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
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070

ALMEIDA LAW GROUP LLC
John R. Parker, Jr. (SBN 257761)
jrparker@almeidalawgroup.com
3550 Watt Avenue, Suite 140
Sacramento, CA 95821
Tel: (916) 616-2936

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-02092-JBG-DTB

FIRST AMENDED 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 CALIFORNIA INVASION OF PRIVACY ACT, CAL. PENAL CODE SECTION 630, *et seq.*
4. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE SECTION 17200, *et seq*.

5. INVASION OF PRIVACY UNDER CALIFORNIA CONSTITUTION

6. INVASION OF PRIVACY - INTRUSION UPON SECLUSION

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

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

9. BREACH OF CONFIDENCE

10. BREACH OF FIDUCIARY DUTY

11. 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

TABLE OF CONTENTS

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

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**" 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.

I. INTRODUCTION

1. Defendant Eisenhower 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 includes a children's center, birth center, bariatric care, emergency center, and the Eisenhower Medical Center 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. Defendant also runs a system of primary care clinics providing medical care to families as well as multiple urgent care locations allowing patients to seek medical consultations on a walk-in basis.[3]

---

[1] *Eisenhower Health Main Campus*, EISENHOWER HEALTH, https://eisenhowerhealth.org/locations/?action=detail&dataRef=15 (last visited on April 19, 2024).

[2] *Eisenhower Medical Center,* EISENHOWER HEALTH, https://eisenhowerhealth.org/locations/?cache=on&action=detail&dataRef=67&template= (last visited on April 19, 2024).

[3] *Eisenhower Primary Care*, EISENHOWER HEALTH, https://eisenhowerhealth.org/services/primarycare/epc/; *Urgent Care*, EISENHOWER HEALTH, https://eisenhowerhealth.org/services/urgent-care/ (last visited on April 19, 2024).

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

4. This case arises from Defendant's systematic violation of the medical privacy rights of its patients by exposing their highly sensitive personal information without knowledge or consent to Meta Platform Inc. d/b/a Facebook ("**Meta**" or "**Facebook**") and Google, via tracking and collection tools surreptitiously enabled on Defendant's website(s).

5. Defendant operates a website, https://www.eisenhowerhealth.org (the "**Website**"), and a patient portal, https://mychart.eisenhowerhealth.org/mychart (the "**Portal**" and collectively with the Website, the "**Web Properties**").

6. Defendant has disregarded the privacy rights of its patients (including potential patients) who used its Web Properties ("**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 enabled unauthorized third parties such as Facebook and Google to intercept the content of its Users' communications on Defendant's Web Properties.

Defendant Intercepted and Disclosed to Meta Plaintiffs' and Class Members' Private Information in Violation of HIPAA and State, Federal and Common Law

7. Unbeknownst to Users and without Users' authorization or informed consent, Defendant installed Facebook's Meta Pixel ("**Meta Pixel**" or "**Pixel**") and other invisible third-party tracking technology, on its Web Properties in order to intercept Users' PII and PHI with the express purpose of disclosing that Private Information to third parties such as Meta and/or Google in violation of HIPAA Privacy Rule and 42 U.S.C. § 1320d-6 as well as state, federal and common law.[4]

[4] At the time of filing this complaint Plaintiffs are unable to determine whether Pixels were embedded inside Defendant's MyChart Portal. However, given Defendant's use of the Meta Pixel on other pages of the Website including the log-in page for its patient Portal, Plaintiffs reasonably believe and, therefore, aver that

8. Meta then improperly accesses and uses the Private Information so that it can associate that information with the individual User whose information was disclosed and then create targeted advertising that it sends to that User's personal Facebook account.

9. Meta is able to personally identify each User with an active Facebook account by using the "c_user" cookie that Meta stores in users' browsers and which reveals a Facebook account-holder's unique "FID" value. A user's FID is linked to their Facebook profile, which personally identifies the user through a wide range of demographic and other information about the user, including the user's name, pictures, personal interests, work history, relationship status, and other details. Because the user's FID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the FID to quickly and easily locate, access, and view the user's corresponding Facebook profile.[5]

10. However, the Pixel collects data regardless of whether the Website visitor has a Facebook account. In fact, Facebook maintains "shadow profiles" on users without Facebook accounts and links the information collected via the Pixel to the user's real-world identity using their shadow profile.[6]

11. The screenshots of Defendant's website, more fully explained *infra*, demonstrate how the Meta Pixel intercepts Users' Private Information, including the

---

Defendant used the Pixels to track information on its entire digital platform, including inside its MyChart Portal. *See also*, Todd Feathers, *et al.*, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022) (listing examples of hospitals that used third party trackers inside password-protected patient portals), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

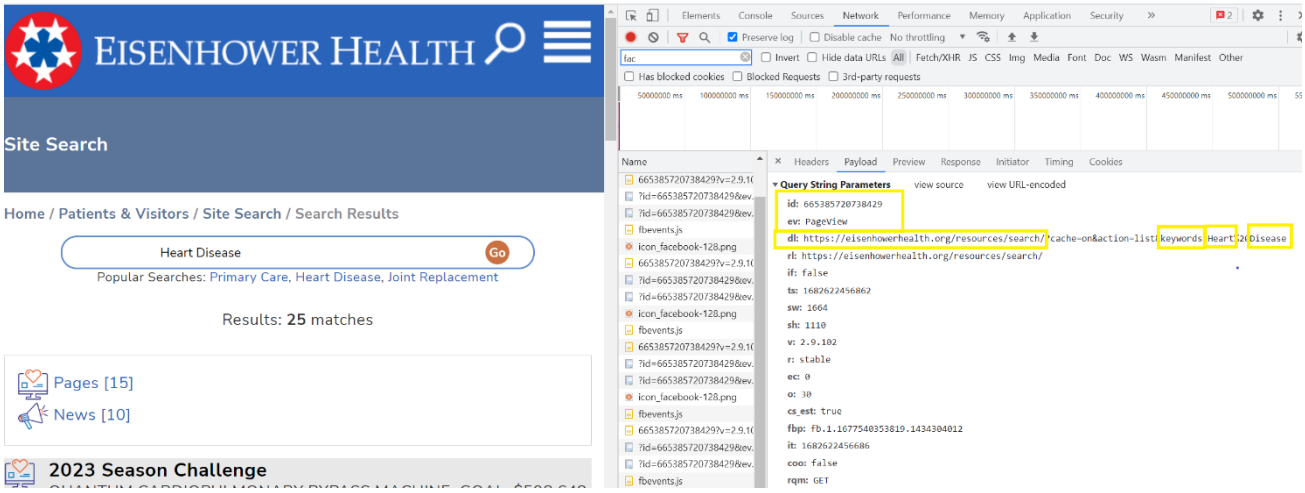
[5] To find the Facebook account associated with a particular c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

[6] Russell Brandom, *Shadow Profiles Are The Biggest Flaw In Facebook's Privacy Defense*, THEVERGE.COM (Apr. 11, 2018), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (last visited Apr. 19, 2024).

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

Private Information of Plaintiffs and Class Members.

12. The first screenshot below shows what a webpage from Defendant's Web Properties looks like and how the Pixel works to disclose information to Meta.



13. On the left-hand side of the screenshot is the page as it appears to any User visiting this webpage. This is the result the User would see when they went to Eisenhower's search bar, typed in "heart disease" and pressed Enter. There are 25 matches for that search on Defendant's Website.

14. The right-hand side of the screenshot shows the information Defendant is disclosing to Meta through the Pixel which runs in the background, unbeknownst to the User.

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

15. Below is a larger image of the left hand of the screenshot above. A closer inspection of the information being conveyed makes it apparent that Defendant is disclosing both personally identifiable information in the form of the c_user FID, which uniquely identifies an individual's Facebook account (as well as other cookies that Facebook is known to utilize to identify individuals), as well as the PHI that the User is sharing with Defendant when they use the Website.

16. The highlighted portions reveal the information that Defendant is sharing with Meta. Beginning at the top, "id=665385…" is the unique ID number of the Pixel installed by Defendant. Immediately to the right is "PageView," a type of 'event' collected by the Pixel as the User navigates the Website which shares the URL of the page that the User is visiting.[7] Finally, continuing to the right on the top line, Defendant is disclosing that the User is visiting the webpage

[7] A url is just the web address that your type in the address bar at the top of the screen or which appear in the address bar when you click on a link. It stands for Uniform Resource Locator. When you go to use google, the url that appears is google.com. And when you click on google maps, the url changes to google.com/maps. It is that extension to the url, "maps" that provides additional pageview information that allows pixels and trackers to know more about your internet usage.

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

"eisenhowerhealth.org/resources."

