

1 188. Plaintiff Robeson used Defendant's services to request and book doctor's
2 appointments for herself, research specific health conditions and treatments, and complete
3 patient web forms.

4 189. Specifically, Plaintiff Robeson utilized Defendant's services for all of her
5 medical needs, including her visits to her primary doctor and specialists (including her
6 [REDACTED]), diagnostic tests (such as [REDACTED]
7 [REDACTED]), and treatments
8 for her medical conditions, including but not limited to, [REDACTED]
9 [REDACTED].

10 190. Plaintiff Robeson also utilized Defendant's Patient Portal to refill
11 prescriptions and to see her test results.

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

14 192. Plaintiff Robeson reasonably expected that her communications with
15 Defendant via the Web Properties were confidential, solely between herself and Defendant,
16 and that such communications would not be transmitted to or intercepted by a third party.

17 193. However, and as a result of the Meta Pixels Defendant chose to install on its
18 Website, Plaintiff Robeson's Private Information was intercepted, viewed, analyzed and
19 used by unauthorized third parties.

20 194. Defendant transmitted Plaintiff Robeson's Facebook ID, computer IP
21 address and other device and unique online identifiers to Facebook. Defendant also
22 transmitted information such as health and medical information including Plaintiff's
23 particular health condition, the type of medical treatment sought, patient status and the fact
24 that Plaintiff attempted to or did book a medical appointment.

25 195. Plaintiff Robeson never consented to the disclosure of or use of her Private
26 Information by third parties or to Defendant enabling third parties, including Facebook, to
27

1 access or interpret such information. Plaintiff Robeson never consented to any third
2 parties' receipt or use of her Private Information.

3 196. Notwithstanding, through the Meta Pixels and similar technologies
4 embedded on Defendant's Website, Defendant transmitted Plaintiff Robeson's Private
5 Information to, at a minimum, Facebook and likely many other third parties like Google,
6 Bing and others.

7 197. As a result, Plaintiff Robeson received targeted ads on Facebook or
8 Instagram related to her specific medical conditions and/or treatments, including but not
9 limited to, ads for biologic drugs and medications for [REDACTED].

10 198. By making these disclosures without her consent, Defendant breached
11 Plaintiff Robeson's privacy and unlawfully disclosed her Private Information.

12 199. Defendant did not inform Plaintiff Robeson that it had shared her Private
13 Information with Facebook.

14 200. Plaintiff Robeson used and continues to use the same devices to maintain and
15 to access an active Facebook account throughout the relevant period for this case.

16 201. Plaintiff Robeson has a continuing interest in ensuring that her Private
17 Information, which, upon information and belief, remains backed up in Defendant's
18 possession, is protected and safeguarded from future unauthorized disclosure(s).

19 202. Plaintiff Robeson would consider using Defendant's services again and/or in
20 greater frequency if she could be assured by Defendant that the violations set forth herein
21 were no longer occurring.

22 ***Plaintiff Carroll's Experience***

23 203. As a condition of receiving Defendant's services, Plaintiff Carroll disclosed
24 her Private Information to Defendant on numerous occasions, and most recently in
25 November 2023.

26 204. Plaintiff Carroll has been a patient of Defendant since at least 2019.

205. Plaintiff Carroll accessed Defendant's Website and Patient Portal on her phone, desktop and laptop to receive healthcare services from Defendant and at Defendant's direction.

206. Plaintiff Carroll used Defendant's services to review doctors and communicate with her providers, research specific health conditions and treatments, and complete patient web forms.

207. Specifically, Plaintiff Carroll utilized Defendant's services for many of her medical needs, including her visits to her primary doctor and specialists including her [REDACTED], diagnostic tests such as x-rays, and treatments for her medical conditions, such as [REDACTED].

208. Plaintiff Carroll also utilized Defendant's Patient Portal to request appointments, complete patient web forms, pay medical bills, refill prescriptions and to see her test results.

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

210. Plaintiff Carroll reasonably expected that her communications with Defendant via the Web Properties were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

211. However, and as a result of the Meta Pixels Defendant chose to install on its Website, Plaintiff Carroll's Private Information was intercepted, viewed, analyzed and used by unauthorized third parties.

212. Defendant transmitted Plaintiff Carroll's Facebook ID, computer IP address and other device and unique online identifiers to Facebook. Defendant also transmitted information such as health and medical information including Plaintiff's particular health condition, the type of medical treatment sought, patient status and the fact that Plaintiff attempted to or did book a medical appointment.

1 213. Plaintiff Carroll never consented to the disclosure of or use of her Private
2 Information by third parties or to Defendant enabling third parties, including Facebook, to
3 access or interpret such information. Plaintiff Carroll never consented to any third parties'
4 receipt or use of her Private Information.

5 214. Notwithstanding, through the Meta Pixels and similar technologies
6 embedded on Defendant's Website, Defendant transmitted Plaintiff Carroll's Private
7 Information to, at a minimum, Facebook and likely many other third parties like Google,
8 Bing and others.

9 215. As a result, Plaintiff Carroll received targeted ads on Facebook or Instagram
10 related to her specific medical conditions and/or treatments, such as ads for [REDACTED]
11 [REDACTED]

12 216. By making these disclosures without her consent, Defendant breached
13 Plaintiff Carroll's privacy and unlawfully disclosed her Private Information.

14 217. Defendant did not inform Plaintiff Carroll that it had shared her Private
15 Information with Facebook.

16 218. Plaintiff Carroll used and continues to use the same devices to maintain and
17 to access an active Facebook account throughout the relevant period for this case.

18 219. Plaintiff Carroll has a continuing interest in ensuring that her Private
19 Information, which, upon information and belief, remains backed up in Defendant's
20 possession, is protected and safeguarded from future unauthorized disclosure(s).

21 220. Plaintiff Carroll would consider using Defendant's services again and/or in
22 greater frequency if she could be assured by Defendant that the violations set forth herein
23 were no longer occurring.

24 ***Common Plaintiff Allegations***

25 221. Defendant intercepted and/or assisted these interceptions of Plaintiffs'
26 communications without Plaintiffs' knowledge, consent, or express written authorization.

1 By failing to receive the requisite consent, Defendant breached confidentiality and
2 unlawfully disclosed Plaintiffs' Private Information.

3 222. As Defendant's patients, Plaintiffs reasonably expected that their online
4 communications with Defendant were solely between themselves and Defendant and that
5 such communications would not be transmitted to or disclosed to a third party. But for their
6 status as Defendant's patients, Plaintiffs would not have disclosed their Private Information
7 to Defendant.

8 223. During their time as Defendant's patients, Plaintiffs never consented to the
9 use of their Private Information by third parties or to Defendant enabling third parties,
10 including Facebook, to access or interpret such information.

11 224. Notwithstanding, through the Tracking Tools, Defendant transmitted
12 Plaintiffs' Private Information to third parties, such as Facebook and Google.

13 225. During the same transmissions, the Website routinely provides Facebook and
14 Google with its patients' IP addresses, and/or device IDs (and, in the case of Facebook,
15 their FIDs) or other information they input into Defendant's Website, like their home
16 address, zip code, or phone number. This is precisely the type of information that HIPAA
17 requires healthcare providers to anonymize to protect the privacy of patients. Plaintiffs'
18 and Class Members identities could be easily determined based on the FID, IP address
19 and/or reverse lookup from the collection of other identifying information that was
20 improperly disclosed.

21 226. After intercepting and collecting this information, Facebook and Google
22 process it, analyze it, and assimilate it into datasets like Core Audiences and Custom
23 Audiences. If the Website visitor is also a Facebook user, Facebook will associate the
24 information that it collects from the visitor with a Facebook ID that identifies their name
25
26
27
28

1 and Facebook profile, i.e., their real-world identity.²⁷ If the patient is a Google user, Google
2 similarly is able to identify the patient.

3 227. Based on the presence of the Pixels and, upon information and good faith
4 belief, Conversions API on Defendant's Website, Defendant unlawfully disclosed
5 Plaintiffs' Private Information to Facebook. The presence of Facebook advertisements
6 confirms Defendant's unlawful transmission of Plaintiffs' Private Information to
7 Facebook. Said differently, Plaintiffs did not disclose this Private Information to any other
8 source—only to Defendant via Defendant's Online Properties.

9 228. In sum, Defendant's Tracking Tools transmitted Plaintiffs' highly sensitive
10 communications and Private Information to Facebook and Google, including
11 communications that contained private and confidential information, without Plaintiffs'
12 knowledge, consent, or express written authorization.

