CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Tiara Avaness (SBN 343928)
tavaness@clarksonlawfirm.com
Valter Malkhasyan (SBN 348491)
vmalkhasyan@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070

Counsel for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

B.K. and N.Z., individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

EISENHOWER MEDICAL CENTER,

Defendant.

Case No.: 5:23-cv-2092

CLASS ACTION COMPLAINT

1. VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE SECTION 56, *et seq*.
2. VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. SECTION 2511(1), *et seq.*
3. VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. SECTION 2511(3)(a), *et seq*
4. VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT, CAL. PENAL CODE SECTION 630, *et seq.*

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

6. INVASION OF PRIVACY UNDER CALIFORNIA CONSTITUTION

7. INVASION OF PRIVACY - INTRUSION UPON SECLUSION

8. BREACH OF IMPLIED CONTRACT

9. VIOLATION OF CALIFORNIA CONSUMERS LEGAL REMEDIES ACT, CAL. CIV. CODE SECTION 1750, *et seq.*

10. VIOLATION OF CALIFORNIA PENAL CODE SECTION 496(a) and (c)

11. NEGLIGENCE

12. BREACH OF CONFIDENCE

13. BREACH OF FIDUCIARY DUTY

14. UNJUST ENRICHMENT

DEMAND FOR JURY TRIAL

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Plaintiffs B.K. and N.Z. (collectively, "**Plaintiffs**"), individually and on behalf of all others similarly situated bring this action against Defendant Eisenhower Medical Center ("**Eisenhower Health**" and/or "**Defendant**").

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

INTRODUCTION

1. Defendant Eisenhower Health is an organization consisting of five major divisions—the main campus, hospital, primary care center, urgent care, and foundation—offering a wide range of clinical services to patients in Southern California.

2. The Eisenhower Health Main Campus ("**Main Campus**") includes a children's center, birth center, bariatric care, emergency center, and the Eisenhower Medical Center Hospital (the "**Hospital**").[1] The Hospital is a full-service hospital where patients are able to receive care from expert clinicians and physicians and is comprised of primary care locations, urgent care center, multi-specialty health center, and specialized programs.[2]

3. Eisenhower Primary Care ("**Primary Care Centers**") is a system of clinics in charge of providing medical care to families.[3]

[1] *Eisenhower Health Main Campus*, EISENHOWER HEALTH, https://eisenhowerhealth.org/locations/?action=detail&dataRef=15.

[2] *Eisenhower Medical Center,* EISENHOWER HEALTH, https://eisenhowerhealth.org/locations/?cache=on&action=detail&dataRef=67&template=.

[3] *Eisenhower Primary Care*, EISENHOWER HEALTH, https://eisenhowerhealth.org/services/primarycare/epc/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

4. Eisenhower Urgent Care ("**Urgent Care Centers**") has multiple locations allowing patients to seek medical consultations on a walk-in basis.[4]

5. Eisenhower Health Foundation (the "**Foundation**") is a 501(c)(3) non-profit organization responsible for all of Eisenhower Health's fundraising.[5]

6. Defendant has disregarded the privacy rights of millions of visitors to and users of its websites ("**Users**" or "**Class Members**") by intentionally, willfully, recklessly and/or negligently failing to implement adequate and reasonable measures to ensure that the Users' personally identifiable information ("**PII**") and protected health information ("**PHI**") (collectively, "**Private Information**") was safeguarded. Instead, Defendant allowed unauthorized third parties, including Meta Platforms, Inc. d/b/a Facebook ("**Facebook**") to intercept the Users' clicks, communications on, and visits of Defendant's websites, including https://www.eisenhowerhealth.org/ (the "**Site**") and https://www.eisenhowerhealth.org/mychart (the "**Portal**" and collectively with the site, the "**Web Properties**").

7. Unbeknownst to Users and without Users' authorization or informed consent, Defendant installed Facebook's Meta Pixel ("**Meta Pixel**" or "**Pixel**") and other third-party tracking technology, in itsWeb Properties in order to intercept and send Private Information to third parties such as Facebook and/or Google LLC.

8. These Pixels collect Users' confidential and private PHI—including but not limited to details about their medical conditions, treatments and providers sought, and appointments—and send it to Facebook without prior, informed consent. These Pixels are snippets of code that track Users as they navigate through a website—logging which pages they visit, each button they click, and what information they provide in online forms. More specifically, the Meta Pixel sends information to Facebook via scripts running in a person's internet browser so each data packet comes

[4] *Urgent Care*, EISENHOWER HEALTH, https://eisenhowerhealth.org/services/urgent-care/.

[5] *Our Mission,* EISENHOWER HEALTH, https://eisenhowerhealth.org/giving/what-we-do/our-mission/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

labeled with a specific internet protocol ("**IP**") address that can be used in combination with other data to identify an individual or household. Additionally, if the person has an active Facebook account, the IP address is paired with their personal unique Facebook ID ("**FID**"), which Facebook uses to identify that individual.

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

10. Defendant encouraged Plaintiffs and Class Members to access and use various digital tools via its Web Properties to, among other things, receive healthcare services, in order to gain additional insights into its Users, improve its return on marketing dollars and, ultimately, increase its revenue.

11. In exchange for installing the Pixels, Facebook provides Defendant with analytics about the advertisements it has placed as well as tools to target people who have visited its Web Properties.

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

an egregious, unauthorized dissemination of highly sensitive Private Information unique to each individual User.

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

14. Alarmingly, the use of Meta Pixels on Defendant's Web Properties tracks extremely sensitive PHI such as health conditions (e.g., diabetes), diagnoses (e.g., COVID-19 or AIDS), procedures, test results, treatment status, the treating physician, allergies, and PII.

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

16. Defendant knew that by embedding the Meta Pixel—a proprietary tracking and advertising tool developed by Facebook—on its Web Properties, they were permitting Facebook to collect and use Plaintiffs' and Class Members' Private Information, including sensitive medical information.

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

18. Defendant's actions constitute an extreme invasion of Plaintiffs' and Class Members' right to privacy and violate federal and state statutory and common law as well as Defendant's own Privacy Policies that affirmatively and unequivocally

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

state that any personal information provided to Defendant will remain secure and protected.[6]

19. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with doctors online; (iii) emotional distress and heightened concerns related to the release of Private Information to third parties; (iv) loss of the benefit of the bargain; (v) diminution of value of the Private Information; (vi) statutory damages and (vii) continued and ongoing risk to their Private Information. Plaintiffs and Class Members have a substantial risk of future harm, and thus injury in fact, due to the continued and ongoing risk of misuse of their Private Information that was shared by Defendant with third parties.

20. Plaintiffs seek, on behalf of themselves and a class of similarly situated persons, to remedy these harms and therefore assert the following statutory and common law claims against Defendant: (i) Violation of the California Confidentiality of Medical Information Act ("**CMIA**"), Cal. Civ. Code § 56, *et seq.*; (ii) Violation of Electronic Communications Privacy Act, 18 U.S.C. §2511(1), *et seq*; (iii) Violation of Electronic Communications Privacy Act, 18 U.S.C. §2511(3)(a), *et seq*; (iv) Violation of the California Invasion of Privacy Act ("**CIPA**"), Cal. Penal Code § 630, *et seq.*; (v) Violation of California's Unfair Competition Law ("**UCL**"), Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful and Unfair Business Practices; (vi) Invasion of Privacy under the California Constitution; (vii) Common Law Invasion of Privacy; (viii) Common Law Breach of Implied Contract; (ix) Violation of California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.*; (x) Violation of California Penal Code § 496, *et seq.*; (xi) Negligence; (xii) Common Law Breach of Confidence, (xiii) Common Law Breach of Fiduciary Duty; and (xiv) Common Law

[6] Eisenhower Health's Privacy Policies (and other affirmative representations) represent to Users that it will not share Private Information with third parties without the patient's consent. *See* https://eisenhowerhealth.org/about/privacy/ (last visited Oct. 10, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Unjust Enrichment.

PARTIES

21. Plaintiff B.K. was a California resident at all relevant times, residing in Riverside County, California, where she intends to remain indefinitely.

22. Plaintiff N.Z. is and at all relevant times was, a California resident, residing in Riverside County, California, where she intends to remain indefinitely.

23. Defendant Eisenhower Medical Center is a not-for-profit organization providing healthcare services to patients in Southern California. Defendant Eisenhower Medical Center is incorporated in California with its principal place of business located at 39000 Bob Hope Drive, Rancho Mirage, CA 92270.[7]

JURISDICTION & VENUE

24. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than one hundred (100) putative class members defined below, and minimal diversity exists because a significant portion of putative class members are citizens of a state different from the citizenship of at least one Defendant.

25. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. Plaintiffs are citizens of California, reside in this District, and used Defendant's Web Properties within this District. Moreover, Defendant received substantial compensation from offering healthcare services in this District, and Defendant made numerous misrepresentations which had a substantial effect in this District, including, but not limited to, representing that it will only disclose Private Information provided to them under certain circumstances, ***which do not*** include disclosure of Private Information for marketing purposes.

[7] *Contact Us,* EISENHOWER HEALTH, https://eisenhowerhealth.org/giving/ways-to-give/campaign/contact-us/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

26. Defendant is subject to personal jurisdiction in California based upon sufficient minimum contacts which exist between Defendant and California. Defendant is incorporated in California, maintains its principal place of business in California, is authorized to conduct and is conducting business in California.

FACTUAL BACKGROUND

27. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to surreptitiously capture and to disclose their Users' Private Information. Specifically, and for example, The Markup reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment.[8] Estimates are that over 664 hospital systems and providers utilize some form of tracking technology on their digital properties.[9]

28. Entities collecting and disclosing Users' Private Information face significant legal exposure under the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), which applies specifically to healthcare providers, health insurance providers and healthcare data clearinghouses.[10]

---

[8] Todd Feathers, *et al.*, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[9] Dave Muoio & Annie Burky, *Advocate Aurora, WakeMed get served class action over Meta's alleged patient data mining,* FIERCE HEALTHCARE (November 4, 2022), https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook.

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

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

> ***Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[12]

OCR makes it clear that information that is routinely collected by vendors on public-facing websites, apps and web-based assets may be PHI as well, including unique identifiers such as IP addresses, device IDs, or email addresses.[13]

---

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

[12] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* U.S. DEP'T OF HEALTH AND HUM. SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Oct. 10, 2023) (emphasis added).

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

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

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

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

a. **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.[14]

b. **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.[15]

c. **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.[16]

[14] *An overview of HTTP*, MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview (last visited Oct. 10, 2023).