17. On the next line down, Defendant is disclosing to Meta the PHI of the User. Specifically, Defendant is disclosing that the User performed a "search" and the "keywords" they typed in for that search were "Heart Disease." Defendant is disclosing to Meta that the User is searching for information related to the condition and treatment of heart disease, personal health information that is protected by HIPAA.

18. Further down, the last highlighted line contains the disclosed PII that allows Meta to specifically associate the PHI shared in the earlier lines with a specific individual.

19. The first highlighted term is "datr" followed by a unique alphanumeric code. The "*datr*" cookie identifies the specific web browser from which the User is sending the communication. It is an identifier that is unique to the User's web browser and is therefore a means of identification for Meta. Meta keeps a record of every datr cookie identifier associated with each of its users.

20. Finally, there is the highlighted "c_user" cookie followed by a number which contains the unique Facebook User ID for the person who is visiting this webpage. This user ID, or FID, can be used to easily find the Facebook account of any User. With a person's FID (for example, FID 12345), anyone can add that number to the end of the Facebook URL to find the User's profile. In this example, typing facebook.com/12345 into a web browser would bring up the Facebook profile of the individual with the FID 12345.

21. As demonstrated by this screenshot, and the ones *infra*, the Pixel Defendant installed on its Web Properties, intercepted both the PII and the PHI of every User that visited every webpage on the Web Properties, with the specific purpose of disclosing that HIPAA-protected health information to Meta.

22. Meta, which created the Pixel and assigns a unique FID to each of its Facebook account holders, knows how to combine the information intercepted and

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

disclosed by Defendant so that Meta can connect each User to the PHI that is disclosed. Meta does this in order to send targeted ads related to the medical conditions and treatments each User shares with Defendant to that User's personal Facebook account.

23. The Pixel intercepts and discloses the information of every Facebook user that visits the Defendant's Web Properties in the same way. So, when Plaintiffs and Class Members visited Defendant's Web Properties, the URLs that describe the medical information on each page they visited (for example: https://eisenhowerhealth.org/ services/oncology/services/breast-center/), and/or the search terms they typed in Defendant's search bar, were simultaneously shared with Meta during every interaction. And together with that PHI, Defendant's Pixel (which relies on Facebook cookies to function) disclosed to Meta the Facebook user ID of every person that visited its Web Properties which allowed Meta to personally identify that user – including Plaintiffs and every Class Member who visited Defendant's Web Properties to research and share HIPAA-protected health information with Defendant while the Pixel was installed on the Web Properties.

24. Plaintiffs and Class Members who visited and used Defendant's Web Properties 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 locate and make an appointment with 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), extremely sensitive PHI such as health conditions (*e.g.*, breast cancer), diagnoses (*e.g.*, stroke, arthritis, COVID-19 or AIDS), procedures sought, treatment status, and/or the names and locations of their personal and other treating physicians, or even their access/interactions on Defendant's online Portal would be intercepted, captured and

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

otherwise shared with Facebook in order to target Plaintiffs and Class Members with ads, in conscious disregard of their privacy rights.

25. Plaintiffs 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.

26. Defendant knew that by embedding the Meta Pixel on its Web Properties it was enabling Facebook to collect and use Plaintiffs' and Class Members' Private Information, including sensitive medical information.

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

28. 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 state that any personal information provided to Defendant will remain secure and protected.[8]

29. 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 unauthorized third parties.

30. Plaintiffs seek, on behalf of themselves and a class of similarly situated

[8] Eisenhower'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 Apr. 19, 2024).

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

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 the California Invasion of Privacy Act ("**CIPA**"), Cal. Penal Code § 630, *et seq.*; (iv) Violation of California's Unfair Competition Law ("**UCL**"), Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful and Unfair Business Practices; (v) Invasion of Privacy under the California Constitution; (vi) Common Law Invasion of Privacy; (vii) Violation of California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.*; (viii) Violation of California Penal Code § 496, *et seq.*; (ix) Common Law Breach of Confidence, (x) Common Law Breach of Fiduciary Duty; and (xi) Common Law Unjust Enrichment.

II. PARTIES

31. Plaintiff B.K. was a California resident at all relevant times, residing in Riverside County, California.

32. Plaintiff N.Z. is and at all relevant times was, a California resident, residing in Riverside County, California.

33. 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.[9]

III. JURISDICTION & VENUE

34. 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

[9] *Contact Us,* EISENHOWER HEALTH, https://eisenhowerhealth.org/giving/ways-to-give/campaign/contact-us/ (last visited Apr. 19, 2024.

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

significant portion of putative class members are citizens of a state different from the citizenship of at least one Defendant.

35. 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.

36. 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.

IV. REPRESENTATIVE PLAINTIFFS' EXPERIENCES

Plaintiff B.K.

37. Plaintiff B.K has been a patient of Defendant since October 2017 and has utilized Defendant's Web Properties since late 2017.

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

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

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

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

41. During the relevant time period (when the Defendant's Pixels were present) Plaintiff B.K. used Defendant's Website, https://www.eisenhowerhealth.org/, to research orthopedic specialists and treatments for her knee pain (and later for her diagnosis of osteoarthritis); look up COVID-19 symptoms, testing and treatments; and look for Defendant's locations close to her address including Defendant's orthopedic center, emergency departments, and COVID testing locations.

42. After beginning to experience knee pain, in or around May 22 and May 24, 2018, Plaintiff B.K. used Defendant's Website to research causes of knee pain; knee arthritis; potential treatments including steroid injections, knee replacements and non-surgical treatments for knee pain; and to look up specific orthopedic surgeons.[10]

43. After seeing two of Defendant's orthopedic specialists in May 2018, Plaintiff B.K. was diagnosed with a specific medical condition (osteoarthritis in her knee) and submitted information to Defendant's Website and Portal about her condition and treatments received such as cortisone injections.

44. Shortly after submitting her protected health information including information concerning her knee pain, knee arthritis, and need for knee pain treatments to Defendant, Plaintiff B.K. began to receive spam and ads on Facebook and other social media related to her specific medical condition, such as ads for titanium knee replacements and knee gel injections, as well as ads for various Eisenhower events and promotions.

45. Upon information and good faith belief, Plaintiff B.K. began receiving these ads after her PII and PHI concerning her knee pain was disclosed by Defendant through the Pixel to Meta. Meta then viewed or otherwise improperly accessed this Private Information so that it could personally identify Plaintiff B.K. by connecting

[10] Defendant's Website has a "Find a Provider" section where you can find doctors based on their last name and/or specialty, gender, location, and language. *See* https://eisenhowerhealth.org/provider/.

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

her c_user FID to her Facebook account. Meta also accesses the PHI disclosed by Defendant so that it can use the specific medical information Plaintiff B.K. shared with Defendant including the specialty and location of her treating physicians to identify specific targeted ads related to Plaintiff B.K.'s medical conditions and perceived medical needs to send to her Facebook account. After accessing and identifying the specific medical conditions and other protected health information it can target with ads, Meta then shares that information with *additional* unauthorized third parties whose businesses and advertisements are related to those conditions.

46. In July 2020 Plaintiff B.K. felt sick with what she believed to be COVID-19. As part of her seeking healthcare from Defendant, she utilized the Website to research COVID-19 symptoms and whether, if she was experiencing severe symptoms, she needed to go to the hospital and/or the emergency care. On July 9, 2020, Plaintiff B.K. went to Defendant's ER and was diagnosed with COVID-19.

47. After submitting her Private Information to Defendant, Plaintiff B.K. began to receive spam and ads on Facebook and other social media related to her COVID-19 symptoms and diagnosis including numerous ads for COVID-19 treatments and the importance of wearing a mask/washing hands. Plaintiff B.K. did not know how an entity such as Facebook would know this information. Plaintiff B.K. felt embarrassed and uncomfortable that Facebook now knew about her diagnosis – the information that only a doctor and close family members were supposed to know, not Facebook. Plaintiff B.K. could not have imagined at that time that Defendant, working with Facebook, shared this sensitive information related to Plaintiff B.K.'s diagnosis.

48. Only several years later did Plaintiff B.K. learn that Defendant shared this sensitive information with Facebook (and other entities) to exploit her medical conditions for financial gain. Plaintiff B.K. was shocked that Facebook was now using B.K.'s sensitive information – her illness – for profits by targeting Plaintiff B.K. based on her medical diagnosis. Plaintiff B.K had placed her trust in Defendant – her

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

medical provider – who had the duty to protect all her information from any third party and treat *all* communications with B.K as confidential. She felt disappointed, embarrassed, and violated from Defendant's betrayal of her trust and troubled that her medical conditions, symptoms, and treatment decisions were at the mercy of a social media conglomerate and its employees.

49. Upon information and good faith belief, Plaintiff B.K. began receiving these ads after her PII and PHI concerning her COVID-19 status was disclosed by Defendant's Pixel to Facebook, which accessed and analyzed that information to identify Plaintiff B.K.'s Facebook account and determine which advertisements would most effectively target her medical condition, in this case her COVID-19 status. Facebook in turn shared the information with other unauthorized third parties so that they could determine if their ads would effectively target that condition.