13 229. Plaintiffs suffered injuries in the form of (i) invasion of privacy; (ii)
14 diminution of value of the Private Information; (iii) statutory damages; (iv) the continued
15 and ongoing risk to their Private Information; and (v) the continued and ongoing risk of
16 harassment, spam, and targeted advertisements specific to Plaintiffs' medical conditions
17 and other confidential information they communicated to Defendant via its Online
18 Properties.

19 230. Plaintiffs have a continuing interest in ensuring that future communications
20 with Defendant are protected and safeguarded from future unauthorized disclosure.
21
22
23

24 ²⁷ A user's Facebook Profile ID is linked to their Facebook profile, which generally
25 contains a wide range of demographic and other information about the user, including
26 pictures, personal interests, work history, relationship status, and other details. Because the
27 user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—
28 or any ordinary person—can easily use the Facebook Profile ID to quickly and easily
locate, access, and view the user's corresponding Facebook profile.

G. Defendant’s Conduct Is Unlawful and Violated Industry Norms

i. Defendant Violated HIPAA Standards

231. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients’ express written authorization.²⁸

232. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, “establishes national standards to protect individuals’ medical records and other individually identifiable health information (collectively defined as ‘protected health information’) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.”²⁹

233. The Privacy Rule broadly defines “protected health information” (“PHI”) as individually identifiable health information (“IIHI”) that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

234. IIHI is defined as “a subset of health information, including demographic information collected from an individual” that is: (1) “created or received by a health care provider, health plan, employer, or health care clearinghouse”; (2) “[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual”; and (3) either (a) “identifies the individual” or (b) “[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103.

²⁸ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

²⁹ HHS.gov, HIPAA For Professionals (last visited Nov. 12, 2023), <https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html>.

235. Under the HIPPA de-identification rule, “health information is not individually identifiable only if”: (1) an expert “determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information” and “documents the methods and results of the analysis that justify such determination”; or (2) “the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

A. Names;

H. Medical record numbers;

J. Account numbers;

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; ... and

R. Any other unique identifying number, characteristic, or code...; and”

The covered entity must not “have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”

45 C.F.R. § 160.514.

236. The HIPAA Privacy Rule requires any “covered entity”—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

237. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 (“Part C”): “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health

information relating to an individual.” The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320d-6.

238. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

239. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall “be fined not more than \$250,000, imprisoned not more than 10 years, or both.”

240. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the HHS instructs:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.³⁰

241. In its guidance for Marketing, the HHS further instructs:

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for

³⁰https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022).

marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.* (Emphasis added).³¹

242. As alleged above, there is an HHS Bulletin that highlights the obligations of "regulated entities," which are HIPAA-covered entities and business associates, when using tracking technologies.³²

243. The Bulletin expressly provides that "[r]egulated 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."

244. Defendant's actions violated HIPAA Rules per this Bulletin.

ii. Defendant Violated Industry Standards

245. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

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

247. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care... Patient privacy encompasses a number of aspects, including, ... personal data (informational privacy)

248. AMA Code of Medical Ethics Opinion 3.2.4 provides:

Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only

³¹<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf> (last visited Nov. 3, 2022).

³² See HHS Bulletin *supra*, note 5.

1 provide data that has been de-identified. [and] (b) Fully inform each patient
 2 whose record would be involved (or the patient's authorized surrogate when
 the individual lacks decision-making capacity about the purposes for which
 access would be granted.

3 249. AMA Code of Medical Ethics Opinion 3.3.2 provides:

4 Information gathered and recorded in association with the care of a patient is
 confidential, regardless of the form in which it is collected or stored.
 5 Physicians who collect or store patient information
 electronically...must...:(c) release patient information only in keeping
 6 ethics guidelines for confidentiality.

7 **H. Plaintiffs' and Class Members' Expectation of Privacy**

8 250. Plaintiffs and Class Members were aware of Defendant's duty of
 9 confidentiality when they sought medical services from Defendant.

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

14 252. Plaintiffs and Class Members would not have used Defendant's Online
 15 Properties, would not have provided their Private Information to Defendant, and would not
 16 have paid for Defendant's healthcare services, or would have paid less for them, had they
 17 known that Defendant would disclose their Private Information to third parties.

18 **I. IP Addresses Are PII**

19 253. On information and belief, through the use of the Tracking Tools on
 20 Defendant's Website, Defendant also disclosed and otherwise assisted third parties with
 21 intercepting Plaintiffs' and Class Members' Computer IP addresses.

22 254. An IP address is a number that identifies the address of a device connected
 23 to the Internet.

24 255. IP addresses are used to identify and route communications on the Internet.

25 256. IP addresses of individual Internet users are used by Internet service
 26 providers, websites, and third-party tracking companies to facilitate and track Internet
 27 communications.

1 257. Facebook tracks every IP address ever associated with a Facebook user, and
2 uses that information for targeting individual homes and their occupants with advertising.

3 258. As to Google, over 70% of online websites use Google’s visitor-tracking
4 products, Google Analytics and Google Ad Manager.

5 259. Whenever a user visits a website that is running Google Analytics and
6 Google Ad Manager, Google’s software scripts on the website surreptitiously direct the
7 user’s browser to send a secret, separate message to Google’s servers in California, which
8 includes the user’s IP address, the user’s geolocation, information contained in Google
9 cookies, any user-ID issued by the website to the user, and information about the browser
10 the user is using.

11 260. Under HIPAA, an IP address is considered PII.³³

12 261. HIPAA further declares information as personally identifiable where the
13 covered entity has “actual knowledge that the information to identify an individual who is
14 a subject of the information.”³⁴

15 262. Consequently, by disclosing IP addresses, Defendant’s business practices
16 violated HIPAA and industry privacy standards.

17 **J. Defendant Was Enriched and Benefitted from the Use of The Tracking Tools**
18 **and Unauthorized Disclosures**

19 263. The primary motivation and a determining factor in Defendant’s interception
20 and disclosure of Plaintiffs’ and Class Members’ Private Information was to commit
21 criminal and tortious acts in violation of federal and state laws as alleged herein, namely,
22 the use of patient data for advertising in the absence of express written consent.
23 Defendant’s further use of the Private Information after the initial interception and
24 disclosure for marketing and revenue generation was in violation of HIPAA and an
25 invasion of privacy. In exchange for disclosing the Private Information of its patients,

26 ³³ HIPAA defines PII to include “any unique identifying number, characteristic or code”
27 and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

28 ³⁴ 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

1 Defendant is compensated by Facebook and Google in the form of enhanced advertising
2 services and more cost-efficient marketing on its platform.

3 264. Retargeting is a form of online marketing that targets users with ads based
4 on their previous internet communications and interactions.

5 265. Upon information and belief, as part of its marketing campaign, Defendant
6 re-targeted patients and potential patients to get more patients to use its services. Defendant
7 did so through use of the intercepted patient data it obtained, procured, and/or disclosed in
8 the absence of express written consent.

9 266. By utilizing the Tracking Tools, the cost of advertising and retargeting was
10 reduced through further use of the unlawfully intercepted and disclosed Private
11 Information, thereby benefitting Defendant while invading the privacy of Plaintiffs and
12 Class Members and violating their rights under federal and Arizona law.

13 **K. Plaintiffs' and Class Members' Private Information Had Financial Value**

14 267. Plaintiffs' data and Private Information has economic value. Facebook
15 regularly uses data that it acquires to create Core and Custom Audiences, as well as
16 Lookalike Audiences and then sells that information to advertising clients. Google has
17 recognized the value of user data and has even instituted a pilot program in which it pays
18 users \$3 per week to track them online.

19 268. Data harvesting is one of the fastest growing industries in the country, and
20 consumer data is so valuable that it has been described as the "new oil." Conservative
21 estimates suggest that in 2018, Internet companies earned \$202 per American user from
22 mining and selling data. That figure is only due to keep increasing; estimates for 2022 are
23 as high as \$434 per user, for a total of more than \$200 billion industry wide.

24 269. The value of health data in particular is well-known and has been reported
25 on extensively in the media. For example, Time Magazine published an article in 2017
26 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it
27

1 described the extensive market for health data and observed that the market for information
2 was both lucrative and a significant risk to privacy.³⁵

3 270. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-
4 identified patient data has become its own small economy: There’s a whole market of
5 brokers who compile the data from providers and other health-care organizations and sell
6 it to buyers.”³⁶

7 271. Indeed, numerous marketing services and consultants offering advice to
8 companies on how to build their email and mobile phone lists—including those seeking to
9 take advantage of targeted marketing—direct putative advertisers to offer consumers
10 something of value in exchange for their personal information. “No one is giving away
11 their email address for free. Be prepared to offer a book, guide, webinar, course or
12 something else valuable.”³⁷

13 272. There is also a market for data in which consumers can participate. Personal
14 information has been recognized by courts as extremely valuable. *See In re Marriott Int’l,*
15 *Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (“Neither
16 should the Court ignore what common sense compels it to acknowledge—the value that
17 personal identifying information has in our increasingly digital economy. Many
18 companies, like Marriott, collect personal information. Consumers too recognize the value
19 of their personal information and offer it in exchange for goods and services.”).