[15] *HTTP cookies*, MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies (last visited Oct. 10, 2023).

[16] *An overview of HTTP*, *supra* note 13. One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses. *HTTP*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

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

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

37. When patients visit Defendant's Web Properties via an HTTP Request to Defendant's server, that server sends an HTTP Response including the Markup that displays the Webpage visible to the User and Source Code, including Defendant's Pixel.

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

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

40. These cookies uniquely identify the User and are sent with each

Messages, MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Web/HTTP/Messages (last visited Oct. 10, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

intercepted communication to ensure the third-party can uniquely identify the patient associated with the Private Information intercepted.

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

42. Facebook's workaround, for example, is called CAPI, which is an "effective" workaround because it does not intercept data communicated from the User's browser. Instead, CAPI "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."[17]

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

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

45. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct Defendant to "[u]se the CAPI in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[18]

46. The third parties to whom a website transmits data through Pixels and associated workarounds do not provide any substantive content relating to the User's

[17] Michael Mata, *Stop Data Loss with Facebook Server-Side Tracking*, MADGICX (March 18, 2022), https://madgicx.com/blog/facebook-server-side-tracking.

[18] *See Best Practices for Conversions API,* META, https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Oct. 10, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

communications. Instead, these third parties are typically procured to track User data and communications for marketing purposes of the website owner (i.e., to bolster profits).

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

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

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

50. For example, when a patient visits www.eisenhowerhealth.org and enters "heart disease" into the search bar, the patient's browser automatically sends an HTTP request to Eisenhower Health's web server. Eisenhower Health's web server automatically returns an HTTP Response, which loads the markup for that particular webpage as depicted in ***Figure 1***.[19]

///

///

///

[19] The image depicted in ***Figure 1*** was taken from https://eisenhowerhealth.org/resources/search/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

51. The patient visiting this particular web page only sees the Markup, not the not the Defendant's Source Code or underlying HTTP Requests and Responses.

52. In reality, Defendant's Source Code and underlying HTTP Requests and Responses share the patient's personal information with Facebook, including the fact that the patient is looking for treatment for his heart disease diagnosis — along with the patient's unique Facebook identifiers.

///

///

///

///

///

///

///

///

///

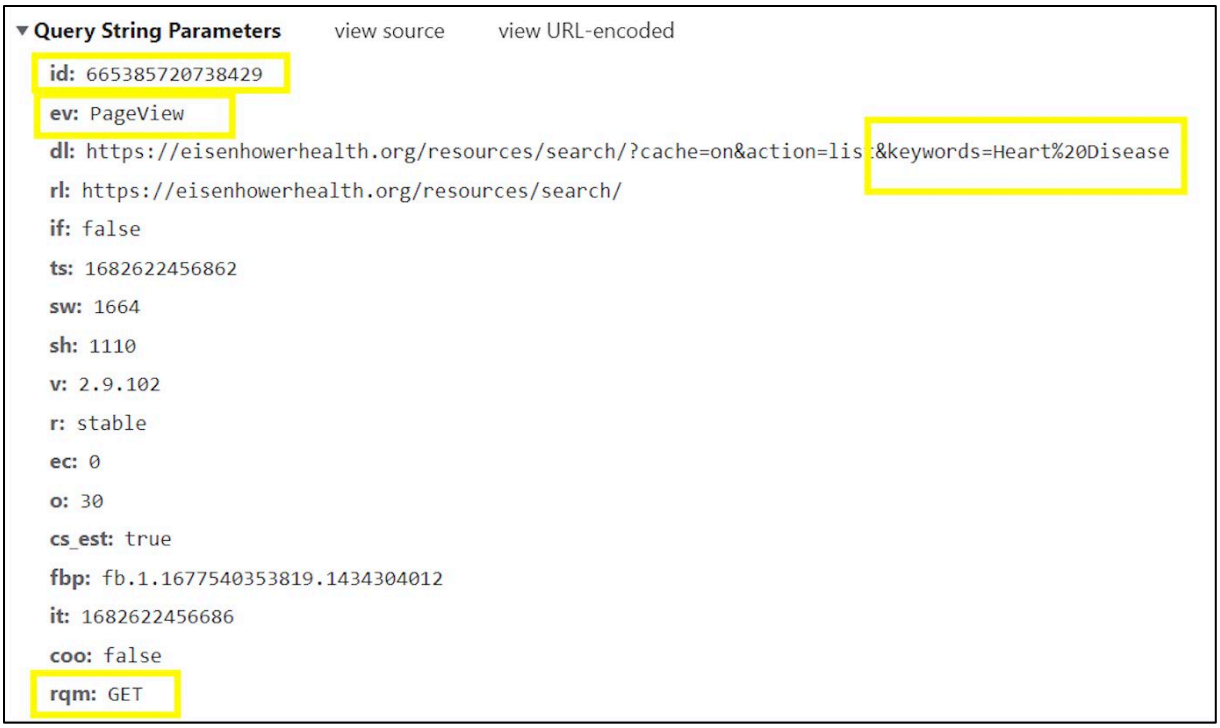
///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Figure 2: An HTTP single communication session sent from the device to Facebook that reveals the User's exact search terms ("heart disease") typed into the search bar along with the User's unique Facebook personal identifier (the c_user field).[20]

Figure 3. An easier-to-read representation of data sent to Facebook when a User enters search terms into Defendant's search bar.

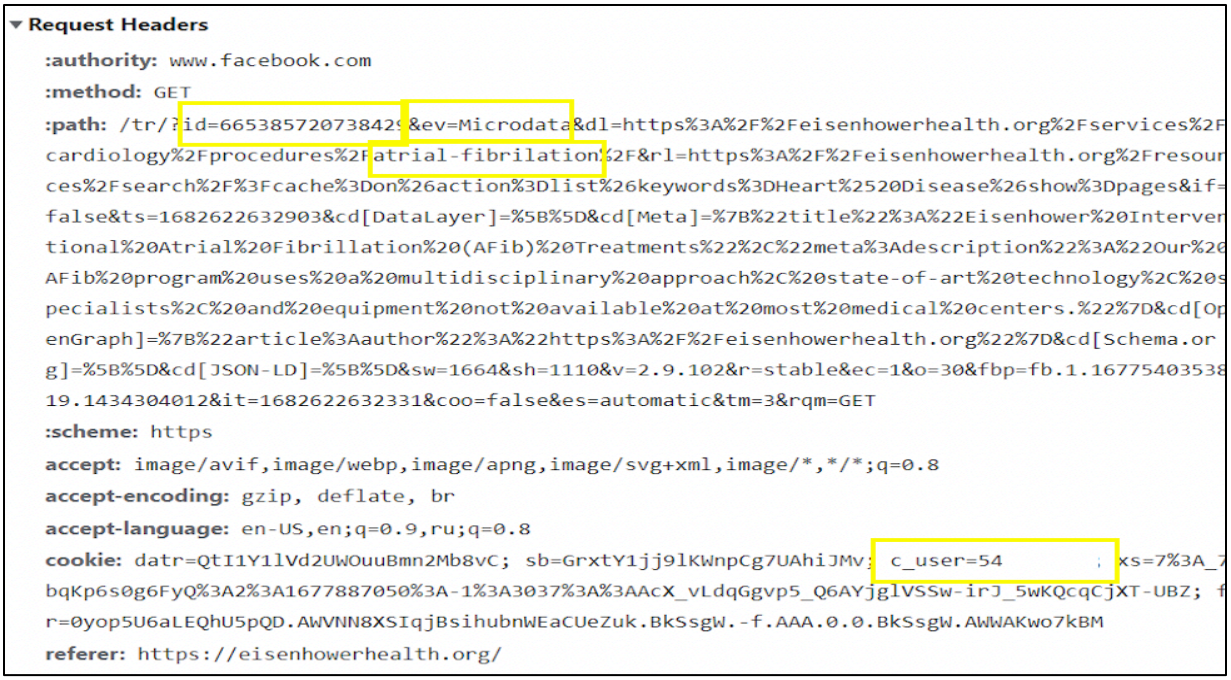


[20] The images depicted in ***Figures 2 and 3*** were taken from https://eisenhowerhealth.org/resources/search/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

53. Similarly, if a User types "Atrial Fibrilation" into Defendant's search bar, Defendant shares that information with Facebook, along with the User's personal identifiers.

Figures 4 and 5: An HTTP single communication session sent from the device to Facebook that reveals the User's exact search terms ("Atrial Fibrilation") along with the User's unique Facebook personal identifier (the c_user field).[21]



[21] The images depicted in ***Figures 4 and 5*** were taken from https://eisenhowerhealth.org/services/cardiology/procedures/atrial-fibrilation/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

54. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions and can command a website visitor's browser to send data transmissions to third parties via Pixels or web bugs,[22] effectively open a spying window through which the webpage can funnel the visitor's data, actions, and communications to third parties.

55. Looking to the previous example, Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) and sending those communications to Facebook.

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

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

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

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

[22] These Pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

communicated to Facebook.

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

60. Defendant utilizes Facebook's Business Tools and intentionally installs the Pixel and/or CAPI on its Web Properties to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties and obligations.

61. Defendant's Web Properties contain a unique identifier which indicates that a Meta Pixel is being used on a particular webpage.

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

63. However, Defendant's Web Properties do not rely on the Pixels to function.

64. While seeking and using Defendant's services as a medical provider, Plaintiffs and Class Members communicated their Private Information to Defendant via its Web Properties.

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

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Private Information to Facebook (or any other third-party).

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

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

69. Through the Source Code deployed by Defendant, the cookies that they use to help Facebook identify patients include but are not necessarily limited to cookies named: "c_user," "datr," "fr," and "fbp."[23]

70. 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 composed of a unique and persistent set of numbers.

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

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

profile.

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

73. The "*fr*" cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.[24]

Defendant's Pixel Disseminates Patient Information Via Its Web Properties.

74. By way of example, if a patient uses https://www.eisenhowerhealth.org to look for medical treatments, they may select "Diabetes and Endocrinology" under the "Programs & Services" tab, which takes them to the list of services offered by Defendant to Users in need of diabetes treatment. On those pages the User can further narrow their search results by services offered by Defendant.