50. The full scope of Defendant's interceptions and disclosures of Plaintiff B.K.'s communications to Meta can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiff B.K.'s patient status, medical knee condition, treatments sought, and prospective specialized healthcare providers, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixel (and which contain information concerning Plaintiff B.K.'s specific medical conditions, queries, as well as types of providers and treatments sought):

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

- https://eisenhowerhealth.org/services/orthopedics/conditions/knee-pain-and-injury/
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Pain
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Arthritis
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Injections
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Replacement
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Gel
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Pain%20Non-Surgical%20Treatments
- https://eisenhowerhealth.org/services/orthopedics/
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Osteoarthritis
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=COVID%20symptoms
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Do%20I%20Have%20Covid
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Do%20I%20Have%20To%20Go%20To%20ER%20If%20I%20Have%20Covid

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

51. Contemporaneously with the interception and transmission of the contents of Plaintiff B.K.'s communications regarding her knee condition on https://www.eisenhowerhealth.org/, Defendant also disclosed to Meta Plaintiff B.K.'s unique personal identifiers, including but not limited to, her Facebook ID and IP address.

52. During the relevant time period, when the Defendant's Pixels were present, Plaintiff B.K. also utilized Defendant's Patient Portal to review her medical records such as her visit summaries with her personal and other treating physicians, doctor's notes, and her test results.

53. The full scope of Defendant's interceptions and disclosures of Plaintiff B.K.'s communications to Meta can only be determined through formal discovery. However, upon information and good faith belief, Defendant intercepted at least the following communications about Plaintiff B.K.'s patient status, via the following URLs or substantially similar URLs were sent to Meta via the Pixel, indicating that Plaintiff B.K. is a patient of Defendant who is about to use her patient portal:

- https://mychart.eisenhowerhealth.org/mychart/Authentication/Login?
- https://eisenhowerhealth.org/resources/mychart/

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

55. Plaintiff B.K. provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

56. As described herein, Defendant worked along with Facebook to intercept Plaintiff B.K.'s communications, including those that contained her Private Information.

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

57. Defendant willfully facilitated these interceptions without Plaintiff B.K.'s knowledge, consent, or express written authorization.

58. Defendant transmitted to Facebook Plaintiff B.K.'s Facebook ID, computer IP address and sensitive health information such as her medical symptoms, conditions, treatments sought, specialty and location of physicians selected, button/menu selections and/or content typed into free text boxes.

59. By doing so without his consent, Defendant breached Plaintiff B.K.'s privacy and unlawfully disclosed her Private Information.

60. Defendant did not inform Plaintiff B.K. that it had shared her Private Information with Facebook.

61. Plaintiff B.K. would not have paid (or would have paid substantially less) for Defendant's services, including her visits to Defendant's providers, tests and treatments sought, had she known that her PHI was being disclosed to unauthorized third parties like Facebook.

Plaintiff N.Z.

62. Plaintiff N.Z. has been a patient of Defendant since 2016 and has utilized Defendant's Web Properties since late 2016.

63. As a condition of receiving Defendant's services, Plaintiff N.Z. disclosed her Private Information to Defendant on numerous occasions, and most recently in the summer of 2021.

64. Plaintiff N.Z. accessed Defendant's Website and Patient Portal on her phone, computer, and tablet to receive healthcare services from Defendant and at Defendant's direction.

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

66. During the relevant time period, when the Defendant's Pixels were present, Plaintiff N.Z. used Defendant's Website, https://www.eisenhowerhealth.org/, to research providers including primary doctors

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

at Defendant's La Quinta family clinic (starting in 2021) and gastroenterologists (including Dr. Gary Annunziata in or around 2018 and Dr. Ajumobi in 2020-2021); specific conditions (such as suspicious breast mass, colon polyps, hemorrhoids and rectal bleeding) and test results for these conditions (at least once a year as well as when Plaintiff N.Z. was getting respective tests done); treatments including further breast testing via repeated mammograms (starting in 2019 when a suspicious lump was discovered in her left breast), surgical removal of hemorrhoids (starting in 2019), colonoscopies due to colon polyps (starting in 2019), and treatments for bleeding hemorrhoids (starting in 2019 and prior to her colonoscopies); and to look for Defendant's locations close to her address around La Quinta.

67. After submitting her Private Information to Defendant, Plaintiff N.Z. began to receive spam and ads on Facebook and other social media related to her medical conditions and treatments, including but not limited to targeted ads or medical studies on breast cancer. Plaintiff N.Z. was shocked and alarmed that she was being targeted with these ads, and confused how would Facebook know such sensitive information. It did not occur to Plaintiff N.Z. nor could she have ever imagined that her medical provider – the entity that has Plaintiff N.Z.'s most private and sensitive medical information - could disclose/share such information with Facebook and use it for commercial purposes and profits.

68. Only years later did Plaintiff N.Z. learn that Defendant shared her medical conditions, symptoms, and treatment with Facebook (and other entities), to exploit Plaintiff N.Z.'s medical condition by social media giant and Defendant for their financial gain. Plaintiff N.Z. had placed her utmost trust in the Defendant – her medical provider, who is supposed to protect all of the medical information from any other third party and treat *every* communication with N.Z. as confidential. She felt embarrassed, frustrated, and violated from Defendant's betrayal of her trust, and devastated that her medical conditions, symptoms, and treatment were now at the hands of the social media giant and thousands of its employees.

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

69. Plaintiff N.Z. began receiving these ads after her PII and PHI concerning her suspicious breast lump (and subsequent repeated mammograms) was disclosed by Defendant through the Pixel to Meta. Meta then viewed or otherwise improperly accessed this Private Information so that it could personally identify Plaintiff N.Z. by connecting her c_user FID to her Facebook account. Meta also accessed the PHI disclosed by Defendant so that it can use the specific medical information Plaintiff N.Z. shared with Defendant including the specialty and location of her treating physicians to identify specific targeted ads related to Plaintiff N.Z.'s medical conditions and perceived medical needs to send to her Facebook account. After accessing and identifying the specific medical conditions and other protected health information it can target with ads, Meta then shares that information with *additional* unauthorized third parties whose businesses and advertisements are related to those conditions.

70. The full scope of Defendant's interceptions and disclosures of Plaintiff N.Z.'s communications to Meta can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiff N.Z.'s medical conditions and current and prospective healthcare providers. The following long-URLs or substantially similar URLs were sent to Meta via the Pixel:

- https://eisenhowerhealth.org/services/oncology/
- https://eisenhowerhealth.org/services/oncology/services/breast-center/

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

- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Colonoscopy%20Colon%20Polyps
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Excessive%20GI%20Bleeding
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Hemorrhoids%20Bleeding
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=How%20Much%20Blood%20Can%20I%20Lose
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Hemorrhoids%20Surgery

///

///

///

///

///

///

///

///

///

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

- https://eisenhowerhealth.org/services/oncology/services/breast-center/diagnosis/
- https://eisenhowerhealth.org/services/oncology/services/breast-center/mammography/
- https://eisenhowerhealth.org/services/digestive/
- https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-screening/
- https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-screening/colorectal-cancer-screening/
- https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-screening/colorectal-cancer-screening/colonoscopy-and-prep-instructions/
- https://eisenhowerhealth.org/services/digestive/faq/
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Suspiscious%20Breast%20Mass
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Suspiscious%20Breast%20Cancer
- https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Colon%20Polyps

71. Contemporaneously with the interception and transmission of Plaintiff N.Z.'s communications on https://www.eisenhowerhealth.org/, Defendant also

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

disclosed to Meta Plaintiff N.Z.'s personal identifiers, including but not limited to her IP address and Facebook ID.

72. During the relevant time period, when the Defendant's Pixels were present, Plaintiff N.Z. also utilized Defendant's Patient Portal to review her medical records including test results for her mammograms, blood work, colonoscopies, as well as to view her bills and payments.

73. The full scope of Defendant's interceptions and disclosures of Plaintiff N.Z.'s communications to Meta can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiff N.Z.'s prospective healthcare providers. The following long-URLs or substantially similar URLs were sent to Meta via the Pixel:

- https://mychart.eisenhowerhealth.org/mychart/Authentication/Login?
- https://eisenhowerhealth.org/resources/mychart/

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

75. Plaintiff N.Z. provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

76. Plaintiff N.Z. is diagnosed with specific medical conditions including a suspicious breast mass, colon polyps and hemorrhoids, and submitted information related to these medical conditions, symptoms, and treatment to Defendant's Website and Portal.

77. As described herein, Defendant enabled Facebook to intercept Plaintiff N.Z.'s communications, including those that contained her Private Information about her medical conditions, symptoms, and treatment.