20 273. Several companies have products through which they pay consumers for a
21 license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are
22 all companies that pay for browsing historical information.

24 ³⁵ See <https://time.com/4588104/medical-data-industry/> (last visited February 16, 2023).

25 ³⁶ See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited March 1, 2023).

26 ³⁷ VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER
27 <https://www.getvero.com/resources/twitter-lead-generation-cards/>. (last visited Nov. 1,
28 2023).

274. Facebook also has paid users for their digital information, including browsing history. Until 2019, Facebook ran a “Facebook Research” app through which it paid \$20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

275. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to \$250 per record on the black market.³⁸

TOLLING

276. Any applicable statute of limitations has been tolled by the “delayed discovery” rule. Plaintiffs did not know (and had no way of knowing) that their PII and PHI was intercepted and unlawfully disclosed to Facebook, Google and potentially other third parties because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

277. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated (“the Class”) pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

278. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

All individuals residing in the United States who are, or were, patients of Defendant or any of its affiliates, used Defendant’s Website, and had their Private Information disclosed to a third party without authorization.

279. The Arizona Class Plaintiffs Blount, Santiago-Laboy and Irazaba seek to represent is defined as:

All individuals residing in the State of Arizona who are, or were, patients of Defendant or any of its affiliates, used Defendant’s Website, and had their Private Information disclosed to a third party without authorization or consent.

280. The California Class that Plaintiff McCulley seeks to represent is defined as:

All individuals residing in the State of California who are, or were, patients of Defendant or any of its affiliates, used

³⁸ Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, SecureLink (June 30, 2021), <https://www.securelink.com/blog/healthcare-data-new-prize-hackers>.

Defendant's Website, and had their Private Information disclosed to a third party without authorization or consent.

281. The Colorado Class that Plaintiffs Schreidl, Freriks and Robeson seek to represent is defined as:

All individuals residing in the State of Colorado who are, or were, patients of Defendant or any of its affiliates, used Defendant's Website, and had their Private Information disclosed to a third party without authorization or consent.

282. The Nationwide Class, Arizona Class, California Class, and Colorado Class are collectively referred to as the "Class" unless otherwise and more specifically identified.

283. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

284. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

285. Numerosity, Fed. R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of thousands of individuals whose PII and PHI may have been improperly disclosed to Facebook, and the Class is identifiable within Defendant's records.

286. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;
- b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

- c. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;
- d. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;
- e. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;
- f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;
- g. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct; and
- h. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their Private Information.

287. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

288. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

1 289. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an
2 appropriate method for fair and efficient adjudication of the claims involved. Class action
3 treatment is superior to all other available methods for the fair and efficient adjudication of
4 the controversy alleged herein; it will permit a large number of Class Members to prosecute
5 their common claims in a single forum simultaneously, efficiently, and without the
6 unnecessary duplication of evidence, effort, and expense that hundreds of individual
7 actions would require. Class action treatment will permit the adjudication of relatively
8 modest claims by certain Class Members, who could not individually afford to litigate a
9 complex claim against a large corporation like Defendant. Further, even for those Class
10 Members who could afford to litigate such a claim, it would still be economically
11 impractical and impose a burden on the courts.

12 290. Policies Generally Applicable to the Class. Fed. R. Civ. P. 23(b)(2). This
13 class action is also appropriate for certification because Defendant has acted or refused to
14 act on grounds generally applicable to the Class, thereby requiring the Court's imposition
15 of uniform relief to ensure compatible standards of conduct toward the Class Members and
16 making final injunctive relief appropriate with respect to the Class as a whole. Defendant's
17 policies challenged herein apply to and affect Class Members uniformly and Plaintiffs'
18 challenge of these policies hinges on Defendant's conduct with respect to the Class as a
19 whole, not on facts or law applicable only to Plaintiff.

20 291. The nature of this action and the nature of laws available to Plaintiffs and
21 Class Members make the use of the class action device a particularly efficient and
22 appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs
23 alleged because Defendant would necessarily gain an unconscionable advantage since they
24 would be able to exploit and overwhelm the limited resources of each individual Class
25 Member with superior financial and legal resources; the costs of individual suits could
26 unreasonably consume the amounts that would be recovered; proof of a common course of
27 conduct to which Plaintiffs were exposed is representative of that experienced by the Class
28

1 and will establish the right of each Class Member to recover on the cause of action alleged;
2 and individual actions would create a risk of inconsistent results and would be unnecessary
3 and duplicative of this litigation.

4 292. The litigation of the claims is manageable. Defendant's uniform conduct, the
5 consistent provisions of the relevant laws, and the ascertainable identities of Class
6 Members demonstrate that there would be no significant manageability problems with
7 prosecuting this lawsuit as a class action.

8 293. Adequate notice can be given to Class Members directly using information
9 maintained in Defendant's records.

10 294. Unless a class-wide injunction is issued, Defendant may continue disclosing
11 the Private Information of Class Members, Defendant may continue to refuse to provide
12 proper notification to Class Members regarding the practices complained of herein, and
13 Defendant may continue to act unlawfully as set forth in this Complaint.

14 295. Further, Defendant has acted or refused to act on grounds generally
15 applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief
16 with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the
17 Federal Rules of Civil Procedure.

18 296. Issue Certification, Fed. R. Civ. P. 23(c)(4). Likewise, particular issues are
19 appropriate for certification because such claims present only particular, common issues,
20 the resolution of which would advance the disposition of this matter and the parties'
21 interests therein. Such particular issues include, but are not limited to, the following:

- 22 a. Whether Defendant owed a legal duty to not disclose Plaintiffs' and
23 Class Members' Private Information;
- 24 b. Whether Defendant breached a legal duty to Plaintiffs and Class
25 Members to exercise due care in collecting, storing, using, and
26 safeguarding their Private Information;

- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;
- e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;
- f. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Class)

297. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

298. Medical providers have a duty to their patients to keep non-public medical information completely confidential, and to safeguard sensitive personal and medical information. This duty arises from the implied covenant of trust and confidence that is inherent in the physician-patient relationship.

299. Medical providers also have a duty to maintain the confidentiality of Plaintiffs' PHI under HIPAA and its implementing regulations.

300. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

1 301. In light of the special relationship between Defendant and Plaintiffs and
2 Class Members, whereby Defendant became a guardian of Plaintiffs' and Class Members'
3 Private Information, Defendant became a fiduciary by its undertaking and guardianship of
4 the Private Information, to act primarily for the benefit of its patients, including Plaintiffs
5 and Class Members: (1) for the safeguarding of Plaintiffs' and Class Members' Private
6 Information; (2) to timely notify Plaintiffs and Class Members of disclosure of their Private
7 Information to unauthorized third parties; and (3) to maintain complete and accurate
8 records of what patient information (and where) Defendant did and does store and disclose.

9 302. Contrary to its duties as a medical provider and its express and implied
10 promises of confidentiality, Defendant installed its Tracking Tools to disclose and transmit
11 to third parties Plaintiffs' and Class Members' communications with Defendant as well as
12 the contents of those communications, including Private Information.

13 303. These disclosures were made for commercial purposes without Plaintiffs' or
14 Class Members' knowledge, consent, or authorization, and were unprivileged.

15 304. The unauthorized disclosures of Plaintiffs' and Class Members' Private
16 Information were intentionally caused by Defendant's employees acting within the scope
17 of their employment. Alternatively, the disclosures of Plaintiffs' and Class Members'
18 Private Information occurred because of Defendant's negligent hiring or supervision of its
19 employees or agents, its failure to establish adequate policies and procedures to safeguard
20 the confidentiality of patient information, or its failure to train its employees or agents to
21 properly discharge their duties under those policies and procedures.

22 305. The third-party recipients included, but may not be limited to, Facebook and
23 Google. Such information was received by these third parties in a manner that allowed
24 them to identify the Plaintiffs and the individual Class Members.

25 306. Defendant's breach of the common law implied covenant of trust and
26 confidence is further evidenced by its failure to comply with federal and state privacy
27 regulations, including:

- a. By failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- b. By failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- c. By failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);
- d. By failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiffs' and Class Members PHI;
- e. By failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. By failing to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);
- g. By impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;
- h. By failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and
- i. By otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

307. The harm arising from a breach of provider-patient confidentiality includes mental suffering due to the exposure of private information and erosion of the essential confidential relationship between the healthcare provider and the patient.

308. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiffs and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiffs and Class members intended to remain private is no longer private;

- b. Plaintiffs and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. General damages for invasion of their rights in an amount to be determined by a jury;
- e. Nominal damages for each independent violation;
- f. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation for such data;
- g. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- h. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information; and
- i. Defendant's actions violated the property rights Plaintiffs and Class members have in their Private Information.

COUNT II
VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
("ECPA")
18 U.S.C. § 2511(1) *et seq.*
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of Plaintiffs and the Class)

309. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

310. The ECPA protects both sending and receipt of communications.

311. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

312. The transmissions of Plaintiffs' Private Information to Defendant via Defendant's Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

1 313. The transmissions of Plaintiffs' Private Information to medical professionals
2 qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

3 314. **Electronic Communications.** The transmission of Private Information
4 between Plaintiffs and Class Members and Defendant via its Website with which they
5 chose to exchange communications are "transfer[s] of signs, signals, writing,...data, [and]
6 intelligence of [some] nature transmitted in whole or in part by a wire, radio,
7 electromagnetic, photoelectronic, or photooptical system that affects interstate commerce"
8 and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

9 315. **Content.** The ECPA defines content, when used with respect to electronic
10 communications, to "include[] *any* information concerning the substance, purport, or
11 meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

12 316. **Interception.** The ECPA defines the interception as the "acquisition of the
13 contents of any wire, electronic, or oral communication through the use of any electronic,
14 mechanical, or other device" and "contents ... include any information concerning the
15 substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

16 317. **Electronic, Mechanical, or Other Device.** The ECPA defines "electronic,
17 mechanical, or other device" as "any device ... which can be used to intercept a[n] ...
18 electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices"
19 within the meaning of 18 U.S.C. § 2510(5):

- 20 a. Plaintiffs' and Class Members' browsers;
- 21 b. Plaintiffs' and Class Members' computing devices;
- 22 c. Defendant's web-servers; and
- 23 d. The Pixel deployed by Defendant to effectuate the sending and
24 acquisition of patient communications.

25 318. Whenever Plaintiffs and Class Members interacted with Defendant's
26 Website, Defendant, through the Tracking Tools embedded and operating on its Website,
27 contemporaneously and intentionally disclosed, and endeavored to disclose the contents of
28

1 Plaintiffs' and Class Members' electronic communications to third parties, including
2 Facebook and Google, without authorization or consent, and knowing or having reason to
3 know that the electronic communications were obtained in violation of the ECPA. 18
4 U.S.C. § 2511(1)(c).

5 319. Whenever Plaintiffs and Class Members interacted with Defendant's
6 Website, Defendant, through the Tracking Tools embedded and operating on its Website,
7 contemporaneously and intentionally used, and endeavored to use the contents of
8 Plaintiffs' and Class Members' electronic communications, for purposes other than
9 providing health care services to Plaintiffs and Class Members without authorization or
10 consent, and knowing or having reason to know that the electronic communications were
11 obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

12 320. Whenever Plaintiffs and Class Members interacted with Defendant's
13 Website, Defendant, through the Tracking Tools it embedded and operated on its Website,
14 contemporaneously and intentionally redirected the contents of Plaintiffs' and Class
15 Members' electronic communications while those communications were in transmission,
16 to persons or entities other than an addressee or intended recipient of such communication,
17 including Facebook and Google.

18 321. Defendant's intercepted communications include, but are not limited to, the
19 contents of communications to/from Plaintiffs' and Class Members' regarding PII and PHI,
20 treatment, medication, and scheduling.

21 322. By intentionally disclosing or endeavoring to disclose the electronic
22 communications of Plaintiffs and Class Members to affiliates and other third parties, while
23 knowing or having reason to know that the information was obtained through the
24 interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a),
25 Defendant violated 18 U.S.C. § 2511(1)(c).

26 323. By intentionally using, or endeavoring to use, the contents of the electronic
27 communications of Plaintiffs and Class Members, while knowing or having reason to know
28

1 that the information was obtained through the interception of an electronic communication
2 in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

3 324. Defendant intentionally used the wire or electronic communications to
4 increase its profit margins. Defendant specifically used the Tracking Tools to track and
5 utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

6 325. Defendant was not acting under color of law to intercept Plaintiffs' and Class
7 Members' wire or electronic communication.

8 326. Plaintiffs and Class Members did not authorize Defendant to acquire the
9 content of their communications for purposes of invading Plaintiffs' privacy via the
10 Tracking Tools.

11 327. Any purported consent that Defendant received from Plaintiffs and Class
12 Members was not valid.

13 328. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of
14 Plaintiffs' and Class Members' electronic communications for the purpose of committing
15 a tortious or criminal act in violation of the Constitution or laws of the United States or of
16 any State – namely, violations of HIPAA, and invasion of privacy, among others.

17 329. The ECPA provides that a “party to the communication” may be liable where
18 a “communication is intercepted for the purpose of committing any criminal or tortious act
19 in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C §
20 2511(2)(d).

21 330. Defendant is a “party to the communication” with respect to patient
22 communications. However, Defendant's simultaneous, unknown duplication, forwarding,
23 and interception of Plaintiffs' and Class Members' Private Information does not qualify for
24 the party exemption.

25 331. Defendant's acquisition of patient communications that were used and
26 disclosed to Facebook and Google was done for purposes of committing criminal and
27 tortious acts in violation of the laws of the United States, including.

- a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;
- b. Invasion of Privacy; and
- c. Breach of Contract.

332. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to “use[] or cause[] to be used a unique health identifier” or to “disclose[] individually identifiable health information to another person ... without authorization” from the patient.

333. The penalty for violation is enhanced where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320d-6.

334. Defendant’s conduct violated 42 U.S.C. § 1320d-6 in that it:

- a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and
- b. Disclosed individually identifiable health information to Facebook and Google without patient authorization.

335. Defendant’s conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant’s use of the Facebook and Google source code was for Defendant’s commercial advantage to increase revenue from existing patients and gain new patients.

336. The fbp, ga, and gid cookies, which constitute programs, commanded Plaintiffs’, and Class Members’ computing devices to remove and redirect their data and the content of their communications with Defendant to Google, Facebook, and others.

337. Defendant knew or had reason to know that the fbp, ga, and gid cookies would command Plaintiffs’ and Class Members’ computing devices to remove and redirect their data and the content of their communications with Defendant to Google, Facebook, and others.

338. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs’ and Class Members’ communications

1 about their individually-identifiable patient health information on its Website, because it
 2 used its participation in these communications to improperly share Plaintiffs' and Class
 3 Members' individually-identifiable patient health information with Facebook and Google,
 4 third-parties that did not participate in these communications, that Plaintiff and Class
 5 Members did not know were receiving their individually-identifiable patient health
 6 information, and that Plaintiff and Class Members did not consent to receive this
 7 information.

8 339. Defendant accessed, obtained, and disclosed Plaintiffs' and Class Members'
 9 Private Information for the purpose of committing the crimes and torts described herein
 10 because it would not have been able to obtain the information or the marketing services if
 11 it had complied with the law.

12 340. As such, Defendants cannot viably claim any exception to ECPA liability.

13 341. Plaintiffs and Class Members have suffered damages as a direct and
 14 proximate result of Defendant's invasion of privacy in that:

- 15 a. Learning that Defendant has intruded upon, intercepted, transmitted, shared,
 16 and used their individually identifiable patient health information (including
 17 information about their medical symptoms, conditions, and concerns, medical
 18 appointments, healthcare providers and locations, medications and treatments,
 19 and health insurance and medical bills) for commercial purposes has caused
 20 Plaintiffs and the Class Members to suffer emotional distress;
- 21 b. Defendant received substantial financial benefits from its use of Plaintiffs' and
 22 Class Members' individually identifiable patient health information without
 23 providing any value or benefit to Plaintiff or the Class Members;
- 24 c. Defendant received substantial, quantifiable value from its use of Plaintiffs'
 25 and Class Members' individually identifiable patient health information, such
 26 as understanding how people use its website and determining what ads people
 27 see on its website, without providing any value or benefit to Plaintiffs or the
 28

Class Members;

- d. Defendant has failed to provide Plaintiffs and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and
- e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

342. As a result of Defendant's violation of the ECPA, Plaintiffs and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT III
INVASION OF PRIVACY
(Intrusion upon Seclusion)
(On Behalf of Plaintiffs and the Class)

343. Plaintiffs repeat and re-allege each allegation contained in the Complaint as if fully set forth herein.

344. The Private Information of Plaintiffs and Class Members consists of private and confidential facts and information that were never intended to be shared beyond private communications.

345. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

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

1 347. Defendant owed a duty to Plaintiffs and Class Members not to give publicity
2 to their private lives to Facebook and Google and, by extension, other third-party
3 advertisers and businesses who purchased Facebook's and Google's advertising services.

4 348. Defendant's unauthorized disclosure of Plaintiffs' and Class Members'
5 Private Information to Facebook and Google, third-party social media, and marketing
6 giants, is highly offensive to a reasonable person.

7 349. Defendant's willful and intentional disclosure of Plaintiffs' and Class
8 Members' Private Information constitutes an intentional interference with Plaintiffs' and
9 the Class Members' interest in solitude or seclusion, either as to their person or as to their
10 private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

11 350. Defendant's conduct constitutes an intentional physical or sensory intrusion
12 on Plaintiffs' and Class Members' privacy because Defendant exceeded its authorization
13 to access Plaintiffs' and Class Members' information and facilitated Facebook's and
14 Google's simultaneous eavesdropping and wiretapping of confidential communications.

15 351. Defendant failed to protect Plaintiffs' and Class Members' Private
16 Information and acted knowingly when it installed the Tracking Tools onto its Website
17 because the purpose of the Tracking Tools is to track and disseminate individual's
18 communications with the Website for the purpose of marketing and advertising.

19 352. Because Defendant intentionally and willfully incorporated the Tracking
20 Tools into its Website and encouraged patients to use that Website for healthcare purposes,
21 Defendant had notice and knew that its practices would cause injury to Plaintiffs and Class
22 Members.

23 353. As a proximate result of Defendant's acts and omissions, the private and
24 sensitive PII and PHI of Plaintiffs and the Class Members was disclosed to third parties
25 without authorization, causing Plaintiff and the Class to suffer damages.

26 354. Plaintiffs, on behalf of themselves and Class Members, seek compensatory
27 damages for Defendant's invasion of privacy, which includes the value of the privacy
28

1 interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment
2 interest, and costs.

3 355. Defendant's wrongful conduct will continue to cause great and irreparable
4 injury to Plaintiffs and the Class since their Private Information is still maintained by
5 Defendant and still in the possession of Facebook, Google, and other third parties and the
6 wrongful disclosure of the information cannot be undone.

7 356. Plaintiffs and Class Members have no adequate remedy at law for the injuries
8 relating to Defendant's continued possession of their sensitive and confidential records. A
9 judgment for monetary damages will not undo Defendant's disclosure of the information
10 to Facebook and Google who, on information and belief, continue to possess and utilize
11 that information.

12 357. Plaintiffs, on behalf of themselves and Class Members, further seek
13 injunctive relief to enjoin Defendant from further intruding into the privacy and
14 confidentiality of Plaintiffs' and Class Members' Private Information and to adhere to its
15 common law, contractual, statutory, and regulatory duties.

16 **COUNT IV**
17 **BREACH OF IMPLIED CONTRACT**
18 **(on behalf of Plaintiffs and the Class)**

19 358. Plaintiffs repeat and re-allege every allegation contained in the Complaint as
20 if fully set forth herein.

21 359. As a condition of utilizing Defendant's Website and receiving services from
22 Defendant's healthcare facilities and professionals, Plaintiffs and the Class Members
23 provided their Private Information and compensation for their medical care.

24 360. When Plaintiffs and Class Members provided their Private Information to
25 Defendant, they entered an implied contract pursuant to which Defendant agreed to
26 safeguard and not disclose their Private Information without consent.

1 parties Plaintiffs' and Class Members' communications with Defendant, including Private
2 Information and the contents of such information.

3 377. These disclosures were made without Plaintiffs' or Class Members'
4 knowledge, consent, or authorization, and were unprivileged.

5 378. The third-party recipients included, but may not be limited to, Facebook
6 and/or Google.

7 379. As a direct and proximate cause of Defendant's unauthorized disclosures of
8 patient personally identifiable, non-public medical information, and communications,
9 Plaintiffs and Class members were damaged by Defendant's breach in that:

- 10 a. Sensitive and confidential information that Plaintiffs and Class members
11 intended to remain private is no longer private;
- 12 b. Plaintiff sand Class members face ongoing harassment and embarrassment
13 in the form of unwanted targeted advertisements;
- 14 c. Defendant eroded the essential confidential nature of the provider-patient
15 relationship;
- 16 d. General damages for invasion of their rights in an amount to be determined
17 by a jury;
- 18 e. Nominal damages for each independent violation;
- 19 f. Defendant took something of value from Plaintiffs and Class Members and
20 derived benefit therefrom without Plaintiffs' and Class Members' knowledge
21 or informed consent and without compensation for such data;
- 22 g. Plaintiffs and Class Members did not get the full value of the medical
23 services for which they paid, which included Defendant's duty to maintain
24 confidentiality;
- 25 h. Defendant's actions diminished the value of Plaintiffs' and Class Members'
26 Private Information; and
- 27 i. Defendant's actions violated the property rights Plaintiffs and Class
28 Members have in their Private Information.

COUNT VII

Violations of the Arizona Consumer Fraud Act

A.R.S. § 44-1521, et seq.

(On behalf of Plaintiffs Blount, Santiago-Laboy, Irazaba, & the Arizona Class)

380. Plaintiffs Blount, Santiago-Laboy and Irazaba repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

381. The ACFA states:

The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.

A.R.S. § 44-1522(A).

382. Plaintiffs Blount, Santiago-Laboy and Irazaba, Arizona Class members, and Defendant are “persons” under the ACFA. A.R.S. § 44-1521(6).

383. The services that Defendant provides are “merchandise” under the ACFA. A.R.S. § 44-1521(5).

384. Defendant made uniform representations to Plaintiffs Blount, Santiago-Laboy and Irazaba and Arizona Class Members that their PII/PHI will remain private, as evidenced by, *inter alia*, its privacy policy. Defendants also committed deceptive omissions in violation of the ACFA by failing to inform Plaintiffs and Arizona Class Members that Defendant would disclose their PII/PHI for commercial purposes without consent. Documents that should have contained such disclosures, but did not, include the privacy policy cited in this Complaint.

385. Defendants separately engaged in unfair acts and practices in violation of the ACFA by failing to implement and maintain reasonable security measures to protect and secure Plaintiffs Blount, Santiago-Laboy and Irazaba’s and Class Members’ PII/PHI in a manner that complied with applicable laws, regulations, and industry standards, or alternatively, by intentionally disclosing Plaintiffs Blount, Santiago-Laboy and Irazaba’s

1 and Arizona Class Members' PII/PHI for commercial purposes without consent. Such acts
 2 and practices violate established public policy, are immoral, unethical, oppressive,
 3 unscrupulous, and substantially injurious to consumers.

4 386. Plaintiffs Blount, Santiago-Laboy and Irazaba and Arizona Class Members
 5 have had their privacy invaded and lost property in the form of their PII/PHI. The harm to
 6 Plaintiffs and Arizona Class Members sufficiently outweighs any justifications or motives
 7 for Defendants' practice of disclosing Private Information for commercial purposes
 8 without consent.

9 387. Plaintiffs Blount, Santiago-Laboy and Irazaba and all other Arizona Class
 10 members were damaged by Defendants' violation of the ACFA because: (i) they paid—
 11 directly or through their insurers—for data security protection they did not receive; (ii)
 12 their PII/PHI was improperly disclosed to unauthorized individuals; (iii) the confidentiality
 13 of their PII/PHI has been breached; (iv) they were deprived of the value of their PII/PHI,
 14 for which there is a well-established national and international market; and (v) they
 15 overpaid for the services that were received without adequate data security.

16 388. Plaintiffs Blount, Santiago-Laboy and Irazaba and Arizona Class Members
 17 are entitled to, *inter alia*, nominal, compensatory, and/or statutory damages as a result of
 18 Defendant's unlawful conduct.

19 **COUNT VIII**
 20 **VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA")**
 21 **Cal. Penal Code §§ 630, et seq.**
 22 **(By Plaintiff McCulley & the California Class)**

23 389. Plaintiff McCulley repeats the allegations contained in the paragraphs above
 24 as if fully set forth herein and brings this count individually and on behalf of the California
 25 Class.

26 390. The California Invasion of Privacy Act ("CIPA") is codified at California
 27 Penal Code §§ 630 to 638.

1 391. CIPA represents a fundamental policy of the state of California which cannot
2 be waived or contracted out of.

3 392. CIPA begins with its statement of purpose.

