

**CLARKSON LAW FIRM, P.C.**

Ryan J. Clarkson (SBN 257074)  
*rclarkson@clarksonlawfirm.com*  
 Yana Hart (SBN 306499)  
*yhart@clarksonlawfirm.com*  
 Tiara Avanness (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)  
*jrpark@almeidagroup.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.*

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

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**

## TABLE OF CONTENTS

I.	INTRODUCTION .....	1
II.	PARTIES.....	9
III.	JURISDICTION & VENUE .....	9
IV.	REPRESENTATIVE PLAINTIFFS’ EXPERIENCES .....	10
V.	FACTUAL BACKGROUND.....	22
	A. The Problematic Use of Invisible Tracking Codes to Collect People’s Data for its Advertising Business.....	22
	B. Defendant Disclosed Patient Healthcare Information, Including Patient Status, in Violation of the HIPAA Privacy Rule .....	29
	C. HIPAA’s Protections Do Not Exclude Internet Marketing .....	31
	D. The Industry was Warned of Third-Party Tracking Tools Resulting in HIPAA Violations, but Defendant Elected to Continue Their Illicit Sharing Anyway .....	33
	E. Defendant Transmitted a Broad Spectrum of Plaintiffs’ & Class Members’ Identifiable Health Information to Meta via the Meta Tracking Tools.....	36
	F. Defendant’s Web Properties Sent Plaintiffs’ and Class Members’ PHI to Facebook Along with Unique Personal Identifiers .....	43
	G. Defendant Violates Its Promises to Users and Patients to Protect Their Confidentiality.....	45
	H. Plaintiffs and Class Members Reasonably Believed That Their Confidential Medical Information Would Not Be Shared with Third Parties .....	48
	I. Plaintiffs and Class Members Have No Way of Determining Widespread Usage of Invisible Pixels.....	49
	J. Defendant Knew Plaintiffs’ Private Information Included Sensitive Medical Information, Including Medical Records.....	50

1	K. Plaintiffs and Class Members Have a Reasonable Expectation of Privacy	
2	in Their Private Information, Especially with Respect to Sensitive	
3	Medical Information.....	52
4	L. Eisenhower Was Enriched & Benefitted from the Use of the Pixel &	
5	other Tracking Technologies that Enabled the Unauthorized Disclosures	
6	Alleged Herein .....	55
7	M. Plaintiffs' & Class Members' Private Information	
8	Has Substantial Value.....	57
9	VI. TOLLING, CONCEALMENT & ESTOPPEL .....	60
10	VII. CLASS ALLEGATIONS.....	61
11	COUNT ONE: VIOLATION OF THE CONFIDENTIALITY OF MEDICAL	
12	INFORMATION ACT CAL. CIV. CODE §§ 56, <i>et seq.</i> .....	67
13	COUNT TWO: VIOLATIONS OF ELECTRONIC COMMUNICATIONS	
14	PRIVACY ACT ("ECPA") 18 U.S.C. § 2511(1), <i>et seq.</i> .....	69
15	COUNT THREE: VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY	
16	("CIPA"), CAL. PENAL CODE § 630, <i>et seq.</i> .....	77
17	COUNT FOUR: VIOLATION OF THE UNFAIR COMPETITION LAW ("UCL")	
18	CALIFORNIA BUSINESS AND PROFESSIONS CODE § 17200, <i>et seq.</i> .....	82
19	A. Unlawful Prong .....	82
20	B. Unfair Prong.....	84
21	COUNT FIVE: INVASION OF PRIVACY UNDER CALIFORNIA'S	
22	CONSTITUTION, ART. I, § 1.....	85
23	COUNT SIX: INVASION OF PRIVACY INTRUSION UPON SECLUSION.....	88
24	COUNT SEVEN: VIOLATION OF CALIFORNIA CONSUMERS LEGAL	
25	REMEDIES ACT, Cal. Civ. Code § 1750, <i>et seq.</i> ("CLRA") .....	90
26		
27		
28		

1	COUNT EIGHT: LARCENY/RECEIPT OF STOLEN PROPERTY (VIOLATION	
2	OF CALIFORNIA PENAL CODE § 496(a) and (c) .....	91
3	COUNT NINE: BREACH OF CONFIDENCE.....	93
4	COUNT TEN: BREACH OF FIDUCIARY DUTY .....	94
5	COUNT ELEVEN: UNJUST ENRICHMENT .....	95
6	VIII. PRAYER FOR RELIEF .....	97
7	IX. JURY TRIAL DEMANDED .....	99