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

78. Defendant willfully facilitated these interceptions without Plaintiff N.Z.'s knowledge, consent, or express written authorization.

79. Defendant transmitted to Facebook Plaintiff N.Z.'s Facebook ID, computer IP address and information such as patient status, medical conditions, treatments, and physicians sought, button/menu selections and/or content typed into free text boxes.

80. By doing so without her consent, Defendant breached Plaintiff N.Z.'s privacy and unlawfully disclosed her Private Information.

81. Defendant did not inform Plaintiff N.Z. that it had shared her Private Information with Facebook and did not obtain her express consent for this disclosure.

82. Plaintiff N.Z. would not have paid (or would have paid substantially less) for Defendant's services, including her visits to Defendant's providers, tests and treatments sought, had she known that her PHI was being disclosed to unauthorized third parties like Facebook.

83. The technical details of how Defendant utilized Meta's invisible tracking technology to capture and unlawfully disclose Plaintiffs' and Class Members' Private Information are discussed more fully below.

V. FACTUAL BACKGROUND

A. The Problematic Use of Invisible Tracking Codes to Collect People's Data for its Advertising Business.

84. Meta operates the world's largest social media company whose revenue is derived almost entirely from selling targeted advertising.

85. The Meta Pixel and other third-party tracking tools also collect and transmit information from Defendant that identifies a Facebook user's status as a patient and other health information that is protected by federal and state law. This occurs through tools that Facebook encourages its healthcare Partners to use, including uploading patient lists to Facebook for use in its advertising systems.

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

86. Meta associates the information it obtains via the Meta Pixel with other information regarding the User, using personal identifiers that are transmitted concurrently with other information the Pixel is configured to collect. For Facebook account holders, these identifiers include the "c_user" cookie IDs, which allow Meta to link data to a particular Facebook account. For both Facebook account holders and users who do not have a Facebook account, these identifiers also include cookies that Meta ties to their browser.

87. 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."[11]

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

89. 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.'"[12]

90. The Meta Pixel is a free and publicly available "piece of code" that third-party web developers can install on their website to "measure, optimize and build audiences for … ad campaigns."[13]

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

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

[13] *Meta Pixel*, META, https://www.facebook.com/business/tools/meta-pixel (last visited Apr. 19, 2024).

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

91. Meta describes the Pixel as "a snippet of Javascript code" that "relies on Facebook cookies, which enable [Facebook] to match … website visitors to their respective Facebook User accounts.[14]

92. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel "can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart."[15]

93. Meta tells advertisers that the Meta Pixel will improve their Facebook advertising, including by allowing them to:

A. "Optimize the delivery of your ads" and "[e]nsure your ads reach the people most likely to take action;" and

B. "Create Custom Audiences from website visitors" and create "[d]ynamic ads [to] help you automatically show website visitors the products they viewed on your website—or related ones."[16]

94. Meta explains that the Pixel "log[s] when someone takes an action on your website" such as "adding an item to their shopping cart or making a purchase," and the user's subsequent action:

[14] *Meta Pixel*, META, https://developers.facebook.com/docs/meta-pixel/ (last visited Apr. 19, 2024).

[15] *Meta Pixel*, META, https://www.facebook.com/business/tools/meta-pixel (last visited Apr. 19, 2024).

[16] *Id.*

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

Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

options to reach those customers again through future Facebook ads.

95. The Meta Pixel is customizable and web developers can choose the actions the Pixel will track and measure on a particular webpage.

96. Meta advises web developers to place the Pixel early in the source code[17] for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website.[18]

97. Meta's "Health" division is dedicated to marketing to and servicing Meta's healthcare "Partners." Meta defines its "Partners" to include businesses that use Meta's products, including the Meta Pixel or Meta Audience Network tools to advertise, market, or support their products and services.

---

[17] Source code is a collection of instructions (readable by humans) that programmers write using computer programming languages such as JavaScript, PHP, and Python. When the programmer writes a set or line of source code, it is implemented into an application, website, or another computer program. Then, that code can provide instructions to the website on how to function. *What is Source Code & Why Is It Important?* (July 19, 2023), https://blog.hubspot.com/website/what-is-source-code (last visited Mar. 13, 2024).

[18] *Meta Pixel: Get Started*, META (2023), *https://developers.facebook.com/docs/meta- pixel/get-started* (last visited Apr. 19, 2024).

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

98. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

99. Healthcare providers like Defendant encourage 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.

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

101. Upon information and belief, Defendant and other companies utilized Plaintiffs' and Class Members' sensitive information and data collected by the Meta Pixels on Defendant's Web Properties in order to advertise to these individuals later on Meta's social platforms.

102. If a healthcare provider, such as Defendant, installs the Meta Pixel code as Meta recommends, patients' actions on the provider's website are contemporaneously redirected to Meta. For example, when a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Meta's source code commands the patient's computing device to send the content of the patient's communication to Meta while the patient is communicating with her healthcare provider. In other words, by design, Meta receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the healthcare provider receives it.

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

103. Thus, the Meta "pixel allows Facebook to be a silent third-party watching whatever you're doing,"[19] which in this case included the content of Defendant's patients' communications with its Web Properties, including their PHI.

104. 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, via data packets labeled with PII, including the User's IP address, the Facebook c_user cookie and third-party cookies allowing Facebook to link the data collected by Meta Pixel to the specific Facebook user.[20]

105. A recent investigation by THE MARKUP revealed that the Meta Pixel was installed inside password-protected patient portals of at least seven U.S. health systems, giving Facebook access to even more patient communications with their providers.[21]

106. 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.[22]

107. Facebook's access to use even only some of these data points—such as just a "descriptive" webpage URL—is problematic. As Laura Lazaro Cabrera, a legal officer at Privacy International, explained: "Think about what you can learn from a URL that says something about scheduling an abortion' . . . 'Facebook is in the

[19] Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows everything*, USA TODAY (Mar. 4, 2020), https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/.

[20] The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users. *See* Maciej Zawadziński & Michal Wlosik, *What Facebook's First-Party Cookie Means for AdTech,* CLEARCODE (Jan. 31, 2024), https://clearcode.cc/blog/facebook-first-party-cookie-adtech/.

[21] *See* Feathers, *et al*., *supra* note 4.

[22] *Id.*

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

business of developing algorithms. They know what sorts of information can act as a proxy for personal data."[23]

108. The collection and use of this data raises serious concerns about user privacy and the potential misuse of personal information. For example, when Users browse Defendant's Web Properties, every step of their activity is tracked and monitored, including the specialties and locations of treating and other selected physicians. By analyzing this data using algorithms and machine learning techniques, Facebook (and other entities tracking this information) can learn a chilling level of detail about Users' medical conditions, behavioral patterns, preferences, and interests.

109. This data can be used not only to provide personalized and targeted content and advertising, but also for more nefarious purposes, such as tracking and surveillance. 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.

110. As pointed out by the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS), 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."[24] As anticipated by the OCR and HHS, Plaintiffs here, as a result of Defendant's impermissible disclosure of

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

[24] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* U.S. DEP'T OF HEALTH AND HUMAN SERVICES (Mar. 18, 2024) https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

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

their medical information resulted in mental anguish, stigma, embarrassment, as well as distrust of their healthcare providers.

111. Unfortunately, several recent reports detail the widespread use of third-party tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to surreptitiously capture and to disclose their Users' Private Information.[25] Estimates are that over 664 hospital systems and providers utilize some form of tracking technology on their digital properties.[26]

B. *Defendant Disclosed Patient Healthcare Information, Including Patient Status, in Violation of the HIPAA Privacy Rule.*

112. Healthcare 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.[27]

113. The HIPAA Privacy Rule sets forth policies to protect all individually identifiable health information ("**IIHI**") that is held or transmitted.[28] 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.

114. Plaintiffs' IIHI captured by the Pixel and sent to Meta included their unique personal identifiers such as their Facebook ID, IP address, device identifiers and browser "fingerprints."

---

[25] 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. Todd Feathers, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, *supra*, note 6.

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

[27] *The HIPAA Privacy Rule*, U.S DEP'T OF HEALTH AND HUMAN SERVICES (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[28] The HIPAA Privacy Rule protects all electronically protected health information a covered entity like Defendant "created, received, maintained, or transmitted" in electronic form. *See* 45 C.F.R. § 160.103.

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

115. Defendant further violated the HIPAA Privacy Rule, among other statutory and common laws, because Plaintiffs' PHI including their specific medical conditions (such as Plaintiff B.K.'s knee pain and/or knee osteoarthritis, Plaintiff's N.Z.'s irregular mammograms, polyps and hemorrhoids, and her husband's heart stroke, lipodermatosclerosis, and diabetes) was disclosed to Meta by the Pixel and other third-party trackers embedded by Defendant on its Web Properties.