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

76. For example, a diabetes patient in search for diabetes services can search for various diabetes treatment options and information, from "endocrinology clinic" and "diabetes prevention" to resources intended to help patients.[25]

---

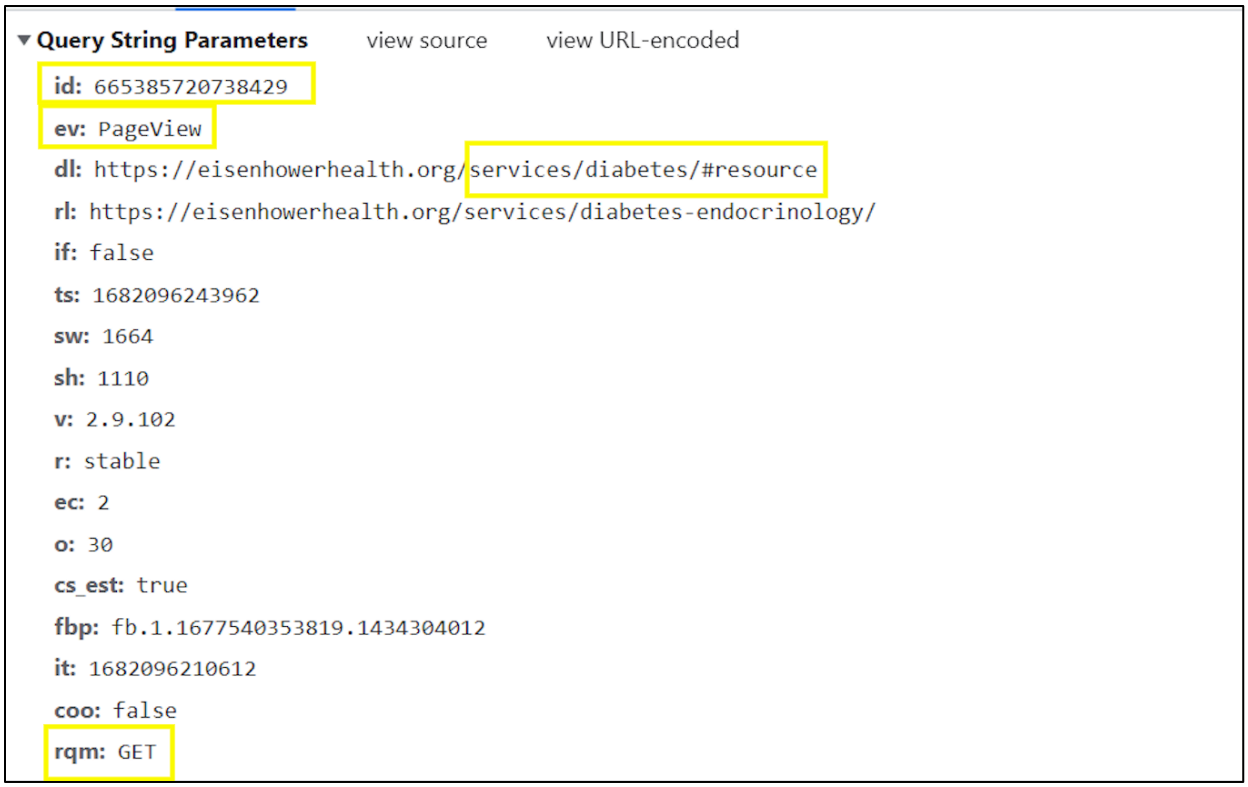
[24] *See* Gunes Acar et al., *Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission* 16 (March 27, 2015), https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

[25] *See Eisenhower Diabetes and Endocrinology Specialty Clinic,* EISENHOWER HEALTH, https://eisenhowerhealth.org/services/diabetes-endocrinology/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

77. From the moment the patient begins searching for diabetes treatment their selections or search parameters are automatically transmitted by the Pixel to Facebook along with the User's unique personal identifiers, as evidenced by ***Figures 6 and 7 below***.

Figure 6: Defendant's transmission to Facebook of User's search parameters showing treatment sought ("diabetes services").



78. The first line of highlighted text, "id: 665385720738429," refers to the Defendant's Pixel ID for this particular Webpage and confirms that the Defendant has downloaded the Pixel into its Source Code on this particular Webpage.

79. In the second line of text, "ev:" is an abbreviation for event, and "PageView" is the type of event. Here, this event means that Defendant's Pixel is sending all the meta information about the webpage which can include information like page title, URL, and page description.

80. The remaining lines of text identify the User as a patient: (i) seeking medical care from Defendant via www.eisenhowerhealth.org; (ii) who has diabetes; and (iii) who is searching for diabetes services.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

81. Finally, the last line of highlighted text ("**GET**"), demonstrates that Defendant's Pixel sent the User's communications, and the Private Information contained therein, alongside the User's personal identifiers, including Facebook ID and other cookies. This is further evidenced by the image below, which was collected during the same browsing session as the previous image.

Figure 7. Defendant's transmission to Facebook of User's search parameters showing treatment sought ("diabetes services") and the User's unique Facebook ID.

82. As mentioned above, if the patient selects other diabetes services, those search parameters are also automatically transmitted to Facebook by Defendant's Pixels, along with the patient's personal identifiers. In addition to sharing patient's conditions and selected treatments via PageView and Microdata events, Defendant's Pixels also share the text of buttons clicked by the patient via the

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

"SubscribedButtonClick" event.

83. For example, if a patient clicks on a button that contains a phone number for a particular service, Defendant sends that information to Facebook via the "SubscribedButtonClick" event, which shares the inner text of the button the User clicked to schedule the procedure:

Figures 8: HTTP communication sessions sent from the User's device to Facebook revealing the inner text of the button clicked by the User, and their personal identifiers.

84. As another example, if a User interested in a particular procedure reviews Defendant's resources for prospective patients, Defendant also shares that information with Facebook, as images below demonstrate:

///

///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Figures 9 & 10: HTTP communication sessions sent from the User's device to Facebook revealing the service sought (stroke rehabilitation) and the inner text of the button clicked by the User interested in stroke rehabilitation.

▼ **Query String Parameters** view source view URL-encoded

id: 665385720738429

ev: SubscribedButtonClick

dl: https://eisenhowerhealth.org/services/rehabilitation/services/stroke/#getstarted

rl: https://eisenhowerhealth.org/services/cardiology/procedures/ablation-for-arrhythmias/

if: false

ts: 1682623520560

cd[buttonFeatures]: {"classList":"","destination":"tel:760-773-2033","id":"","imageUrl":"","innerText":"760-773-2033","numChildButtons":0,"tag":"a","type":null,"name":""}

cd[buttonText]: 0-0-0

cd[formFeatures]: []

cd[pageFeatures]: {"title":"Eisenhower Stroke Rehabilitation Program - Stroke Rehab"}

▼ **Request Headers**

:authority: www.facebook.com

:method: GET

:path: /tr/?id=665385720738429&ev=SubscribedButtonClick&dl=https%3A%2F%2Feisenhowerhealth.org%2Fservices%2Frehabilitation%2Fservices%2Fstroke%2F%23getstarted&rl=https%3A%2F%2Feisenhowerhealth.org%2Fservices%2Fcardiology%2Fprocedures%2Fablation-for-arrhythmias%2F&if=false&ts=1682623520560&cd[buttonFeatures]=%7B%22classList%22%3A%22%22%2C%22destination%22%3A%22tel%3A760-773-2033%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22760-773-2033%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%7D&cd[buttonText]=0-0-0&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22Eisenhower%20Stroke%20Rehabilitation%20Program%20-%20Stroke%20Rehab%22%7D&sw=1664&sh=1110&v=2.9.102&r=stable&ec=3&o=30&cs_est=true&fbp=fb.1.1677540353819.1434304012&it=1682622819455&coo=false&es=automatic&tm=3&rqm=GET

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

accept-language: en-US,en;q=0.9,ru;q=0.8

cookie: datr=QtI1Y1lVd2UWOuuBmn2Mb8vC; sb=GrxtY1jj9lKWnpCg7UAhiJMv; c_user=540643061; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AAcX_vLdqGgvp5_Q6AYjglVSSw-irJ_5wKQcqCjXT-UBZ; fr=0yop5U6aLEQhU5pQD.AWVNN8XSIqjBsihubnWEaCUeZuk.BkSsgW.-f.AAA.0.0.BkSsgW.AWWAKwo7kBM

referer: https://eisenhowerhealth.org/

85. This information is automatically sent from the User's device to Facebook, and it reveals the User's FID (c_user field) along with each search filter the User selected.

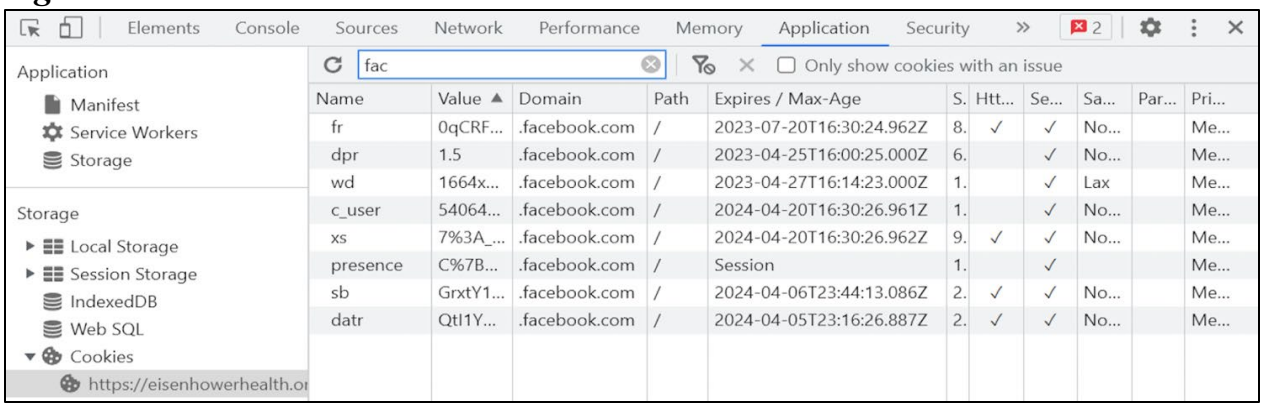
86. A User who accesses Defendant's website while logged into Facebook will transmit the c_user cookie to Facebook, which contains that user's unencrypted

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Facebook ID, and other personal cookie values including the datr and fr cookies.

87. When accessing www.eisenhowerhealth.org, for example, Facebook receives as many as eight (8) cookies:

Figure 11



88. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.[26] Facebook, at a minimum, uses the fr cookie to identify Users.[27]

89. At each stage, Defendant Eisenhower Health also utilized the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a User:[28]

Figure 12

Name	Value	Domain	Path	Expires / Max-Age
_fbp	fb.1.1677540353819.1434304012	.eisenhowerhealth.org	/	2023-07-20T16:48:11.000Z

90. The fr cookie expires after ninety (90) days unless the User's browser logs back into Facebook.[29] If that happens, the time resets, and another ninety (90) days begins to accrue.