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

11 Cal. Penal Code § 630.

12 393. California Penal Code § 631(a) provides, in pertinent part:

13 Any person who, by means of any machine, instrument, or
14 contrivance, or in any other manner . . . willfully and without the
15 consent of all parties to the communication, or in any unauthorized
16 manner, reads, or attempts to read, or to learn the contents or meaning
17 of any message, report, or communication while the same is in transit
18 or passing over any wire, line, or cable, or is being sent from, or
19 received at any place within this state; or who uses, or attempts to use,
20 in any manner, or for any purpose, or to communicate in any way, any
21 information so obtained, or who aids, agrees with, employs, or
22 conspires with any person or persons to unlawfully do, or permit, or
23 cause to be done any of the acts or things mentioned above in this
24 section, is punishable by a fine not exceeding two thousand five
25 hundred dollars (\$2,500)[.]

26 394. Simply put, a defendant must show it had the consent of all parties to a
27 communication before it can record any portion of that communication.

28 395. At all relevant times, Defendant has been a person that CIPA applies. Cal.
Penal Code §631(a).

 396. At all relevant times, Defendant aided, employed, agreed with, and conspired
with Facebook to track and intercept Plaintiff's and the California Class Members' internet
communications while using Defendant's Website.

 397. These communications were intercepted by a third party during the
communications and without the knowledge, authorization or consent of Plaintiff and
California Class Members.

1 398. Defendant intentionally inserted an electronic device (the Tracking Tools)
2 that, without the knowledge and consent of Plaintiff and Class members, recorded and
3 transmitted their confidential communications with Defendant to a third party.

4 399. Defendant willingly facilitated and aided Facebook's interception and
5 collection of Plaintiff's and California Class Members' Private Information by embedding
6 the Pixel(s) on the Website, thereby assisting Facebook's eavesdropping.

7 400. The following items constitute "machine[s], instrument[s], or
8 contrivance[s]" under the CIPA, and even if they do not, the Pixel falls under the broad
9 catch-all category of "any other manner":

- 10 a. The computer codes and programs Facebook used to track Plaintiff's and
11 California Class Members' communications while they were navigating the
12 Website;
- 13 b. Plaintiff's and California Class Members' browsers;
- 14 c. Plaintiff's and California Class Members' computing and mobile devices;
- 15 d. Facebook's web and ad servers;
- 16 e. The web and ad servers from which Facebook tracked and intercepted
17 Plaintiff's and California Class Members' communications while they were
18 using a web browser to access or navigate the Website;
- 19 f. The computer codes and programs used by Facebook to effectuate its tracking
20 and interception of Plaintiff's and Class Members' communications while they
21 were using a browser to visit the Website; and
- 22 g. The plan Facebook carried out to effectuate its tracking and interception of
23 Plaintiff's and Class Members' communications while they were using a web
24 browser or mobile application to visit the Website.

25 401. Defendant fails to disclose to Users that it is using the Pixel to track and
26 automatically and simultaneously transmit highly sensitive personal communications to a
27 third party, and in fact, expressly disavows using the Pixel on its Website. Defendant is

1 necessarily aware that these communications are confidential as its Website Notice of
2 Privacy Practices acknowledges the confidential nature of private medical information and
3 disclaims that it is being shared with unidentified third parties without Plaintiff's and
4 California Class Members' express authorization. Thus, Defendant is acting in intentional
5 violation of Plaintiff's privacy.

6 402. The patient communication information that Defendant transmits while using
7 the Pixel constitutes protected health information.

8 403. As demonstrated herein, Defendant violates CIPA by aiding and permitting
9 third parties to receive its patients' online communications in real time through its Website
10 without their consent.

11 404. By choosing to install the Pixel and disclosing Plaintiff's and California
12 Class Members' private health information, Defendant violated Plaintiff's and California
13 Class Members' statutorily protected right to privacy.

14 405. As a result of the above violations and pursuant to CIPA Section 637.2,
15 Defendant is liable to Plaintiff and California Class Members for the greater of: a) treble
16 actual damages related to their loss of privacy in an amount to be determined at trial; or b)
17 for statutory damages in the amount of \$5,000 per violation. Penal Code § 637.2
18 specifically states that "[i]t is not a necessary prerequisite to an action pursuant to this
19 section that the Plaintiff has suffered, or be threatened with, actual damages."

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

24 407. Based on the foregoing, Plaintiff and California Class Members seek all other
25 relief as the Court may deem just and proper, including all available monetary relief,
26 injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees
27 and costs.

COUNT IX
VIOLATION OF THE CONFIDENTIALITY OF MEDICAL INFORMATION
ACT (“CMIA”)
Cal. Civ. Code §§ 56, et seq.
(By Plaintiff McCulley & the California Class)

408. Plaintiff McCulley repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the California Class.

409. The California Confidentiality of Medical Information Act, California Civil Code §§ 56, et seq. (“CMIA”) prohibits health care providers from disclosing medical information relating to their patients without patient authorization.

410. “Medical information” refers to “any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care . . . regarding a patient’s medical history, mental or physical condition, or treatment. ‘Individually Identifiable’ means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual[.]” Cal. Civ. Code § 56.05.

411. The CMIA applies to Defendant in all regards. Defendant is a business under Cal. Civil Code §56.06 and therefore, is subject to the requirements of the CMIA, including but not limited to §§56.10 and 56.101.

412. Defendant is a “provider of health care” as defined by California Civil Code § 56.06(b).

413. Plaintiff and California Class Members are patients, and, as a health care provider, Defendant has an ongoing obligation to comply with the CMIA’s requirements.

414. Cal. Civil Code § 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” Section 56.101 of the CMIA states, in pertinent part, that “[a]ny provider of health care . . . or contractor . . . who negligently

1 creates, maintains, preserves, stores, abandons, destroys, or disposes of medical
2 information shall be subject to the remedies and penalties . . .” Cal. Civ. Code §§ 56.10,
3 56.101. Through the conduct described herein, Defendant violated the CMIA, including
4 these sections.

5 415. As set forth above, device identifiers, web URLs, Internet Protocol (IP)
6 addresses and other characteristics that can uniquely identify Plaintiff McCulley and
7 California Class Members are transmitted to Defendant in combination with patient
8 medical conditions, medical concerns, treatment(s) sought by the patients, medical history
9 and other medical information. This is protected health information under the CMIA.

10 416. This private medical information is intercepted and transmitted to Facebook
11 via Defendant’s use of the Pixel and other enabling software on its Website. Facebook ID
12 is also an identifier sufficient to allow identification of an individual. Along with patients’
13 Facebook ID, Defendant discloses to Facebook several pieces of information regarding
14 patients’ use of its Website, including but not limited to the following: patient medical
15 conditions, medical concerns, treatment(s) sought by the patients, medical specialty of the
16 doctor(s) searched for and selected by patients and appointment information.

17 417. Upon information and belief, the private medical information of Plaintiff
18 McCulley and California Class Members that was improperly intercepted and transmitted
19 to Facebook via Defendant’s use of the Pixel was subsequently improperly viewed,
20 accessed, acted upon and otherwise used by Facebook to, among other things, tailor
21 advertisements to them based on their medical conditions and other private medical
22 information for gain.

23 418. The information described above constitutes medical information pursuant
24 to the CMIA because it is patient information derived from a provider of health care
25 regarding patients’ medical treatment and physical condition, and this medical information
26 is linked with individually identifying information. *See* Cal. Civ. Code § 56.05(i).

1 419. As demonstrated herein, Defendant fails to obtain its patients' authorization
2 for the disclosure of medical information and fails to disclose in its Privacy Policy that it
3 shares protected health information with Facebook or other third parties for marketing
4 purposes.

5 420. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of
6 medical information must be:

7 (1) Clearly separate from any other language present on the same page and is
8 executed by a signature which serves no other purpose than to execute the
9 authorization;

10 (2) signed and dated by the patient or her representative;

11 (3) state the name and function of the third party that receives the information; and

12 (4) state a specific date after which the authorization expires.

13 CMIA Section 56.11.

14 421. Further, the Website Notice of Privacy Practices does not require consumers
15 to agree to them by selecting or clicking a "checkbox" presented in a sufficiently
16 conspicuous manner to put Plaintiffs on notice of them. Accordingly, the information set
17 forth in Defendant's Website Privacy Notice does not qualify as a valid authorization.

18 422. As described above, Defendant is intentionally violating the CMIA by
19 choosing to install the Pixel and disclosing its patients' medical information to Facebook
20 along with the patients' individually identifying information. Accordingly, Plaintiff and
21 California Class Members seek all relief available for Defendant's CMIA violations.

22 423. Based on the foregoing, Plaintiff and California Class Members seek nominal
23 damages, compensatory damages, punitive damages, attorneys' fees and costs of litigation
24 for Defendant's violation(s) of the CMIA.