116. HIPAA also protects against revealing an individual's status as a patient of a healthcare provider.[29] Thus, by purposely disclosing Plaintiffs' activities on the Web Properties and the specialties and locations of Plaintiffs' treating and other selected physicians to Meta, Defendant further violated the HIPAA Privacy Rule.

117. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

118. Defendant unlawfully revealed Plaintiffs' and Class Members' patient status to Facebook and likely other unauthorized third parties in violation of HIPAA when the Meta Pixel captured and disclosed Plaintiffs' and Class Members' activity on patient-dedicated webpages of the Web Properties, such as Patient Financial Services, Patient Education Resources, Schedule an Appointment, and the Patient Portal.

///

///

[29] *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 HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Apr. 19, 2024).

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

C. *HIPAA's Protections Do Not Exclude Internet Marketing.*

119. As the OCR reminded entities regulated under HIPAA (like Defendant) 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.***[30]

120. The OCR makes it clear that information that is routinely collected by vendors on public-facing websites may be PHI, including unique identifiers such as IP addresses, device IDs, or email addresses.[31]

121. HHS has also confirmed that healthcare providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the healthcare provider:

> This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.* it is indicative that the individual has received or will receive healthcare services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or healthcare or payment for care.[32]

122. Further, HIPAA applies to healthcare providers' webpages with tracking technologies even outside the patient portal, i.e. to "unauthenticated" webpages:

> [T]racking technologies on unauthenticated webpages may access to PHI, in which case the HIPAA Rules apply to the

[30] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, supra*, note 27 (emphasis added) (updated Mar.18, 2024) (last visited Apr. 19, 2024).

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

[32] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, supra*, note 27 (updated Mar.18, 2024) (last visited Apr. 19, 2024) .

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

> regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal … [and ***pages] that address[] specific symptoms or health conditions***, such as pregnancy or miscarriage, ***or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances***. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a healthcare provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.

123. **The HHS bulletin reminds covered entities, like Defendant, of its long-standing duty to safeguard PHI**, explicitly noting that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," and proceeding to explain how online tracking technologies violate the same HIPAA privacy rules that have existed for decades.[33]

124. Disclosures of PHI for online marketing or sales purposes require patient authorization under HIPAA, which Defendant did not obtain here. *See* 45 CFR § 164.508(a)(3) ("a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of: (A) a face-to-face communication made by a covered entity to an individual; or (B) a promotional gift of nominal value provided by the covered entity."); 45 CFR § 164.508(a)(4) ("a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart [and] [s]uch authorization must state that the disclosure will result in remuneration to the covered entity.").

125. As a result, a healthcare provider like Defendant may not disclose PHI to a tracking technology vendor, like Meta, unless it has properly notified its Website Users and entered into a business associate agreement with the vendor in question.

[33] *Id.* (emphasis added).

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

126. Despite this clear guidance, Defendant disclosed Plaintiffs' and Class Members' PHI without their consent and without a business associate agreement with Meta anyway.

D. *The Industry was Warned of Third-Party Tracking Tools Resulting in HIPAA Violations, but Defendant Elected to Continue Their Illicit Sharing Anyway.*

127. Recognizing the distinct privacy dangers third party tracking tools present, the Federal Trade Commission ("**FTC**") joined HHS in warning HIPAA-covered entities and non-HIPAA covered entities alike that unauthorized disclosure of sensitive health information is through online tracking technology must be prevented.[34]

128. According to the FTC, "health information" is "anything that conveys information – or enables an inference – about a consumer's health" and provides an example that location-data alone (such as "repeated trips to a cancer treatment facility") "may convey highly sensitive information about a consumer's health."[35]

129. The FTC and HHS explicitly warned the industry and healthcare providers like Defendant that transmitting "health information" to Google and Facebook via third party tracking tools is an unfair business practice:

> "When consumers visit a hospital's website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing

[34] *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, FEDERAL TRADE COMMISSION (Jul. 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

[35] Elisa Jillson, *A baker's dozen takeaways from FTC cases*, FEDERAL TRADE COMMISSION (Jul. 25, 2023), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases.

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

> everything in our powers to protect consumers' health information from potential misuse and exploitation."[36]

130. Indeed, this decree by the FTC responds to real consumer concern for the privacy of their medical information. A recent national study from CVS Health revealed that nearly 90% of people found data security and privacy (e.g., keeping private health information confidential) among the most important factors concerning health care.[37]

131. This underscores the severity of Defendant's use of tracking technology like the "Meta/Facebook pixel" that, as the FTC alerts, "gather[s] identifiable information about users, [] without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app."[38]

132. The FTC and HHS warning to the healthcare industry highlights the "[r]ecent research,[39] news reports,[40] FTC enforcement actions,[41] and [] OCR

---

[36] *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, supra,* note 40.

[37] *The 2021 Health Care Insights Study*, CVS HEALTH (2021), https://www.cvshealth.com/content/dam/enterprise/cvs-enterprise/pdfs/2021/cvs-health-health-care-insights-study-2021-report-executive-summary.pdf (last visited Apr. 19, 2024).

[38] *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, supra,* note 40.

[39] Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, ASSOCIATION FOR COMPUTING MACHINERY (Nov. 7, 2022), https://dl.acm.org/doi/10.1145/3559613.3563190.

[40] *See, e.g.*, Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.

[41] *U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; In the Matter of BetterHelp, Inc., FTC Dkt. No. C-4796 (Jul. 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169- betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case

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

bulletin[42]" concerning the privacy risks resulting from the use of tracking technologies like Meta Pixel.

133. The industry wide warning delineates that these privacy risks are the very privacy violations that HIPAA Privacy Rules are designed to protect against:

> "If you are a covered entity or business associate ("regulated entities") under HIPAA, you **must** comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium.
>
> The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI. **HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules**. OCR's December 2022 bulletin about the use of online tracking technologies by HIPAA regulated entities provides a general overview of how the HIPAA Rules apply.[] This bulletin discusses what tracking technologies are and reminds regulated entities of their obligations to comply with the HIPAA Rules when using tracking technologies."[43]

134. As HIPAA regulated entity, Defendant was required to comply with HIPAA Privacy Rules and heed this warning. However, Defendant chose to continue siphoning Plaintiffs' and Class Members' PHI, in knowing violation of HIPAA and the wealth of regulatory guidance, and in conscious disregard of clear federal warnings and consumer concern.

135. Defendant's purposeful violation of HIPAA despite clear warnings is emblematic of systemic privacy issues at Eisenhower medical facilities in particular. ProPublica even identified Defendant as the #1 hospital-culprit in California with the

---

No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; In the Matter of Flo Health Inc., FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

[42] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, supra*, note 27 (updated March 18, 2024) (last visited Apr. 19, 2024).

[43] *Model Letter: Use of Online Tracking Technologies*, FEDERAL TRADE COMMISSION (Jul. 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.

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

most privacy-related deficiencies from 2012 to 2015—riddled with HIPAA violations and unauthorized disclosures of PHI.[44]

E. *Defendant Transmitted a Broad Spectrum of Plaintiffs' & Class Members' Identifiable Health Information to Meta via the Meta Tracking Tools.*

136. Every website is comprised of "Markup" and "Source Code." Markup consists of the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Web Properties.

137. 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. Source Code is designed to be readable by humans and formatted in a way that developers and other users can understand.

138. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions including the ability to command a website user's browser to send data transmissions to third parties like Facebook, via the Meta Pixel.[45]

139. Defendant's Pixel, embedded in its JavaScript Source Code on the Web Properties, manipulates a User's browser by secretly instructing it to duplicate a User's communications (HTTP Requests) and sending those communications to Facebook.

140. This occurs because the Pixel is programmed to automatically track and transmit Users' communications, and this occurs contemporaneously, invisibly, and without the Users' knowledge.

---

[44] Charles Ornstein, *The Consequences for Violating Patient Privacy in California? Depends Where the Hospital Is*, PROPUBLICA (Dec. 31, 2015), https://www.propublica.org/article/california-patient-privacy-law-inconsistent-enforcement.

[45] 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

141. Eisenhower's Source Code essentially commands a patient's browser to re-direct their actions on the Web Properties (characterized as "Event Data" by the Pixel), which contain PHI, through the HTTPS protocol to Meta at a Meta "endpoint," *i.e.*, a URL at a domain controlled by Meta that exists for the purpose of acquiring such information.