91. The _fbp cookie expires after ninety (90) days unless the User's browser

[26] Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* 33 (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.
[27] *Cookies Policy*, META, https://www.facebook.com/policy/cookies/ (last visited Oct. 10, 2023).
[28] *Id.*
[29] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

accesses the same website.[30] If that happens, the time resets, and another ninety (90) days begins to accrue.

92. The Facebook Tracking Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—i.e., Defendant.[31]

93. 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.[32]

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

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

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

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

98. Plaintiffs were never provided with any written notice that Defendant disclosed its Website users' Private Information nor were they provided any means of opting out of such disclosures.

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

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

100. Defendant does not have the legal right to use or share Plaintiffs' and Class Members' data, as this information is protected by the HIPAA Privacy Rule.

---

30 *Id.*

31 This is confirmable by using developer tools to inspect a website's cookies and track network activity.

32 This is confirmable by tracking network activity.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

The Privacy Rule does not permit the use and disclosure of Private Information to Facebook for use in targeted advertising.[33]

101. Beyond Defendant's legal obligations to protect the confidentiality of individuals' Private Information, Defendant's privacy policies and online representations affirmatively and unequivocally state that any personal information provided to Defendant will remain secure and protected.[34]

102. Further, Defendant represents to Users that they will only disclose Private Information provided to them under certain circumstances, ***none of which apply here***.[35] Defendant's privacy policies do ***not*** permit Defendant to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes.

103. In fact, Defendant acknowledges in its Notice of Privacy Practices that it "will not sell, trade or rent your personal information to other people or businesses unless we have your consent."[36]

104. Moreover, Defendant represents that it will disclose Users' PHI when required to in limited circumstances. Defendant represents that it may transfer or share User's PHI "to successors in title to our business (third parties who by our company or the relevant part of the business)" or to "comply with lawful requests to disclose personal information to certain authorities."[37]

105. Further, Defendant's Privacy Policy represents:

> "We are committed to protecting the privacy of your medical information. We are required by law to maintain the confidentiality of information that identifies you and the care you receive."
>
> "We ensure, to the best of our ability, that our systems are secure so as to protect your personal information from misuse."

---

33 *See* 45 C.F.R. § 164.502.

34 *Privacy Policy*, EISENHOWER HEALTH, https://eisenhowerhealth.org/about/privacy/ (last visited Oct. 10, 2023).

35 *See id*.

36 *See id.*

37 *See id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

> "For example, like many web sites, we use cookies, log files and links to tell us how you use our site, but we do not collect or store personally identifiable information."[38]

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

107. Finally, in its privacy policy, Defendant acknowledges that, "We will not sell, trade or rent your personal information to other people or businesses unless we have your consent."[39]

108. Defendant failed to issue a notice that Plaintiffs' and Class Members' Private Information had been impermissibly disclosed to an unauthorized third party. In fact, Defendant ***never*** disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications, data, and Private Information with Facebook and other unauthorized third parties.[40]

109. Defendant has unequivocally failed to adhere to a single promise vis-à-vis its duty to safeguard Private Information of its Users. Defendant has made these privacy policies and commitments available on its websites. Defendant includes these privacy policies and commitments to maintain the confidentiality of its Users' sensitive information as terms of its contracts with those Users, including contracts entered with Plaintiffs and the Class Members. In these contract terms and other

---

[38] *Privacy Policy*, EISENHOWER HEALTH, https://eisenhowerhealth.org/about/privacy/.

[39] *See id.*

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

representations to Plaintiffs and Class Members and the public, Defendant promised to take specific measures to protect Plaintiffs' and Class Members' Private Information, consistent with industry standards and federal and state law. However, it failed to do so.

110. Even non-Facebook users can be individually identified via the information gathered on the Digital Platforms, like an IP address or personal device identifying information. This is precisely the type of information for which HIPAA requires the use of de-identification techniques to protect patient privacy.[41]

111. In fact, in an action currently pending against Facebook related to use of their Pixel on healthcare provider web properties, Facebook explicitly stated it requires Pixel users to "post a prominent notice on every page where the Pixel is embedded and to link from that notice to information about exactly how the Pixel works and what is being collected through it, so it is not invisible."[42] Defendant did not post such a notice.

112. Facebook further stated that "most providers [...] will not be sending [patient information] to Meta because it violates Meta's contracts for them to be doing that."[43]

113. Despite a lack of disclosure, Defendant allowed third parties to "listen in" on patients' confidential communications and to intercept and use for advertising purposes the very information they promised to keep private, in order to bolster their profits.

---

[41] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH AND HUM. SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Oct. 10, 2023).

[42] *See* Transcript of the argument on Plaintiff's Motion for Preliminary Injunction in *In re Meta Pixel Healthcare Litig.*, Case No. CV-22-03580-WHO (N.D. Cal. Nov. 9, 2022) (Hon. J. Orrick), at 19:12-18; *see also In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218 (N.D. Cal. Dec 22, 2022).

[43] *Id.* at 7:20-8:11.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

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

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

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

117. Plaintiffs and Class Members relied to their detriment on Defendant's uniform representations and omissions regarding protection privacy, limited uses, and lack of sharing of their Private Information.

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

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

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

120. Plaintiffs and Class Members did not realize that tracking Pixels exist because they are invisibly embedded within Defendant's web pages that users might

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

interact with.[44] Patients and Users of Defendant's Web Properties do not receive any alerts during their uses of Defendant's Web Properties stating that Defendant tracks and shares sensitive medical data with Facebook, allowing Facebook and other third parties to subsequently target all users of Defendant's website for marketing purposes.

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

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

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

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

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

---

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Facebook's Use of Tracking Pixels in Advertising Business.

126. Facebook is one of the largest advertising companies in the country, with over 2.9 billion active users.[45]

127. Realizing the value of having direct access to millions of consumers, in 2007, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming it to be a "completely new way of advertising online" that would allow "advertisers to deliver more tailored and relevant ads."[46]

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

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

129. One of its most powerful advertising tools is Meta Pixel, formerly known as Facebook Pixel, which launched in 2015.

130. Ad Targeting has been extremely successful due, in large part, to Facebook's ability to target people at a granular level. "Among many possible target audiences, Facebook offers advertisers, [for example,] 1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"[47]

---

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

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

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

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

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

134. Alternatively, Facebook can link the data to a users' Facebook account through the "Facebook Cookie." The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users.[48]

135. Facebook can also link Private Information to Facebook accounts through identifying information collected through Meta Pixel through what Facebook calls "Advanced Matching."[49] There are two forms of Advanced Matching: manual

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

[49] Illia Lahunou, *What is Advanced Matching in Facebook Pixel and How it Works,* VERFACTO, https://www.verfacto.com/blog/ecommerce/advanced-matching-facebook-pixel/ (last visited Oct. 10, 2023); *see also About advanced matching for web*, META, https://www.facebook.com/business/help/611774685654668?id=120537668283214 2 (last visited Oct. 10, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

matching and automatic matching. Using Manual Advanced Matching the website developer manually sends data to Facebook to link users. Using Automatic Advanced Matching, the Meta Pixel scours the data it receives to search for recognizable fields, including name and email address to match users to their Facebook accounts.[50]

136. A recent investigation revealed that the Meta Pixel was installed inside password-protected patient portals of at least seven health systems.[51] When a User navigates through their patient portal, the Meta Pixel sends Facebook sensitive data including but not limited to, the User's medication information, prescriptions, descriptions of their issues, notes, test results, and details about upcoming doctor's appointments.

137. David Holtzman, a health privacy consultant was "deeply troubled" by the results of The Markup's investigation and indicated "it is quite likely a HIPAA violation" by the hospitals, such as Defendant.[52]

138. Laura Lazaro Cabrera, a legal officer at Privacy International, indicated that Facebook's access to use even only some of these data points—such as just the URL—is problematic. She explained, "Think about what you can learn from a URL that says something about scheduling an abortion' . . . 'Facebook is in the business of developing algorithms. They know what sorts of information can act as a proxy for personal data."[53]

139. When Users visit websites that have incorporated the Meta Pixel, the Pixel collects information about Users' activity on that website. This information is then shared with Facebook and, in tandem with data from the Users' Facebook profile

[50] *Id.*
[51] *See* Feathers, *et al*., *supra* note 8.
[52] *Id.*
[53] Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, THE MARKUP (Sept. 25, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

such as their age, gender, and interests, can be used to target the user with advertisements on Facebook and other websites that use the Meta Pixel.

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

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

142. This level of surveillance and monitoring raises important ethical and legal questions about privacy, consent, and the use of personal data. It is important for Users to be aware of how their data is being collected and used, and to have control over how their information is shared and used by advertisers and other entities.

143. Moreover, the misuse of this data could potentially lead to the spread of false or misleading information, which could have serious consequences, particularly in the case of health-related information. As an example, the Cambridge Analytica scandal revealed that personal data was misused to target individuals with political propaganda and misinformation.[54]

144. The Cambridge Analytica scandal involved the misuse of personal data collected from Facebook users, which was then used to target individuals with

[54] Sam Meredith, *Here's Everything You Need to Know about the Cambridge Analytica Scandal*, CNBC (March 23, 2018), https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

political advertising and propaganda. The scandal highlighted the potential dangers of using personal data for targeted advertising and the need for greater transparency and accountability in the collection and use of personal information.[55] One of the ways that Cambridge Analytica was able to collect personal data was through the use of third-party apps that collected data from users and their friends. This data was then used to build detailed profiles of individuals, which were used to target them with personalized political ads and propaganda.

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

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

147. Finally, as pointed out by the OCR, impermissible disclosures of such data in the healthcare context "may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI…. This tracking information could also be misused to promote misinformation, identity theft, stalking, and harassment."[56]

148. In conclusion, as Judge Orrick pointed out in a recent decision allowing claims under California and common law against Regents of the University of California for collecting personal medical data via the Meta Pixel to go forward, "[p]ersonal medical information is understood to be among the most sensitive information that could be collected about a person" and unauthorized transmission or

[55] *Id.*

[56] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, supra* note 12.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

interception of such data by third parties may constitute a "highly offensive" intrusion of privacy. *Doe v. Regents of Univ. of Cal.*, 23-cv-00598-WHO (N.D. Cal. May 6, 2023).

Defendant Knew Plaintiffs' Private Information Included Sensitive Medical Information, Including Medical Records.