COUNT X
VIOLATION OF THE UNFAIR COMPETITION LAW (“UCL”)
Cal. Bus. & Prof. Code § 17200, et seq. – Unlawful Business Practices
(By Plaintiff McCulley & the California Class)

424. Plaintiff McCulley repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the California Class.

425. Plaintiff McCulley, California Class Members and Defendant are each a “person” under Cal. Bus. & Prof. Code § 17201.

426. The acts, omissions and conduct of Defendant as alleged herein constitute “business practices” within the meaning of the UCL.

427. California Business and Professions Code §§ 17201, et seq., prohibits acts of unfair competition, which includes unlawful business practices.

428. Plaintiff McCulley brings her claim for injunctive relief as she has no confidence that Defendant has altered its privacy practices and she may wish to use Defendant’s services in the future.

429. Plaintiff McCulley brings her claim for restitution in the alternative to her claims for damages.

430. Defendant engaged in unlawful business practices by disclosing Plaintiff McCulley’s and California Class Members’ Private Information to unrelated third parties, including Facebook, without prior consent in violation of the consumer protection and privacy statutes alleged herein.

431. Defendant’s unlawful acts and practices include violations of Plaintiff McCulley’s and Class Member’s constitutional rights to privacy; Cal. Penal Code §§ 630, et. seq. ; Cal. Civ. Code §§ 56, et. seq. ; 18 U.S.C. § 2511(1), et seq.; 18 U.S.C. § 2511(3)(a), et seq.; and 18 U.S.C. § 1030, et seq.

1 432. Because Defendant is in the business of providing medical and mental
2 healthcare services, Plaintiff McCulley and California Class Members relied on Defendant
3 to advise them of any potential disclosure of their private information.

4 433. Plaintiff McCulley and California Class Members were entitled to assume
5 (and did assume) that Defendant would take appropriate measures to keep their private
6 information private and confidential.

7 434. Plaintiff McCulley and the California Class Members reasonably relied upon
8 the representations Defendant made in its Privacy Policy, including those representations
9 concerning the confidentiality of patient information.

10 435. Defendant's failure to disclose that it was sharing Private Information with
11 third parties constitutes a material omission of fact. Additionally, Defendant's express
12 representation that it was not using Tracking Tools on its Website is false and misleading
13 to Defendant's patients and members of the Class.

14 436. Defendant was in sole possession of and had a duty to disclose the material
15 information that Plaintiff McCulley's and California Class Members' Private Information
16 was being shared with a third party.

17 437. Defendant also had a duty to disclose the material information that Plaintiff
18 McCulley's and California Class Members' Private Information was being shared with a
19 third party as: a) Defendant had superior knowledge of such facts and Plaintiff McCulley
20 and California Class Members had no other way to obtain the information; b) by reason of
21 its status as a provider of medical and mental healthcare services, Defendant was in a
22 special relationship with Plaintiff McCulley and California Class Members—Medical
23 providers have a duty (defined by HIPAA and other federal and state laws and regulations)
24 to keep patients' non-public medical information completely confidential; c) the facts not
25 disclosed relate to health and safety of Plaintiff McCulley and California Class Members;
26 d) Defendant made certain affirmative statements regarding its privacy policy but failed to
27 disclose all material facts (including that it was sharing Private Information with third-

1 parties, and not using Tracking Tools, as described herein) making its partial disclosures
2 misleading, confusing and deceptive to reasonable consumers in the California Class.

3 438. Had Defendant disclosed that it shared Private Information with third parties,
4 Plaintiff McCulley would not have used Defendant's services at the level she did or would
5 have paid considerably less for those services. As a result, Plaintiff suffered injury and
6 out of pocket loss.

7 439. The harm caused by Defendant's conduct outweighs any potential benefits
8 attributable to such conduct and there were reasonably available alternatives to further
9 Defendant's legitimate business interests other than the conduct described herein.

10 440. As a direct result of their reliance on Defendant's representations that it
11 would keep personal information confidential, Plaintiff and California Class Members
12 shared highly sensitive information through their use of the Website, causing them to suffer
13 injury and loss when Defendant disclosed that information to a third party.

14 441. Plaintiff McCulley requests appropriate injunctive and declaratory relief
15 against the continuation of the practices described and complained of herein. Such relief
16 will create a public benefit. Plaintiff McCulley separately seeks public injunctive relief on
17 behalf of the general public of California who have yet to deal with Defendant in the
18 manner described herein, but are likely to in the future, and therefore, are in need of
19 protection provided by the public injunctive relief sought. Such public injunctive relief will
20 create additional public benefits.

21 442. As a direct result of Defendant's violations of the UCL, Plaintiff McCulley
22 and California Class Members have suffered injury in fact and lost money or property
23 including, but not limited to, payments to Defendant and/or other valuable consideration,
24 such as access to their private and personal data. The unauthorized access to Plaintiff
25 McCulley's and California Class Members' private and personal data also diminished the
26 value of that information.

1 449. Plaintiff McCulley and the California Class Members reasonably relied upon
2 the representations Defendant made in its Privacy Policy, including those representations
3 concerning the confidentiality of patient information.

4 450. Defendant was in sole possession of and had a duty to disclose the material
5 information that Plaintiff McCulley's and Class Members' private information was being
6 shared with a third party.

7 451. Had Defendant disclosed that it shared Private Information with third parties,
8 Plaintiff McCulley and the California Class would not have used Defendant's services at
9 the level she did or would have paid considerably less for those services.

10 452. The harm caused by the Defendant's conduct outweighs any potential
11 benefits attributable to such conduct and there were reasonably available alternatives to
12 further Defendant's legitimate business interests other than Defendant's conduct described
13 herein.

14 453. Defendant's acts, omissions and conduct also violate the unfair prong of the
15 UCL because those acts, omissions and conduct offended public policy (including the
16 aforementioned federal and state privacy statutes and state consumer protection statutes,
17 such as HIPAA and CIPA, the ECPA, and CFAA, and constitute immoral, unethical,
18 oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff
19 McCulley and California Class Members.

20 454. As a direct result of their reliance on Defendant's representations that it
21 would keep personal information confidential and Defendant's express representation that
22 it did not use Tracking Tools on its Website, Plaintiff McCulley and California Class
23 Members shared highly sensitive information through their use of the Website, causing
24 them to suffer damages when Defendant disclosed that information to a third party.

25 455. As a direct result of Defendant's violations of the UCL, Plaintiff McCulley
26 and California Class Members have suffered injury in fact and lost money or property,
27 including but not limited to payments to Defendant and/or other valuable consideration.

1 The unauthorized access to Plaintiff McCulley's and California Class Members' private
2 and personal data also diminished the value of that information.

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

9
10 **COUNT XII**
11 **VIOLATION OF THE COLORADO CONSUMER PROTECTION ACT**
12 **Colo. Rev. Stat. Section 6-1-101 et seq.**
13 **(On behalf of Plaintiffs Schreidl, Freriks, Robeson & the Colorado Class)**

14 457. Plaintiffs Schreidl, Freriks, Robeson repeat the allegations contained in the
15 foregoing paragraphs as if fully set forth herein and bring this claim individually and on
16 behalf of the Colorado Class.

17 458. The Colorado Consumer Protection Act, Colo. Rev. Stat. Section 6-1-101 et
18 seq. prohibits deceptive acts or practices in the conduct of any business, trade, or
19 commerce, or in the furnishing of any service in the state of Colorado.

20 459. Plaintiffs Schreidl, Freriks, Robeson and the members of the Colorado Class
21 may maintain claims under the Colorado Consumer Protection Act pursuant to Colo. Rev.
22 Stat. Section 6-1-113 and seek damages, restitution, injunctive relief, reasonable attorneys;
23 fees and costs and other relief that may be just and equitable in the circumstances. Plaintiffs
24 and members of the Colorado Class are (a) actual or potential consumer of Defendant's
25 goods, services, or property and have been injured as a result of Defendant's deceptive
26 trade practices; or (b) are successors in interest to an actual consumer who purchased the
27 defendant's goods, services, or property; or (c) In the course of their person's business or
28 occupation, were injured as a result of Defendant's deceptive trade practice.