142. The information Eisenhower sends to Meta from its use of the Meta Pixel and other tracking tools includes, but is not limited to, the following:

a. The exact search terms entered by a User on the Website, including searches for the User's medical symptoms and conditions, specific medical providers and their specialty, and treatments sought;

b. descriptive URLs that describe the categories of the Website, categories that describe the current section of the Website, and the referrer URL that caused navigation to the current page;

c. the communications a User exchanges through Defendant's Web Properties by clicking and viewing webpages, including communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including, upon information and good faith belief, whether they are made while a User is still logged in to the Patient Portal or around the same time that the User has scheduled an appointment, called the medical provider, or logged in or out of the Patient Portal;

d. when a User sets up or schedules an appointment;

e. information that a User clicks on in an appointment form;

f. when a User clicks a button to call the provider from a mobile device directly from Defendant's Website;

g. when a User clicks to register for the Patient Portal, clicks to log into the Portal, and/or accesses other patient-dedicated web pages; and

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

h. the same or substantially similar communications that patients exchange with health insurance companies, pharmacies, and prescription drug companies.

143. Thus, Defendant is, in essence, handing patients a tapped device and once one of its webpages 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 unauthorized third parties such as Facebook.

144. For example, when a patient visits www.eisenhowerhealth.org and enters "heart disease," "diabetes" or "stroke rehabilitation" into the search bar, their browser automatically sends an HTTP request to Eisenhower's web server. Eisenhower's web server automatically returns an HTTP response, which loads the Markup for that particular webpage.

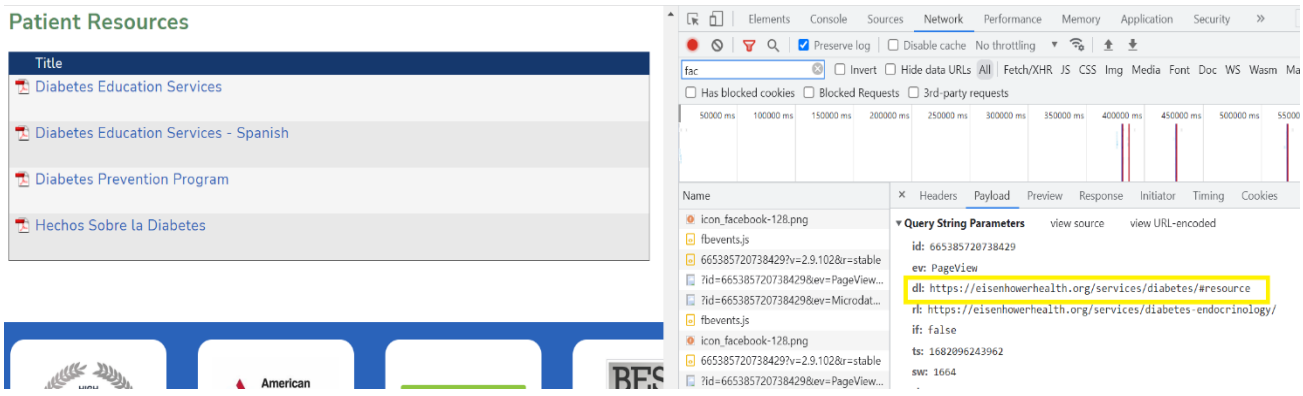
145. The patient visiting this particular web page only sees the Markup, not the Defendant's source code or underlying HTTP Requests and Responses.

146. In reality, Defendant's Source Code and underlying HTTP Requests and Responses share the patient's personal information with Facebook, including the fact that a User was looking for treatment for their heart disease, diabetes, or stroke diagnosis — along with the User's unique personal identifiers.

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

Figure 1: An example of a HTTP communication session sent by the Pixel from the User's device to Facebook that reveals the User's search for diabetes resources, along with the User's unique Facebook personal identifier (the c_user field).

Figure 2. An easier-to-read representation of a User's search for "diabetes" "resources" sent to Facebook when a User enters them into Defendant's search bar.



147. Since Plaintiffs brought this action, Defendant has removed the Meta Pixel from its Web Properties and has re-configured its source code.

148. However, because of the way Defendant's source code operated with the embedded Meta Pixel, when Plaintiff B.K. used the search bar on

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

https://www.eisenhowerhealth.org to look for medical treatments for her knee pain, her exact search terms (including "knee pain," "knee arthritis," "knee osteoarthritis," "knee injections, "knee replacement," and "non-surgical treatments for knee pain") were transmitted by Defendant's Pixel to Meta, disclosing her specific medical conditions.

149. Similarly, when Plaintiff N.Z. used the search bar on https://www.eisenhowerhealth.org to look up her medical conditions and potential treatments for it (including "suspicious breast mass," "colon polyps," "hemorrhoids and excessive bleeding," "colonoscopy and excessive bleeding," "abnormal mammogram") were transmitted by Defendant's Pixel to Meta, disclosing her specific medical conditions.

150. When Plaintiffs and Class Members clicked on Defendant's "Programs & Services" tab, it took them to the list of services offered by Defendant to Users in need of various medical treatments. On those pages the User can further narrow their search results by services offered by Defendant.

151. 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.

152. 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.[46]

[46] *Eisenhower Diabetes and Endocrinology Specialty Clinic,* EISENHOWER HEALTH, https://eisenhowerhealth.org/services/diabetes-endocrinology/ (last visited Apr. 19, 2024).

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

153. 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.

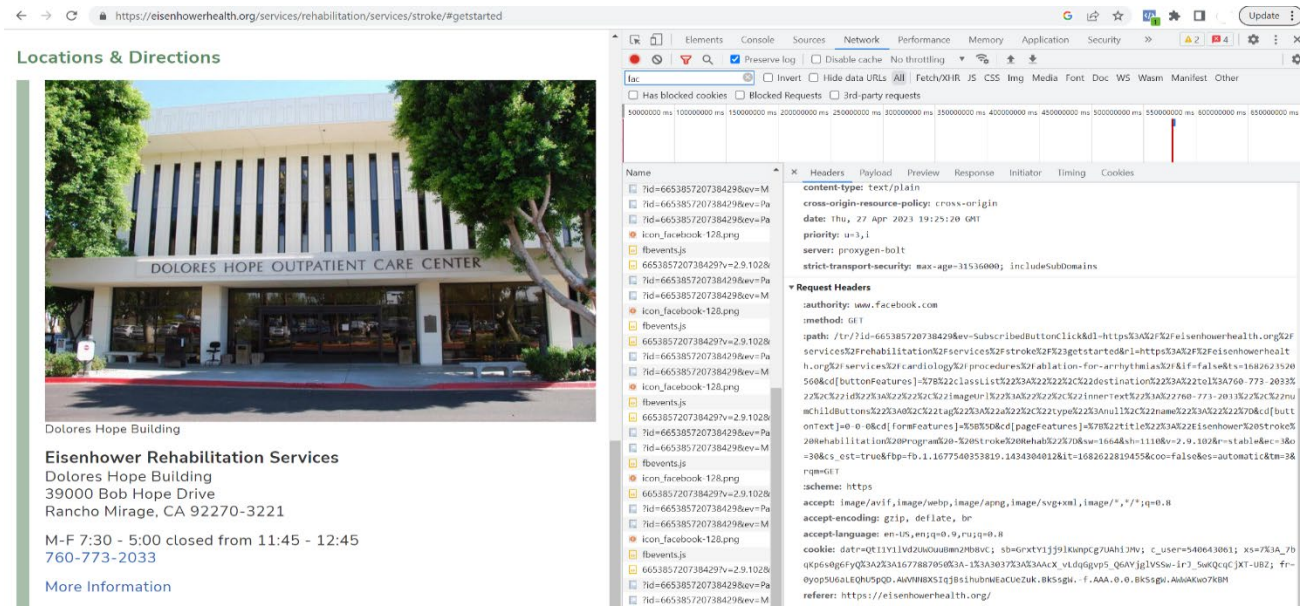
154. The transmission identifies the User as a patient: (i) seeking medical care from Defendant via www.eisenhowerhealth.org; (ii) who has diabetes; and (iii) who is searching for diabetes services.

155. Similarly, a patient who has experienced a stroke can search for post-stroke treatments, including rehabilitation services.

156. From the moment the patient begins searching for post-stroke treatment their selections or search parameters are automatically transmitted by the Pixel to Facebook along with the User's unique personal identifiers.

157. The transmission identifies the User as a patient: (i) seeking medical care from Defendant via www.eisenhowerhealth.org; (ii) who has had a stroke; and (iii) who is searching for stroke rehabilitation services.

158. If the patient chooses to click the phone number for Defendant's rehabilitation services center, that action is shared with Meta as well, via a "SubscribedButtonClick" event which captures the phone number of the clinic accessed by the patient, as evidenced by the images below in ***Figures 3 & 4***:



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

▼ 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%2Fgetstarted&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%2260-773-2033%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=54 ; 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/

159. As described above, if the patient selects other services, those search parameters are also automatically transmitted to Facebook by Defendant's Pixel, along with the patient's personal identifiers.

160. For example, after Plaintiff N.Z.'s mammogram revealed a suspicious mass in her breast in or around 2019, she looked up Defendant's breast imaging services at the Lucy Curci Cancer Center in order to schedule repeated mammograms.