149. Defendant was aware that by incorporating the Meta Pixel onto its Web Properties, this would result in the disclosure and use of Plaintiffs' and Class Members' Private Information, including sensitive medical information.

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

151. Indeed, software companies like MyChart that provide online access to medical records utilized by Defendant have "specifically recommended heightened caution around the use of custom analytics." Despite this, Defendant continued to use the Meta Pixel on its Web Properties.

152. At all times relevant herein Meta notified its partners, including Defendant, to have the rights to collect, use, and share user data before providing any data to Meta.[57] Although Meta's intent is questionable, Defendant had been on notice of this Pixel-tracking ever since they activated such Pixel technology on its Web Properties.

///

///

///

///

[57] *See In re Meta Pixel Healthcare Litig.*, No. 22-cv-03580-WHO, 2022 U.S. Dist. LEXIS 230754, at *13-14 (N.D. Cal. Dec. 22, 2022)

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

> **Information from partners.**
> Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services —whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.
>
> Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from.
>
> To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

153. Meta changed this provision again in July 2022, while still requiring partners to have the right to share patient information with Meta:[58]

> **How do we collect or receive this information from partners?**
>
> Partners use our Business Tools, integrations and Meta Audience Network technologies to share information with us.
>
> These Partners collect your information when you visit their site or app or use their services, or through other businesses or organizations they work with. We require Partners to have the right to collect, use and share your information before giving it to us.

154. Defendant had the explicit option to disable the Pixel technology on its Web Properties, but chose not to exercise this option, thereby continuing to share data with Facebook despite the availability of preventive measures.

[58] Meta, *Data Policy: Information from Partners, vendors and third parties* (Jan. 1, 2023), https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors.

155. Meta advised third party entities, like Defendant, to refrain from sending any information they did not have the legal right to send and expressly emphasized not to transmit health information. Yet, Defendant, in direct contravention of these disclosures, and more importantly despite Defendant's promises to keep all health-related data about patients confidential, continued to employ Pixel tracking on its Web Properties, thereby sharing sensitive patient data without proper authorization or consent.

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

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

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

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

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

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

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

163. For example, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[59] Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[60]

164. Users act consistent with these preferences. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.[61]

165. Medical data is particularly even more valuable because unlike other personal information, such as credit card numbers which can be quickly changed, medical data is static. This is why companies possessing medical information, like Defendant, are intended targets of cyber-criminals.[62]

---

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

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

[61] Margaret Taylor, *How Apple Screwed Facebook*, WIRED (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

166. Patients using Defendant's Web Properties must be able to trust that the information they input including their physicians, their health conditions and courses of treatment will be protected. Indeed, numerous state and federal laws require this. And these laws are especially important when protecting individuals with particular medical conditions such as HIV or AIDS that can and do subject them to regular discrimination. Furthermore, millions of Americans keep their health information private because it can become the cause of ridicule and discrimination. For instance, despite the anti-discrimination laws, persons living with HIV/AIDS are routinely subject to discrimination in healthcare, employment, and housing.[63]

167. The concern about sharing medical information is compounded by the reality that advertisers view this type of information as particularly high value. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one article put it: "the datafication of family life can begin from the moment in which a parent thinks about having a baby."[64] The article continues, "[c]hildren today are the very first generation of citizens to be datafied from before birth, and we cannot foresee — as yet — the social and political consequences of this historical transformation. What is particularly worrying about this process of datafication of children is that companies like . . . Facebook . . . are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[65]

168. Other privacy law experts have expressed concerns about the disclosure to third parties of a users' sensitive medical information. For example, Dena

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

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

[65] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance and how much you pay for that coverage, increase the rate you are charged on loans, and leave you vulnerable to workplace discrimination.[66]

169. A 2021 report by Invisibly found that personal medical information is one of the most valuable pieces of information within the market for data. The report noted that "[i]t's worth acknowledging that because health care records often feature a more complete collection of the PII User's identity, background, and personal identifying information (PII), health care records have proven to be of particular value for data thieves. While a single social security number might go for $0.53, a complete health care record sells for $250 on average.[67]

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

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

[67] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, NO. 220 (Apr. 2, 2013) https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited Oct. 10, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

Plaintiff B.K.

171. Plaintiff has a knee condition and has been a patient at Eisenhower Health in Southern California since 2013. Plaintiff started using the Eisenhower Health website over three years ago, utilizing the Web Properties many times in the recent years. Plaintiff has had a Facebook account for over a decade, and started to receive unsolicited advertisements relating to her medical conditions shortly after visiting Eisenhower Health's Web Properties.

172. Defendant encouraged Plaintiff to utilize Eisenhower Health's website and online portal in order to search for doctors, make appointments, review medical treatments, and to review charts from previous exams.[68]

173. While using Defendant's Web Properties, Plaintiff communicated sensitive – and what she expected to be confidential – personal and medical information to Defendant.

174. Plaintiff used Eisenhower Health's Web Properties to research healthcare providers (including orthopedic specialists and primary care doctors) and communicate with them, research particular medical concerns and treatments, fill out forms and questionnaires, schedule and attend appointments including knee replacements, and perform other tasks related to her specific medical inquiries and treatment.

[68] *See, e.g.*, *MyChart,* EISENHOWER HEALTH, https://eisenhowerhealth.org/resources/mychart/ ("MyChart is the Eisenhower Health patient portal and will allow you to access your Eisenhower Medical Records online and to communicate with your Eisenhower provider online.").

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

175. Plaintiff also utilized Eisenhower Health's Patient Portal to refill prescriptions, look at her bills and payments, and to see her test results and notes from her appointments.

176. While using Eisenhower Health's digital services, Plaintiff communicated and received information regarding her appointments, treatments, medications, and clinical information, including her surgeries, lab work, and scans. As a result of the Meta Pixel Defendant chose to install on its Web Properties, this information was intercepted, viewed analyzed, and used by unauthorized third parties.

177. Plaintiff accessed Eisenhower Health's Web Properties in connection with receiving healthcare services from Eisenhower Health or Eisenhower Health's affiliates at Eisenhower Health's direction and with Eisenhower Health's encouragement.

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

179. As a medical patient using Eisenhower Health's health services, Plaintiff reasonably expected that her online communications with Eisenhower Health were solely between herself and Eisenhower Health, and that such communications would not be transmitted or intercepted by a third party. Plaintiff also relied on Eisenhower Health's Privacy Policies in reasonably expecting Eisenhower Health would safeguard his Private Information. But for her status as Eisenhower Health's patient and its representations via its Privacy Policies, Plaintiff would not have disclosed her Private Information to Eisenhower Health.

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

Plaintiff N.Z.

181. Plaintiff has been a patient at Eisenhower Health in Southern California since at least 2016. Plaintiff started using the Eisenhower Health website over seven years ago, utilizing the Web Properties many times in the recent years for herself and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

for her husband. Plaintiff has had a Facebook account for over a decade and started to receive unsolicited advertisements relating to her husband's medical conditions, including but not limited to, shortly after visiting Eisenhower Health's Web Properties.

182. Defendant encouraged Plaintiff and her husband to utilize Eisenhower Health's Web Properties in order to search for doctors, make appointments, review medical treatments, and to review charts from previous exams.

183. While using Defendant's Web Properties, Plaintiff communicated sensitive – and what she expected to be confidential – personal and medical information to Defendant.

184. Plaintiff used Eisenhower Health's Web Properties to research healthcare providers and communicate with them, research particular medical concerns and treatments, fill out forms and questionnaires, schedule and attend appointments, and perform other tasks related to her and her husband's specific medical inquiries and treatment.

185. Plaintiff also utilized Eisenhower Health's Patient Portal to refill prescriptions, look at her and her husband's bills and payments, and to see their test results and notes from their appointments.

186. While using Eisenhower Health's Web Properties, Plaintiff communicated and received information regarding her and her husband's appointments, treatments, medications, and clinical information, including her surgeries, lab work, and scans. As a result of the Meta Pixel Defendant chose to install on its Web Properties, this information was intercepted, viewed analyzed, and used by unauthorized third parties.

187. Plaintiff accessed Eisenhower Health's Web Properties in connection with receiving healthcare services from Eisenhower Health or Eisenhower Health's affiliates at Eisenhower Health's direction and with Eisenhower Health's encouragement.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

189. As a medical patient (and her husband's proxy) using Eisenhower Health's health services, Plaintiff reasonably expected that her online communications with Eisenhower Health were solely between herself and Eisenhower Health, and that such communications would not be transmitted or intercepted by a third party. Plaintiff also relied on Eisenhower Health's Privacy Policies in reasonably expecting Eisenhower Health would safeguard her and her husband's Private Information. But for her status as Eisenhower Health's patient and its representations via its Privacy Policies, Plaintiff would not have disclosed her and her husband's Private Information to Eisenhower Health.

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

TOLLING, CONCEALMENT & ESTOPPEL

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

192. Defendant secretly incorporated the Meta Pixel into its Web Properties and patient portals, providing no indication to Users that their User Data, including their Private Information, would be disclosed to unauthorized third parties.

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

194. Plaintiffs and Class Members could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of Meta Pixels is highly technical and there were no disclosures or other indications that would

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

inform a reasonable consumer that Defendant was disclosing and allowing Facebook to intercept Users' Private Information.

195. The earliest Plaintiffs and Class Members could have known about Defendant's conduct was approximately in April or May of 2023. Nevertheless, at all material times herein, Defendant falsely represented to Plaintiffs that their health information is not and will not be disclosed to any third party.

196. As alleged above, Defendant has a duty to disclose the nature and significance of its data disclosure practices but failed to do so. Defendant is therefore estopped from relying on any statute of limitations under the discovery rule.

CLASS ALLEGATIONS

197. **Class Definition:** Plaintiffs bring this action on behalf of themselves and on behalf of various classes of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.:

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

> **Nationwide Class**: All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel on Defendant's Web Properties.

199. The California Subclass that Plaintiffs seek to represent is defined as:

> **California Subclass:** All individuals residing in the State of California whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel on Defendant's Web Properties.

200. The Nationwide Class, and the California Subclass are referred to collectively as the "Classes." Excluded from the Classes are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant's officer or director, any successor or assign and any Judge who adjudicates this case, including their staff and immediate family.

201. **The following people are excluded from the Classes:** (1) any Judge or Magistrate presiding over this action and members of their immediate families; (2)

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

202. Plaintiffs reserve the right under Federal Rule of Civil Procedure 23 to amend or modify the Classes to include a broader scope, greater specificity, further division into subclasses, or limitations to particular issues. Plaintiffs reserve the right under Federal Rule of Civil Procedure 23(c)(4) to seek certification of particular issues.