1 460. The Colorado Consumer Protection Act pursuant to Colo. Rev. Stat. Section
2 6-1-105, prohibits, deceptive trade practices, including but not limited to:

3 (b) Either knowingly or recklessly makes a false representation as to the source,
4 sponsorship, approval, or certification of goods, services, or property;

5 (c) Either knowingly or recklessly makes a false representation as to affiliation,
6 connection, or association with or certification by another;

7 (e) Either knowingly or recklessly makes a false representation as to the
8 characteristics, ingredients, uses, benefits, alterations, or quantities of goods, food,
9 services, or property or a false representation as to the sponsorship, approval,
10 status, affiliation, or connection of a person therewith;

11 (g) Represents that goods, food, services, or property are of a particular standard,
12 quality, or grade, or that goods are of a particular style or model, if he knows or
13 should know that they are of another;

14 (i) Advertises goods, services, or property with intent not to sell them as
15 advertised;

16 (u) Fails to disclose material information concerning goods, services, or property
17 which information was known at the time of an advertisement or sale if such
18 failure to disclose such information was intended to induce the consumer to enter
19 into a transaction;

20 (rrr) Either knowingly or recklessly engages in any unfair, unconscionable,
21 deceptive, deliberately misleading, false, or fraudulent act or practice.

22 461. By the acts and conduct alleged herein, Defendant committed unfair or
23 deceptive acts and practices in violation of the Colorado Consumer Protection Act, by:

24 h. promising to maintain the privacy and security of Plaintiffs Schreidl's,
25 Freriks', Robesons and Colorado Class Members' protected health information
26 as required by law;

- i. installing the Tracking Tools to operate as intended and transmit Plaintiffs' and Colorado Class Members' Private Information without their authorization to Facebook;
- j. failing to disclose or omitting material facts to Plaintiff and Colorado Class Members regarding the disclosure of their Private Information to Facebook;
- k. failing to take proper action to ensure the Tracking Tool were configured to prevent unlawful disclosure of Plaintiffs' and Colorado Class Members' Private Information;
- l. unlawfully disclosing Plaintiffs' and Colorado Class Members' Private Information to Facebook or Google;
- m. deceptively representing to Plaintiffs and Colorado Class Members that it did not use Tracking Tools when it did.

462. Defendant knew or should have known that its conduct was of the nature prohibited by the Colorado Consumer Protection Act.

463. Defendant's actions also constitute deceptive trade practices because Defendant knew it failed to disclose to Plaintiffs Schreidl, Freriks, Robeson and Colorado Class Members that their healthcare related communications via the Website would be disclosed to Facebook or Google.

464. Defendant's actions also constitute deceptive trade practices because Defendant intended that Plaintiffs Schreidl, Freriks, Robeson and Colorado Class Members rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods, merchandise and services.

465. Specifically, Defendant was aware that Plaintiffs Schreidl, Freriks, Robeson and Colorado Class Members depended and relied upon it to keep their communications confidential and Defendant instead disclosed that information to Facebook or Google.

466. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Tracking Tools to disclose and transmit Plaintiffs'

1 and Colorado Class Members' personally identifiable, non-public medical information,
2 and the contents of their communications exchanged with Defendant to third parties, i.e.,
3 Facebook.

4 467. Defendant's disclosures of Plaintiffs' and Colorado Class Members' Private
5 Information were made without their knowledge, consent, or authorization, and were
6 unprivileged.

7 468. The harm arising from a breach of provider-patient confidentiality includes
8 erosion of the essential confidential relationship between the healthcare provider and the
9 patient.

10 469. Defendant willfully, knowingly, intentionally, and voluntarily engaged in the
11 aforementioned acts when it incorporated the Tracking Tools on its Website, with
12 knowledge of the Tracking Tool's purpose and functionality, and further utilized the
13 benefits that Tracking Tools provides website owners to the detriment of Plaintiffs
14 Schreidl, Freriks, Robeson and the Colorado Class Members.

15 470. Plaintiffs Schreidl, Freriks, Robeson and the Colorado Class Members could
16 not have avoided the harms described herein through the exercise of ordinary diligence.

17 471. As a result of Defendant's actions, Plaintiffs Schreidl, Freriks, Robeson and
18 Colorado Class Members have suffered harm and injury.

19 472. Defendant's unlawful conduct is ongoing. Thus, injunctive and declaratory
20 relief is necessary and appropriate to prevent further violations.

21 473. Plaintiffs Schreidl, Freriks, Robeson and Colorado Class Members have been
22 damaged as a direct and proximate result of Defendant's invasion of their privacy and are
23 entitled to just compensation, including monetary damages.

24 474. Plaintiffs Schreidl, Freriks, Robeson and Colorado Class Members seek
25 appropriate relief for these injuries, including but not limited to damages that will
26 reasonably compensate Plaintiffs and Colorado Class Members for the harm to their
27

1 privacy interests as a result of Defendant's violation of the Colorado Consumer Protection
2 Act.

3 475. Plaintiffs Schreidl, Freriks, Robeson and Colorado Class Members seek all
4 other relief as the Court may deem just and proper, including all available monetary relief,
5 injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees
6 and costs.

7 **PRAYER FOR RELIEF**

8 **WHEREFORE**, Plaintiffs, on behalf of themselves and Class Members, requests
9 judgment against Defendant and that the Court grant the following:

- 10 A. For an Order certifying the Class and appointing Plaintiffs and Counsel to
11 represent such Class;
- 12 B. For equitable relief enjoining Defendant from engaging in the wrongful
13 conduct alleged in this Complaint pertaining to the misuse and/or disclosure
14 of the Private Information of Plaintiffs and Class Members;
- 15 C. For injunctive relief requested by Plaintiffs, including, but not limited to,
16 injunctive and other equitable relief as is necessary to protect the interests of
17 Plaintiffs and Class Members:
- 18 D. For an award of damages, including, but not limited to, actual, consequential,
19 statutory, punitive, and nominal damages, as allowed by law in an amount to
20 be determined;
- 21 E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by
22 law;
- 23 F. For prejudgment interest on all amounts awarded; and
- 24 G. Such other and further relief as this Court may deem just and proper.

25 **DEMAND FOR JURY TRIAL**

26 Plaintiffs hereby demand that this matter be tried before a jury.
27
28

1 DATE: November 22, 2023

Respectfully Submitted,

2 **ZIMMERMAN REED LLP**

3 s/ Hart L. Robinovitch

4 Hart L. Robinovitch (AZ SBN 020910)

5 14648 N. Scottsdale Road, Suite 130

6 Scottsdale, AZ 85254

7 Telephone: (480) 348-6400

8 Facsimile: (480) 348-6415

9 Email: hart.robinovitch@zimmreed.com

10 David S. Almeida

11 Elena A. Belov

12 **ALMEIDA LAW GROUP LLC**

13 849 W. Webster Avenue

14 Chicago, Illinois 60614

15 Tel: (312) 576-3024

16 david@almeidalawgroup.com

17 elena@almeidalawgroup.com

18 Mark S. Reich

19 **LEVI & KORSINSKY, LLP**

20 55 Broadway, 4th Floor, Suite 427

21 New York, NY 10006

22 Telephone: (212) 363-7500

23 Facsimile: (212) 363-7171

24 Email: mreich@zlk.com

25 Kevin D. Neal

26 William F. King

27 Kenneth N. Ralston

28 **GALLAGHER & KENNEDY, P.A.**

2575 East Camelback Road

Phoenix, Arizona 85016-9225

Gary M. Klinger

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Telephone: (866) 252-0878

gklinger@milberg.com

Glen L. Abramson

Alexandra M. Honeycutt

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

800 S. Gay Street, Suite 1100

Knoxville, TN 37929

Telephone: (866) 252-0878

gabramson@milberg.com

ahoneycutt@milberg.com

1 Bryan L. Bleichner
2 Philip J. Krzeski
3 **CHESTNUT CAMBRONNE PA**
4 100 Washington Avenue South, Suite 1700
5 Minneapolis, MN 55401
6 Phone: (612) 339-7300
7 Fax: (612) 336-2940
8 *bbleichner@chestnutcambronne.com*
9 *pkrzeski@chestnutcambronne.com*

6 Terence R. Coates
7 Dylan J. Gould
8 **MARKOVITS, STOCK & DEMARCO,**
9 **LLC**
10 119 E. Court St., Ste. 530
11 Cincinnati, Ohio 4502
12 Phone: (513) 651-3700
13 Fax: (513) 665-0219
14 *tcoates@msdlegal.com*
15 *dgould@msdlegal.com*

12 Joseph M. Lyon
13 **THE LYON FIRM**
14 2754 Erie Ave.
15 Cincinnati, Ohio 45208
16 Phone: (513) 381-2333
17 Fax: (513) 766-9011
18 *jlyon@thelyonfirm.com*

16 Cristina Perez Hesano
17 **PEREZ LAW GROUP PLLC**
18 7508 N 59th Ave.
19 Glendale, AZ 85301
20 623-826-5593
21 Email: *cperez@perezlawgroup.com*

19 *Counsel for Plaintiff and the Putative Class*