161. This information would have been disclosed to Facebook (and likely other unauthorized third parties at least in the form of a descriptive URL, https://eisenhowerhealth.org/services/oncology/services/breast-center/, along with Plaintiff N.Z.'s unique personal identifiers including her Facebook ID and IP address.

162. Defendant would have also shared the fact that several times in the past five years Plaintiff N.Z. was looking up information on colorectal cancer screening tests and colonoscopy prep instructions.

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

163. For Plaintiff B.K., Defendant would have disclosed that starting in May 2018 she was looking up procedures to treat knee pain (including knee replacement), including but not limited to sharing the descriptive URL https://eisenhowerhealth.org/services/orthopedics/conditions/knee-pain-and-injury/#procedures that she visited on Defendant's Website.

F. *Defendant's Web Properties Sent Plaintiffs' and Class Members' PHI to Facebook Along with Unique Personal Identifiers.*

164. As described herein, Defendant's Meta Pixel (and other third-party trackers) 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 treatments or therapies; (iv) terms and phrases entered into Defendant's search bar; (v) the specialty and location of personal, treating, and other physicians and providers sought together with any medical specialties; (vi) selected locations or facilities for treatment; and (vii) web pages viewed.

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

166. Through the source code deployed by Defendant, the cookies that it uses to help Facebook identify patients include but are not necessarily limited to cookies named: "c_user," "datr," "fr," and "fbp."

167. 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

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

to quickly and easily locate, access, and view the User's corresponding Facebook profile.

168. 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.

169. The "fr" cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.[47] Facebook, at a minimum, uses the fr cookie to identify Users.[48]

170. At each stage, Defendant Eisenhower 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:[49]

171. The fr cookie expires after ninety (90) days unless the User's browser logs back into Facebook.[50] If that happens, the time resets, and another ninety (90) days begins to accrue.

172. The _fbp cookie expires after ninety (90) days unless the User's browser accesses the same website.[51] If that happens, the time resets, and another ninety (90) days begins to accrue.

173. The Facebook Meta Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—i.e., Defendant.[52]

[47] Gunes Acar et al., *Facebook Tracking Through Social Plug-ins*, BELGIAN PRIVACY COMMISSION, (Mar. 27, 2015), https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.
[48] *Cookies Policy*, META, https://www.facebook.com/policy/cookies/ (last visited Apr. 19, 2024).
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] This is confirmable by using developer tools to inspect a website's cookies and track network activity.

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

174. 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.[53]

175. 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.

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

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

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

179. 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.

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

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

181. 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.[54]

182. Further, Defendant represents to Users that it will only disclose Private Information provided to them under certain circumstances, ***none of which apply***

[53] This is confirmable by tracking network activity.

[54] *Privacy Policy*, EISENHOWER HEALTH, https://eisenhowerhealth.org/about/privacy/ (last visited Apr. 19, 2024).

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

here.[55] Defendant's privacy policies do ***not*** permit Defendant to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes.

183. 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."[56]

184. 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."[57]

185. 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."
>
> "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."[58]

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

187. Defendant acknowledges that, "We will not sell, trade or rent your personal information to other people or businesses unless we have your consent."[59]

188. 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

---

[55] *See id.*
[56] *See id.*
[57] *See id.*
[58] *Privacy Policy*, EISENHOWER HEALTH, https://eisenhowerhealth.org/about/privacy/ (last visited Apr. 19, 2024).
[59] *See id.*

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

sensitive and confidential communications, data, and Private Information with Facebook and other unauthorized third parties.[60]

189. 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 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.

190. 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.[61]

191. 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

[60] 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 (Oct. 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 (Aug. 19, 2022), https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html.

[61] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule, supra,* note 32.

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

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."[62] Defendant did not post such a notice, further underscoring the purposefulness of its HIPAA and other violations alleged.

192. 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."[63]

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

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

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

195. 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.

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

[62] *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).

[63] *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

197. 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.

198. 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.

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

199. Plaintiffs and Class Members did not realize that tracking Pixels exist because they are invisibly embedded within Defendant's web pages that users might interact with.[64] 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.

200. 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.

201. Defendant knew or should have known that Plaintiffs and Class Members would reasonably rely on and trust Defendant's promises regarding the tracking

[64] FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FEDERAL TRADE COMMISSION (Mar. 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

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.

202. 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.

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

204. 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.

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

205. 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 with personal, treating, and other physicians, typed specific medical queries into the search bar, and otherwise interacted with Defendant's Web Properties.

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

206. 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.[65] 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.

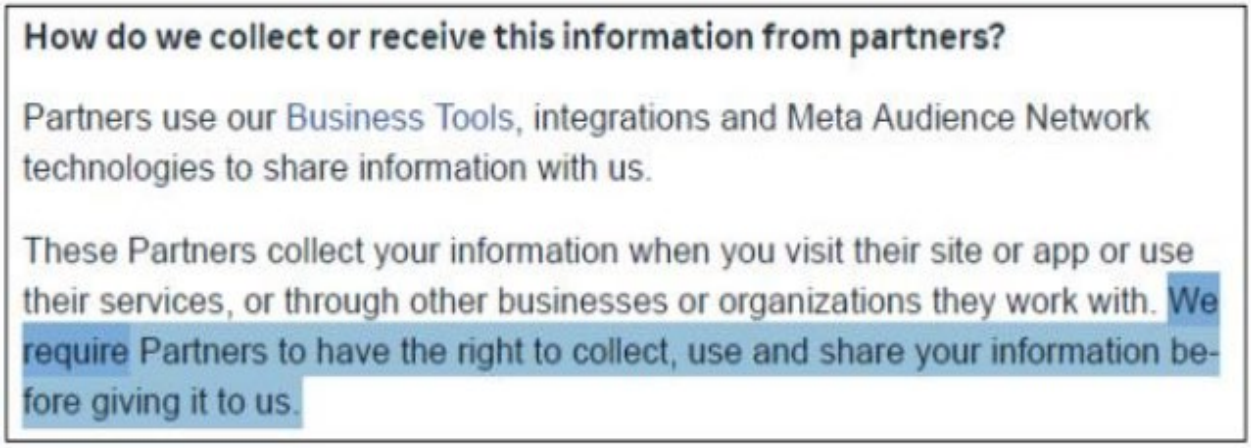
> **Information from partners.**
> Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities 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.

207. Meta changed this provision again in July 2022, while still requiring partners to have the right to share patient information with Meta:[66]

[65] *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)

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

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



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.

208. 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 and industry wide warnings that it was violating HIPAA.

209. 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, the industry wide warnings, 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.

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

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

211. HIPAA sets national standards for safeguarding protected health information. For example, HIPAA limits the permissible uses of health information

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

and prohibits the disclosure of this information without explicit authorization. *See* 45 C.F.R. § 164.HIPAA also requires that covered entities implement appropriate safeguards to protect this information. *See* 45 C.F.R. § 164.530(c)(1).

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

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

214. 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.

215. 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.

216. 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.[67] 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.[68]

[67] *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/.

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

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

217. 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.[69]

218. 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.[70]

219. 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.[71]

220. 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

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

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

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

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

about having a baby."[72] 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."[73]

221. Other privacy law experts have expressed concerns about the disclosure to third parties of a users' sensitive medical information. For example, Dena Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance and how much you pay for that coverage, increase the rate you are charged on loans, and leave you vulnerable to workplace discrimination.[74]

222. 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.

L. *Eisenhower Was Enriched & Benefitted from the Use of the Pixel & other Tracking Technologies that Enabled the Unauthorized Disclosures Alleged Herein.*

223. Meta advertises its' Pixel as a piece of code "that can help you better understand the ***effectiveness of your advertising*** and the actions people take on your

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

[73] *Id.*

[74] *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.

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

site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting. And when you use the Conversions API alongside the Pixel, it creates a more reliable connection that helps the delivery system ***decrease your costs***."[75]

224. Retargeting is a form of online marketing that targets Users with ads based on previous internet communications and interactions. Retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.[76]

225. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook via the tracking technologies and the Pixel embedded on, in this case, Defendant's Website.

226. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures, "includes URL names of pages visited, and actions taken - all of which could be potential examples of health information."[77]

227. In exchange for disclosing the Private Information of their patients, Eisenhower is compensated by Facebook and likely other third parties in the form of enhanced advertising services and more cost-efficient marketing on their platform.

[75] *What is the Meta Pixel?,* META, https://www.facebook.com/business/tools/meta-pixel (emphasis added) (last visited Apr. 19, 2024).
[76] Louis Meletiou, *The complex world of healthcare retargeting,* MEDICO DIGITAL (Jul. 10, 2023) https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/.
[77] *Id*.