203. The requirements of Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) are met in this case.

204. The Fed. R. Civ. P. 23(a) elements of Numerosity, Commonality, Typicality, and Adequacy are all satisfied.

205. **Numerosity:** The exact number of Class Members is not available to Plaintiffs, but it is clear that individual joinder is impracticable. Hundreds of thousands of people have used Eisenhower Health's Web Properties since at least 2015. Members of the Class can be identified through Defendant's records or by other means.

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

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

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

a. Entering a declaratory judgment against Defendant—declaring that Defendant's interception of Plaintiffs' and Class Members' Private Information is in violation of the law;

b. Entering an injunction against Defendant:

i. preventing Defendant from sharing Plaintiffs' and Class Members' Private Information among itself and other third parties;

ii. requiring Defendant to alert and/or otherwise notify all users of its websites and portals of what information is being collected, used, and shared;

iii. requiring Defendant to provide clear information regarding its practices concerning data collection from the users/patients of Defendant's Web Properties, as well as uses of such data;

iv. requiring Defendant to establish protocols intended to remove all personal information which has been leaked to Facebook

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

and/or other third parties, and request Facebook/third parties to remove such information;

v. and requiring Defendant to provide an opt out procedure for individuals who do not wish for their information to be tracked while interacting with Defendant's Web Properties.

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

i. Whether Defendant's acts and practices violated California's Constitution, Art. 1, § 1;

ii. Whether Defendant's acts and practices violated California's Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq*.;

iii. Whether Defendant's acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;

iv. Whether Defendant's unauthorized disclosure of Users' Private Information was negligent;

v. Whether Defendant owed a duty to Plaintiffs' and Class Members not to disclose their Private Information to unauthorized third parties;

vi. Whether Defendant breached its duty to Plaintiffs and Class Members not to disclose their Private Information to unauthorized third parties;

vii. Whether Defendant represented to Plaintiffs and the Class that it would protect Plaintiff's and the Class Members' Private Information;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

viii. Whether Defendant violated Plaintiffs' and Class Members' privacy rights;

ix. Whether Defendant's practices violated California's Confidentiality of Medical Information Act, Civ. Code §§ 56, *et seq.*;

x. Whether Defendant's practices violated California's Constitution, Art. 1, § 1;

xi. Whether Plaintiffs and Class Members are entitled to actual damages, enhanced damages, statutory damages, and other monetary remedies provided by equity and law;

xii. Whether injunctive and declaratory relief, restitution, disgorgement, and other equitable relief is warranted.

211. **Superiority:** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by individual Class Members will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual Class Members to obtain effective relief from Defendant's misconduct. Even if Class Members could mount such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort and expense will be enhanced, and uniformity of decisions ensured.

212. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant misrepresented that it would disclose personal information only for limited purposes that did not include purposes of delivering advertisements or collecting data for commercial use or supplementing consumer profiles created by data aggregators and advertisers;

b. Whether Defendant's privacy policies misrepresented that it collected and shared User information with third-party service providers only for the limited purpose of providing access to its services;

c. Whether Defendant misrepresented that it had in place contractual and technical protections that limit third-party use of User information and that it would seek User consent prior to sharing Private Information with third parties for purposes other than provision of its services;

d. Whether Defendant misrepresented that any information it receives is stored under the same guidelines as any health entity that is subject to the strict patient data sharing and protection practices set forth in the regulations propounded under HIPAA;

e. Whether Defendant misrepresented that it complied with HIPAA's requirements for protecting and handling Users' PHI;

f. Whether Defendant shared the Private Information that Users provided to Defendant with advertising platforms, including Facebook, without adequate notification or disclosure, and without Users' consent, in violation of health privacy laws and rules and its own privacy policy;

g. Whether Defendant integrated third-party tracking tools, consisting of automated web beacons ("**Pixels**") in its website that shared Private Information and User activities with third parties for unrestricted purposes, which included advertising, data analytics, and other commercial purposes;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

h. Whether Defendant shared Private Information and activity information with Facebook using Facebook's tracking Pixels on its Web Properties without Users' consent;

i. Whether Facebook used the information that Defendant shared with it for unrestricted purposes, such as selling targeted advertisements, data analytics, and other commercial purposes.

COUNT ONE

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

(On behalf of Plaintiffs and the California Subclass)

213. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

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

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

216. Section 56.101 of the CMIA states, in pertinent part, that "[a]ny provider of health care . . . who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties . . ." Cal. Civ. Code §§ 56.10, 56.101.

217. Plaintiffs' and California Subclass Members' Private Information constitutes "medical information" under the CMIA because it consists of individually identifiable information in possession of and derived from a provider of healthcare

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

regarding Plaintiffs' and California Subclass Members' medical history, test results, mental or physical condition, and/or treatment.

218. Defendant violated Cal. Civ. Code § 56.10 because they failed to maintain the confidentiality of Users' medical information, and instead "disclose[d] medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization" by soliciting, intercepting, and receiving Plaintiffs' and California Subclass Members' Private Information, and sharing it with advertisers and for advertising purposes. Specifically, Defendant knowingly, willfully, or negligently disclosed Plaintiffs' and California Subclass Members' medical information to Facebook, allowing Facebook to now advertise and target Plaintiffs and California Subclass Members, misusing their extremely sensitive Private Information.

219. Defendant violated Cal. Civ. Code § 56.101 because they knowingly, willfully, or negligently failed to create, maintain, preserve, store, abandon, destroy, and dispose of medical information in a manner that preserved its confidentiality by soliciting, intercepting, and receiving Plaintiffs' and California Subclass Members' Private Information, and sharing it with advertisers and for advertising purposes for Facebook's and Defendant's financial gain.

220. Defendant intentionally embedded Facebook Pixels, which facilitate the unauthorized sharing of Plaintiffs' and California Subclass Members' medical information.

221. Defendant violated Cal Civ. Code § 56.36(b) because they negligently released confidential information and records concerning Plaintiffs and California Subclass Members in violation of their rights under the CMIA.

222. As a direct and proximate result of Defendant's misconduct, Plaintiffs and California Subclass Members had their private communications containing information related to their sensitive and confidential Private Information intercepted, disclosed, and used by third parties.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

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

COUNT TWO

VIOLATIONS 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 Nationwide Class*)

225. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

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

227. 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.

228. The transmissions of Plaintiffs' PII and PHI to Defendant's Web Properties qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

229. **Electronic Communications**. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant's Web Properties with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

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

231. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding PII and PHI, diagnosis of certain conditions, treatment/medication for such conditions, and scheduling of appointments, including annual mammograms, surgeries, ER visits, lab work, and scans. Furthermore, Defendant intercepted the "contents" of Plaintiffs' communications in at least the following forms:

a. The parties to the communications;

b. The precise text of patient search queries;

c. Personally, identifying information such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;

d. The precise text of patient communications about specific doctors;

e. The precise text of patient communications about specific medical conditions;

f. The precise text of information generated when patients requested or made appointments,

g. The precise text of patient communications about specific treatments;

h. The precise text of patient communications about scheduling appointments with medical providers;

i. The precise text of patient communications about billing and payment;

j. The precise text of specific buttons on Defendant's Web Properties that patients click to exchange communications, including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

k. The precise dates and times when patients click to Log-In on Defendant's Web Properties;

l. The precise dates and times when patients visit Defendant's Web Properties;

m. Information that is a general summary or informs third parties of the general subject of communications that Defendant sends back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information.

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

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

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices

c. Defendant's web servers; and

d. The Pixel code deployed by Defendant to effectuate the sending and acquisition of

patient communications.

234. By utilizing and embedding the Pixel on its Web Properties, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

235. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Private Information to third parties such as Facebook.

236. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding PII and PHI, treatment, medication, and scheduling.

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

238. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

239. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

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

241. Defendant is not a party for purposes to the communication based on its unauthorized duplication and transmission of communications with Plaintiffs and the Class. However, even assuming Defendant is a party, Defendant's simultaneous,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

unknown duplication, forwarding, and interception of Plaintiffs' and Class Members' Private Information does not qualify for the party exemption.

242. Defendant's acquisition of patient communications that were used and disclosed to Facebook was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;

b. Invasion of privacy;

c. Breach of confidence;

d. Breach of fiduciary duty;

e. California Invasion of Privacy Act, §§ 630, *et seq.*;

f. California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56, *et seq.*;

243. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it: Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and disclosed individually identifiable health information to Facebook without patient authorization.

244. 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.

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

246. 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 about their Private Information on its Web Properties, because it used its participation in these communications to improperly share Plaintiffs' and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Class Members' Private Information with Facebook and third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know was receiving their information, and that Plaintiffs and Class Members did not consent to receive this information.

247. As such, Defendant cannot viably claim any exception to ECPA liability.

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

a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their PII and PHI (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiffs and the Class Members to suffer emotional distress;

a. Defendant received substantial financial benefits from its use of Plaintiffs' and the Class Members' PII and PHI without providing any value or benefit to Plaintiffs or the Class members;

b. Defendant received substantial, quantifiable value from its use of Plaintiffs' and the Class Members' PII and PHI, such as understanding how people use its Web Properties and determining what ads people see on its Web Properties, without providing any value or benefit to Plaintiffs or the Class Members;

c. 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 its patient information; and

d. 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, medical treatment, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

249. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' Private Information for financial gain.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

251. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading their privacy via the Pixel.

252. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

253. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's Web Properties, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

254. As a result of Defendant's violation of the ECPA, Plaintiffs and the Class 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 THREE

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")

18 U.S.C. § 2511(3)(a), *et seq.*

Unauthorized Divulgence by Electronic Communications Service

(On Behalf of Plaintiffs and the Nationwide Class)

255. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

256. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

257. Electronic Communication Service. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

258. Defendant's Web Properties are an electronic communication service. Specifically, the Web Properties provide to users thereof the ability to send or receive electronic communications. In the absence of Defendant's Web Properties, internet users could not send or receive communications regarding Plaintiffs' and Nationwide Class Members' Private Information.

259. Intentional Divulgence. Defendant intentionally designed and implemented the Pixel within its Web Properties, and was or should have been aware that, if misconfigured, it could divulge Plaintiffs' and Nationwide Class Members' Private Information.

260. While in Transmission. Upon information and belief, Defendant's divulgence of the contents of Plaintiffs' and Nationwide Class Members' communications was contemporaneous with their exchange with Defendant's Web Properties, to which they directed their communications.

261. Defendant divulged the contents of Plaintiffs' and Nationwide Class Members' electronic communications to third parties like Facebook without authorization.

262. Exceptions do not apply. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication as follows:

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or,

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency." 18 U.S.C. § 2511(3)(b).

263. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

264. Defendant's divulgence of the contents of Plaintiffs' and Nationwide Class Members' communications on Defendant's Web Properties to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

265. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

266. Defendant's divulgence of the contents of user communications on Defendant's browsers through the Pixel code was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (a) Plaintiffs and Nationwide Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Web Properties with which Plaintiffs and Nationwide Class Members were exchanging information.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

267. Moreover, Defendant divulged the contents of Plaintiffs' and Nationwide Class Members' communications through the Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

268. The contents of Plaintiffs' and Nationwide Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

269. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and reasonable attorney fees and other litigation costs reasonably incurred.

COUNT FOUR

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

(On behalf of Plaintiffs and the California Subclass)

270. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

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

272. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following: (1) "intentionally taps, or makes any unauthorized connection…with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system," (2) "willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

transit or passing over any wire, line or cable or is being sent from or received at any place within [the state of California]," (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained," or (4) ***aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section***" (emphasis added).

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

274. Defendant's Web Properties are a "machine, instrument, contrivance, or ... other manner" used to engage in the prohibited conduct at issue here.

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

276. At all relevant times, by using the Facebook Pixel, Facebook willfully and without the consent of Plaintiffs and California Subclass Members, read or attempted to learn the contents or meaning of electronic communications of Plaintiffs

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

and putative California Subclass Members on Defendant's Web Properties. This occurred while the electronic communications were in transit or passing over any wire, line, or cable, or were being sent from or received at any place within California. Facebook intercepted Plaintiffs' and California Subclass Members' communications – including the very terms and phrases they typed into the search bar – without their authorization or consent.

277. Defendant knowingly installed Pixel tracking technology on its Web Properties, which systematically transmitted all communications between Plaintiffs and the Defendant's Web Properties to Meta. Indeed, Meta released an explicit statement to the Court on November 9, 2022, that it neither desired nor intended to possess health information data. In April 2018, Meta proactively added a clause to its user contract specifying that it requires each of its partners, including Defendant, to have "lawful" rights to collect, use, and share user data before providing any data to Meta.

278. Defendant had the explicit option to disable the Pixel technology on its Web Properties, but chose not to exercise this option, thereby continuing to share data with Facebook despite the availability of preventive measures.

279. These assertions highlight that Meta advised third party entities, like Defendant, to refrain from sending any information they did not have the legal right to send and expressly emphasized not to transmit health information. Yet, Defendant, in direct contravention of these advisories and in a clear display of intent, continued to employ Pixel tracking on its Web Properties, thereby sharing sensitive patient data without proper authorization or consent.

280. Additionally, by embedding Facebook Pixels on its Web Properties, Defendant aided, agreed with, employed, and conspired with Facebook to wiretap consumers communications on Defendant's Web Properties using the Facebook Pixel snipped codes and to accomplish the wrongful conduct at issue here.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

282. Defendant both intercepted and aided Facebook in the interception of "contents" of Plaintiffs' communications in at least the following forms:

a. The parties to the communications;

b. The precise text of patient search queries;

c. Personally identifying information such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;

d. The precise text of patient communications about specific doctors;

e. The precise text of patient communications about specific medical conditions;

f. The precise text of information generated when patients requested or made appointments;

g. The precise text of patient communications about specific treatments;

h. The precise text of patient communications about scheduling appointments with medical providers;

i. The precise text of patient communications about billing and payment;

j. The precise text of specific buttons on Defendant's Webs Properties that patients click to exchange communications, including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;

k. The precise dates and times when patients click to Log-In on Defendant's Web Properties;

l. The precise dates and times when patients visit Defendant's Web Properties;

m. Information that is a general summary or informs third parties of the

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

general subject of communications that Defendant sends back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information; and

n. Any other content that Defendant has aided third parties in scraping from webpages or communication forms at Web Properties.

283. Defendant gave substantial assistance to Facebook in violating the privacy rights of Defendant's patients, despite the fact that Defendant's conduct constituted a breach of the duties of confidentiality that medical providers owe their patients. Defendant knew that the installation of the Meta Pixel on its Web Properties would result in the unauthorized disclosure of its patients' communications to Facebook, yet nevertheless did so anyway.

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

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

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

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

288. In addition to statutory damages, Defendant's breach caused Plaintiffs and Class Members, at minimum, the following damages: (1) Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private; and (2) 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 sharing the benefit of such value.

COUNT FIVE

VIOLATION OF THE UNFAIR COMPETITION LAW ("UCL")

CALIFORNIA BUSINESS AND PROFESSIONS CODE § 17200, *et seq*.

(On behalf of Plaintiffs and the Nationwide Class and, alternatively, the California Subclass)

289. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

A. Unlawful Prong

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

291. Defendant's conduct, as alleged herein, was also fraudulent within the meaning of the UCL. Defendant made deceptive misrepresentations and omitted known material facts in connection with the solicitation, interception, disclosure, and use of Plaintiffs' and Nationwide Class Members' Private Information. Defendant actively concealed and continued to assert misleading statements regarding its protection and limitation on the use of the Private Information. Meanwhile, Defendant was collecting and sharing Plaintiffs' and Nationwide Class Members' Private Information without their authorization or knowledge to profit off of the information, and deliver targeted advertisements to Plaintiffs and Nationwide Class Members, among other unlawful purposes.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

293. Had Plaintiffs and Nationwide Class Members known Defendant would disclose and misuse their Private Information in contravention of Defendant's representations, they would never have used Defendant's Web Properties Portal and would not have shared their Private Information.

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

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

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

B. Unfair Prong

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

299. Because Defendant are in the business of providing medical healthcare services, Plaintiffs and Nationwide Class Members relied on Defendant to advise them of any potential disclosure of their Private Information.

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

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

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

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

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

305. Defendant's acts, omissions and conduct also violate the unfair prong of the UCL because those acts, omissions and conduct offended public policy (including the aforementioned federal and state privacy statutes and state consumer protection

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

statutes, such as HIPAA), and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and Nationwide Class Members.

306. As a direct result of Plaintiffs' and Nationwide Class Members' reliance on Defendant's representations that Defendant would keep their Private Information confidential and Defendant's express representation that they would not share Private Information with third parties without the Users' express consent, Plaintiffs and Nationwide Class Members shared highly sensitive information through their use of the Web Properties, causing them to suffer damages when Defendant disclosed said information to a third party.

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

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

COUNT SIX

INVASION OF PRIVACY UNDER CALIFORNIA'S CONSTITUTION, ART. I, § 1.

(On behalf of Plaintiffs and the California Subclass)

309. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

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

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

313. At all relevant times, by using Facebook's Meta Pixel to record and communicate individually identifying information alongside their confidential medical communications, Defendant invaded Plaintiffs' and California Subclass Members' privacy rights under the California Constitution.

314. Plaintiffs and California Subclass Members had a reasonable expectation that their communications, identity, health information, and other data would remain confidential, and that the Defendant would not install wiretaps on its Web Properties to secretly transmit communications to a third party.

315. Plaintiffs and California Subclass Members did not authorize the Defendant to record and transmit their Private Information – including private medical communications alongside their personally identifiable health information – to a third party, Facebook. *See* Figures 2-15 of Defendant's Web Properties above.

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

317. As a result of the Defendant's actions, Plaintiffs and California Subclass Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

318. Plaintiffs and California Subclass Members have been damaged as a direct and proximate result of the Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

319. Plaintiffs and California Subclass Members seek appropriate relief for their injuries, including but not limited to damages that will reasonably compensate Plaintiffs and California Subclass Members for the harm to their privacy interests as a result of the intrusion(s) upon Plaintiffs' and California Subclass Members' privacy.

320. Plaintiffs and California Subclass Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of the Defendant's conduct, injuring Plaintiffs and California Subclass Members in conscious disregard of their rights.

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

COUNT SEVEN

INVASION OF PRIVACY

INTRUSION UPON SECLUSION

(On behalf of Plaintiffs and the Nationwide Class)

322. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

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

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

325. Defendant failed to protect and release to unknown and unauthorized third parties the Private Information of Plaintiffs and Nationwide Class Members.

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

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

328. Defendant's privacy policy specifically provides, "We will not sell, trade or rent your personal information to other people or businesses unless we have your consent."[69]

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

330. Defendant's unauthorized surreptitious recording, monitoring, and sharing of the Users' activities, searches, researching diagnosis and treatment, searching for doctors and medical specialists violated expectations of privacy that have been established by social norms.

331. As a proximate result of such unauthorized disclosures, Plaintiffs' and Nationwide Class Members' reasonable expectations of privacy in their Private

[69] *Notice of Privacy Policy*, *supra* note 40.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Information was unduly frustrated and thwarted and caused damages to Plaintiffs and Nationwide Class Members.

332. Plaintiffs and Nationwide Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's conduct, directed at injuring Plaintiffs and Nationwide Class Members in conscious disregard of their rights.

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

COUNT EIGHT

BREACH OF IMPLIED CONTRACT

(On behalf of Plaintiffs and the Nationwide Class)

334. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

335. When Plaintiffs and Nationwide Class Members provided their Private Information to Defendant in exchange for services, they entered into implied contracts by which Defendant agreed to safeguard and not disclose such Private Information without consent.

336. Plaintiffs and Nationwide Class Members accepted Defendant's offers of services and provided their Private Information to Defendant via the Web Properties.

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

338. Plaintiffs and Nationwide Class Members fully performed their obligations under the implied contracts with Defendant.

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

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

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

COUNT NINE

VIOLATION OF CALIFORNIA CONSUMERS LEGAL REMEDIES ACT,

Cal. Civ. Code § 1750, *et seq.* ("CLRA")

(*On behalf of Plaintiffs & the California Subclass*)

342. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

343. Defendant engaged in "unfair methods of competition and unfair or deceptive acts . . . in a transaction . . . that result[ed] . . . in the sale . . . of goods" to Plaintiffs and the California Subclass Members in violation of Cal. Civ. Code § 1750 and Cal. Civ. Code § 1770(a)(5), (7), (9), (14), (16).

344. For instance, Defendant made representations that it would protect Plaintiffs' and the Subclass Members' privacy interest, including promising that it will keep Private Information private and secure, that Defendant does not sell Users' Private Information, and that it will only disclose Private Information under certain circumstances, none of which was true.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

345. Defendant made these representations with no intention of living up to these representations. Contrary to these representations, Defendant disclosed and allowed third parties to intercept its customers' Private Information.