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

228. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many are not HIPAA-complaint or are only HIPAA-compliant if certain steps are taken.[78]

229. For example, Freshpaint a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant", and "If you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[79]

230. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[80]

231. Thus, utilizing the Pixels directly benefits Eisenhower by, among other things, reducing the cost of advertising and retargeting.

M. *Plaintiffs' & Class Members' Private Information Has Substantial Value.*

232. Plaintiffs' and Class Members' Private Information had value, and Defendant's disclosure and interception harmed Plaintiffs and the Class by not compensating them for the value of their Private Information and in turn decreasing the value of their Private Information.

233. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

---

[78] *The guide to HIPAA compliance in analytics,* PIWIK PRO, https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Apr. 19, 2024).

[79] *Id*.

[80] *The complex world of healthcare retargeting, supra*, note 76.

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

234. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[81] A 2015 article from TechCrunch accurately noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[82] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

235. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

236. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[83]

237. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

238. In 2023, the Value Examiner published a report that focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned

[81] *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[82] Pauline Glikman and Nicolas Glady, *What's The Value Of Your Data*?, TECHCRUNCH (Oct. 13, 2015) https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.

[83] Kevin Mercadante, *10 Apps for Selling Your Data for Cash*, BEST WALLET HACKS (Nov. 18, 2023), https://wallethacks.com/apps-for-selling-your-data/.

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

providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[84]

239. In 2021, Trustwave Global Security published a report entitled *Hackers, breaches, and the value of healthcare data*. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[85]

240. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "*How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[86]

241. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[87]

242. The dramatic difference in the price of healthcare data when compared to other forms of private information that is commonly sold is evidence of the value of PHI.

---

[84] Todd Zigrang & Jessica Bailey-Wheaton, *Valuing Healthcare Data*, HEALTH CAPITAL, https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Apr. 19, 2024).

[85] *Hackers, breaches, and the value of healthcare data*, IMPRIVATA (Jun. 30, 2021) https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (citing *The Value of Data*, https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

[86] Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, TIME (Jan. 9, 2017), https://time.com/4588104/medical-data-industry/).

[87] Christina Farr, *Hospital execs say they are getting flooded with requests for your health data*, CNBC (Dec. 18, 2019) https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

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

243. But these rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

244. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

VI. TOLLING, CONCEALMENT & ESTOPPEL

245. 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.

246. 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.

247. 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.

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

249. 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.

250. 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.

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

VII. CLASS ALLEGATIONS

251. **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.:

252. 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.

253. 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.

254. 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.

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

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

256. 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.

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

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

259. **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's Web Properties since at least 2015. Members of the Class can be identified through Defendant's records or by other means.

260. **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.

261. **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.

262. **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.

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

Plaintiffs and Plaintiffs' counsel are committed to vigorously prosecuting this action on behalf of the Class members.

263. 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 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.

264. **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:

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

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;

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;

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

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

265. **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.

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

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

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;

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

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

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)

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

268. 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.

269. 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 . . . ."

270. 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.

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

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

272. 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.

273. 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.

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

275. 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.

276. 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.

277. As a result of Defendant's unlawful conduct, Plaintiffs and California Subclass Members suffered an injury, including violation to their rights of privacy,

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

loss of the privacy of their Private Information, loss of control over their sensitive personal information, and suffered aggravation, inconvenience, and emotional distress.

278. 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*)

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

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

281. 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.

282. 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).

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

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

284. **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).

285. 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.

286. **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).

287. **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.

288. 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

289. 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.

290. 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.

291. This information was, in turn, used by third parties, such as Facebook to 1) place Plaintiffs and Class Members in specific health-related categories and 2) target Plaintiffs and Class Members with particular advertising associated with their specific health conditions.

292. 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).

293. 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).

294. 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.

295. The ECPA provides that a "party to the communication" may liable where a "communication is intercepted for the purpose of committing any criminal or

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

tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

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

297. Here, as alleged above, Defendant violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing IIHI to a third party. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

298. Plaintiffs' and Class Members' information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiff's expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant intentionally used the wire or electronic communications to intercept Plaintiffs Private Information in violation of the law.

299. 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.

300. 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.

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

301. 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.

302. Defendant's acquisition of patient communications that were used and disclosed to Facebook was also 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. Invasion of privacy;

b. Breach of confidence;

c. Breach of fiduciary duty;

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

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

303. 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 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.

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

305. 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,

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

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;

B. 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;

C. 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;

D. Defendant has failed to provide Plaintiffs and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of its patient information; and

E. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, medical treatment, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

306. 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.

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

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

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

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

310. Consumers have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that caused third-party Pixels and cookies (including but not limited to the fbp, ga and gid cookies) and other tracking technologies to be deposited on Plaintiffs' and Class members' computing devices as "first-party" cookies that are not blocked.

311. Defendant's scheme or artifice to defraud in this action consists of:

A. the false and misleading statements and omissions in its privacy policy set forth above, including the statements and omissions recited in the claims below;

B. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Facebook.

312. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiffs' and Class Members' property:

A. property rights to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

B. property rights to determine who has access to their computing devices.

313. 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

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

provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

314. 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

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

(On behalf of Plaintiffs and the California Subclass)

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

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

317. 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:

A. "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,"

B. "willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire,

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

line or cable or is being sent from or received at any place within [the state of California],"

C. "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained," or

D. ***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).

318. 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).

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

320. 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.

321. 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.

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

322. 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 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.

323. 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.

324. 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.

325. 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.

326. By embedding Facebook Pixels on its Web Properties, Defendant aided, agreed with, employed, and conspired with Facebook to wiretap consumers

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

communications on Defendant's Web Properties using the Facebook Pixel snipped codes and to accomplish the wrongful conduct at issue here.

327. 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.

328. 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;

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; and

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

329. 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.

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

331. 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.

332. 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

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

whether their website communications will be collected, viewed, or otherwise improperly accessed, stored, and used by Facebook.

333. 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.

334. 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 FOUR

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)

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

A. Unlawful Prong

336. 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.

337. 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

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

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.

338. 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*.

339. 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.

340. 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.

341. 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.

342. 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.

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

B. Unfair Prong

343. 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.

344. 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.

345. 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.

346. 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.

347. 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.

348. 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.

349. 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.

350. The harm caused by the Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives

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

to further Defendant's legitimate business interests other than Defendant's conduct described herein.

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

352. 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.

353. 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.

354. 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.

///

///

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

COUNT FIVE

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

(On behalf of Plaintiffs and the California Subclass)

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

356. 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.

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

358. 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.

359. 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.

360. 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.

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

361. 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.

362. 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.

363. 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.

364. 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.

365. 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.

366. 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.

367. 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.

///

///

///

///

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

COUNT SIX

INVASION OF PRIVACY

INTRUSION UPON SECLUSION

(On behalf of Plaintiffs and the Nationwide Class)

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

369. 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.

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

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

372. 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.

373. 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.

374. 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."[88]

375. 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.

376. 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.

377. As a proximate result of such unauthorized disclosures, Plaintiffs' and Nationwide Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted and caused damages to Plaintiffs and Nationwide Class Members.

378. 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.

379. 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.

///

///

[88] *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

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

COUNT SEVEN

VIOLATION OF CALIFORNIA CONSUMERS LEGAL REMEDIES ACT, Cal. Civ. Code § 1750, *et seq.* ("CLRA")

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

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

381. 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).

382. 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.

383. 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.

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

385. 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).

386. 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.

387. 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 EIGHT

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

(On behalf of Plaintiffs and the California Subclass)

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

389. 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 *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).

390. 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.

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

391. 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.

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

393. 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.

394. 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.

395. 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.

396. 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).

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

397. 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 NINE

BREACH OF CONFIDENCE

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

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

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

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

401. 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.

402. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Pixel (and other tracking technologies) to disclose and transmit Plaintiffs' and Class Members' Private Information and the contents of their communications exchanged with Defendant to third parties.

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

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

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

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

406. 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

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

407. 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 TEN

BREACH OF FIDUCIARY DUTY

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

408. 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

409. 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.

410. 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.

411. 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.

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

COUNT ELEVEN

UNJUST ENRICHMENT

(On behalf of Plaintiffs and Nationwide Class)

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

414. 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

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

parties. Defendant received payments for medical services from Plaintiffs and Class Members.

415. 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.

416. 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, 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.

417. 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.

418. 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

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

targeted advertising related to Users' respective medical conditions and treatments sought.

419. 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.

420. 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.

421. 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.

422. 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.

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

424. 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.

VIII. 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

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

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;

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.

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

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.

IX. JURY TRIAL DEMANDED

Plaintiffs demand a jury trial on all triable issues.

DATED: April 22, 2024

CLARKSON LAW FIRM, P.C.

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

ALMEIDA LAW GROUP LLC

/s/ John R. Parker, Jr.
John R. Parker, Jr. (SBN 257761)

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