346. Further, Defendant failed to disclose it secretly shared, used, and allowed third parties to intercept Plaintiffs' and Subclass Members' Private Information.

347. Defendant was under a duty to disclose this information given Defendant's relationship with its customers and Defendant's exclusive knowledge of its misconduct (e.g., the tracking technology incorporated on Defendant's Website, the fact that Private Information is disclosed to unauthorized third parties, that Defendant allowed third parties to intercept Private Information through this technology, and how Defendant and third parties used this data).

348. Plaintiffs and Subclass Members would not have purchased, or would have paid significantly less for, Defendant's medical services had Defendant not made these false representations. Defendant profited directly from these sales, including through payment for these services, and from the Private Information disclosed and intercepted.

349. Plaintiffs, individually and on behalf of the Subclass Members, seek an injunction requiring Defendant to obtain consent prior to disclosing and otherwise using Plaintiffs' and Subclass Members' Private Information and to delete the Private Information already collected, and any other relief which the court deems proper.

COUNT TEN

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

(On behalf of Plaintiffs and the California Subclass)

350. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

351. Courts recognize that internet users have a property interest in their personal information and data. *See Calhoun v. Google, LLC,* 526 F. Supp. 3d 605, at

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

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

353. Penal Code § 496(a) creates an action against "any" person who (1) receives "any" property that has been stolen or obtained in any manner constituting theft, knowing the property to be stolen or obtained, or (2) conceals, sells, withholds, or aids in concealing or withholding "any" property from the owner, knowing the property to be so stolen or illegally obtained.

354. Under Penal Code § 1.07(a)(38), "person" means "an individual, corporation, or association." Thus, Defendant is a person under section 496(a).

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

356. Defendant meets the grounds for liability of section 496(a) because it:

a. knew the Private Information was stolen or obtained by theft and/or false pretenses; and, with such knowledge,

b. transmitted such information to unauthorized third parties, like Facebook.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

357. Defendant violated the second ground for liability of section 496(a) because it:

a. knew the Private Information was stolen or obtained by theft; and, with such knowledge,

b. concealed, withheld, or aided in concealing or withholding said data from their rightful owners by unlawfully tracking the data and disclosing it to unauthorized third parties, like Facebook.

358. As a direct and proximate result of the acts and omissions described above, Plaintiffs and California Subclass Members were injured by the Defendant's violations of section 496(a).

359. Pursuant to California Penal Code § 496(c), the Plaintiffs and California Subclass Members seek actual damages, treble damages, costs of suit, and reasonable attorneys' fees.

COUNT ELEVEN

NEGLIGENCE

(On behalf of Plaintiffs and the Nationwide Class)

360. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

361. Defendant owed a duty to Plaintiffs and the Nationwide Class to exercise due care in collecting, storing, safeguarding, and preventing any disclosure of their Private Information. This duty included but was not limited to: (a) preventing Plaintiffs' and Nationwide Class Members' Private Information from being to be disclosed to unauthorized third parties; and (b) destroying Plaintiffs' and Nationwide Class Members' Private Information within an appropriate amount of time after it was no longer required by Defendant.

362. Defendant's duties to use reasonable care arose from several sources, including those described below. Defendant had a common law duty to prevent foreseeable harm to others, including Plaintiffs and Nationwide Class Members, who

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

were the foreseeable and probable victims of any data misuse, such as disclosure of Private Information to unauthorized parties.

363. Defendant had a special relationship with Plaintiffs and Nationwide Class Members, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Nationwide Class Members resulting from unauthorized disclosure of their Private Information to third parties such as Facebook. Plaintiffs and Nationwide Class Members were compelled to entrust Defendant with their Private Information. At relevant times, Plaintiffs and Nationwide Class Members understood that Defendant would take adequate data storage practices to safely store their Private Information. Only Defendant had the ability to protect Plaintiffs' and Nationwide Class Members' Private Information collected and stored on Defendant's Web Properties.

364. Defendant's duty to use reasonable measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of [PHI]." 45 C.F.R. § 164.530(c)(1).

365. Defendant's conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiffs' and the Nationwide Class Members' Private Information by failing to protect this information.

366. Plaintiffs and Nationwide Class Members trusted Defendant and in doing so provided Defendant with their Private Information, based upon Defendant's representations that it "committed to protecting the privacy of [users'] medical information." and Defendant is "required by law to maintain the confidentiality of

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

information that identifies [users] and the care [users'] receive."[70] Defendant failed to do so.

367. Defendant breached its duty in this relationship to collect and safely store Plaintiffs' and Nationwide Class Members' Private Information.

368. Plaintiffs' and the Nationwide Class Members' Private Information would have remained private and secure had it not been for Defendant's wrongful and negligent breach of its duties. Defendant's negligence was, at least, a substantial factor in causing Plaintiffs' and Nationwide Class Members' Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing Plaintiffs and the Nationwide Class Members other injuries because of the unauthorized disclosures.

369. The damages suffered by Plaintiffs and the Nationwide Class Members were the direct and reasonably foreseeable result of Defendant's negligent breach of its duties to maintain Users' Private Information. Defendant knew or should have known that its unauthorized disclosure of highly sensitive Private Information was a breach of its duty to collect and safely store such information.

370. Defendant's negligence directly caused significant harm to Plaintiffs and the Nationwide Class. Specifically, Plaintiffs and Nationwide Class Members are now subject to their sensitive information being accessed by unauthorized parties, which may lead to significant harms.

371. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

372. Defendant had a fiduciary duty to protect the confidentiality of its communications with Plaintiffs and Nationwide Class Members by virtue of the explicit privacy representations Defendant made on its websites to Plaintiffs and members of the Nationwide Class.

373. Defendant had information relating to Plaintiffs and Nationwide Class Members that it knew or should have known to be confidential.

[70] *Privacy Policy*, *supra* note 40.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

374. Plaintiffs' and Nationwide Class Members' communications with Defendant about sensitive Private Information and their status as patients of Defendant were not matters of general knowledge.

375. Defendant breached its fiduciary duty of confidentiality by designing its data protection systems in a way to allow for a data breach of a massive caliber.

376. At no time did Plaintiffs or Nationwide Class Members give informed consent to Defendant's conduct.

377. As a direct and proximate cause of Defendant's actions, Plaintiffs and Nationwide Class Members suffered damage in that the information they intended to remain private is no longer so and their Private Information was disclosed to, tracked, and intercepted by third-party Internet tracking companies, including Facebook, without their knowledge or consent.

COUNT TWELVE

BREACH OF CONFIDENCE

(*On Behalf of Plaintiffs and the Nationwide Class*)

378. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

379. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

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

381. Plaintiffs' and Class Members' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Privacy Policies.

382. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Pixel (and other tracking technologies) to

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

disclose and transmit Plaintiffs' and Class Members' Private Information and the contents of their communications exchanged with Defendant to third parties.

383. The third-party recipients included, but were not limited to, Facebook and other online marketers.

384. Defendant's disclosures of Plaintiffs' and Class Members' Private Information were made without their knowledge, consent or authorization, and were unprivileged.

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

386. 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. Defendant eroded the essential confidential nature of the provider-patient relationship;

c. 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 compensating Plaintiffs and Class Members for the data;

d. 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;

e. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information; and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

f. Defendant's actions violated the property rights Plaintiffs and Class Members have in their Private Information.

387. Plaintiffs and Class Members are therefore entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation. Plaintiffs are also entitled to punitive damages.

COUNT THIRTEEN

BREACH OF FIDUCIARY DUTY

(*On Behalf of Plaintiffs and the Nationwide Class*)

388. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

389. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

390. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant' relationship with its patients and former patients, in particular, to keep secure their Private Information.

391. Defendant breached its fiduciary duties to Plaintiffs and Class Members by disclosing their Private Information to unauthorized third parties, and separately, by failing to notify Plaintiffs and Class Members of this fact.

392. As a direct and proximate result of Defendant' breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

and are entitled to compensatory, nominal, and/or punitive damages, and disgorgement of profits, in an amount to be proven at trial.

COUNT FOURTEEN

UNJUST ENRICHMENT

(On behalf of Plaintiffs and Nationwide Class)

393. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

394. Plaintiffs and Class Members personally and directly conferred a benefit on Defendant by paying Defendant for health care services, which included Defendant's obligation to protect Plaintiffs' and Class Members' Private Information. Defendant was aware of Plaintiffs' privacy expectations, and in fact, promised to maintain Plaintiffs' Private Information confidential and not to disclose to third parties. Defendant received payments for medical services from Plaintiffs and Class Members.

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

396. Plaintiffs and Class Members would not have used Defendant's Web Properties had they known that Defendant would collect, use, and disclose this information to Facebook, Google, and other third parties. The services that Plaintiffs and Class Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

which included Defendant's promise that any patient communications with Defendant would be treated as confidential and would never be disclosed to third parties for marketing purposes without the express consent of patients.

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

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

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

400. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in the loss of value of their Private Information and the lost profits from the use of their Private Information.

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

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

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

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

PRAYER FOR RELIEF

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

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

B. That the Court enter an order:

a. Preventing Defendant from sharing Plaintiffs' and Class Members' Private Information among other third parties;

b. Requiring Defendant to alert and/or otherwise notify all users of its websites and portals of what information is being collected, used, and shared;

c. Requiring Defendant to provide clear information regarding its practices concerning data collection from the users/patients of Defendant's Web Properties, as well as uses of such data;

d. Requiring Defendant to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

e. Requiring Defendant to provide an opt out procedures for individuals who do not wish for their information to be tracked while interacting with Defendant's Web Properties;

f. Mandating the proper notice be sent to all affected individuals, and posted publicly;

g. Requiring Defendant to delete, destroy, and purge the Private Information of Users unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Users;

h. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

C. That the Court award Plaintiffs and the Class Members damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

D. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiffs and the Class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

E. Plaintiffs and the Class be awarded with pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

F. Plaintiffs and the Class be awarded with the reasonable attorneys' fees and costs of suit incurred by their attorneys;

G. Plaintiffs and the Class be awarded with treble and/or punitive damages insofar as they are allowed by applicable laws; and

H. Any and all other such relief as the Court may deem just and proper under the circumstances.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

JURY TRIAL DEMANDED

Plaintiffs demand a jury trial on all triable issues.

DATED: October 12, 2023

CLARKSON LAW FIRM, P.C.

/s/ Yana Hart
Ryan Clarkson, Esq.
Yana Hart, Esq.
Tiara Avaness, Esq.
Valter Malkhasyan, Esq.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com