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

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

### 9 **I. INTRODUCTION**

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

14 2. The Eisenhower Health Main Campus includes a children’s center, birth  
 15 center, bariatric care, emergency center, and the Eisenhower Medical Center  
 16 Hospital.<sup>1</sup> The Hospital is a full-service hospital where patients are able to receive  
 17 care from expert clinicians and physicians and is comprised of primary care locations,  
 18 urgent care center, multi-specialty health center, and specialized programs.<sup>2</sup>

19 3. Defendant also runs a system of primary care clinics providing medical  
 20 care to families as well as multiple urgent care locations allowing patients to seek  
 21 medical consultations on a walk-in basis.<sup>3</sup>

22  
 23 <sup>1</sup> *Eisenhower Health Main Campus*, EISENHOWER HEALTH,  
 24 <https://eisenhowerhealth.org/locations/?action=detail&dataRef=15> (last visited on  
 April 19, 2024).

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

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

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

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

9           6. Defendant has disregarded the privacy rights of its patients (including  
10 potential patients) who used its Web Properties ("**Users**" or "**Class Members**") by  
11 intentionally, willfully, recklessly and/or negligently failing to implement adequate  
12 and reasonable measures to ensure that the Users' personally identifiable information  
13 ("**PII**") and protected health information ("**PHI**") (collectively, "**Private**  
14 **Information**") was safeguarded. Instead, Defendant enabled unauthorized third  
15 parties such as Facebook and Google to intercept the content of its Users'  
16 communications on Defendant's Web Properties.

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

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

25  
26 <sup>4</sup> At the time of filing this complaint Plaintiffs are unable to determine whether  
27 Pixels were embedded inside Defendant's MyChart Portal. However, given  
28 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.<sup>5</sup>

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.<sup>6</sup>

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>.

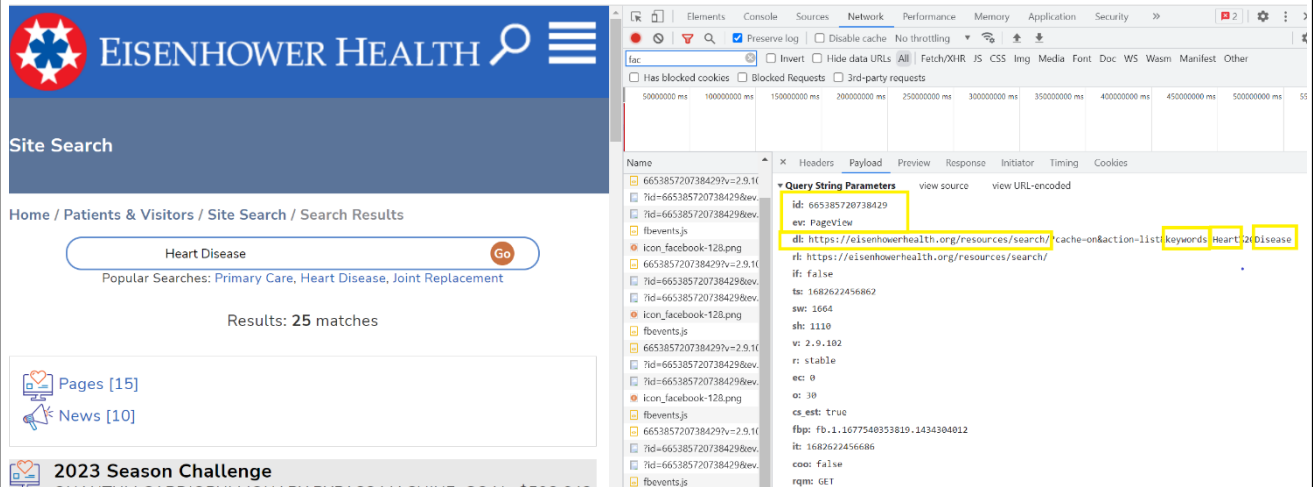
<sup>5</sup> To find the Facebook account associated with a particular c\_user cookie, one simply needs to type [www.facebook.com/](https://www.facebook.com/) followed by the c\_user ID.

<sup>6</sup> 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).



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.

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.

▼ Request Headers

```
:authority: www.facebook.com
:method: GET
:path: /tr/?id=665385720738429&ev=PageView&dl=https%3A%2F%2Feisenhowerhealth.org%2Fresources%2Fsearch%2F%3Fcache%3Don%26action%3Dlist%26keywords%3FHeart%2520Disease&rl=https%3A%2F%2Feisenhowerhealth.org%2Fresources%2Fsearch%2F&if=false&ts=1682622456862&sw=1664&sh=1110&v=2.9.102&r=s1able&ec=0&o=30&cs_est=true&fbp=fb.1.1677540353819.1434304012&it=1682622456686&coo=false&rqm=GIT
: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=QtI1Y1lVd2UW0uuBmn2Mb8vC; sb=GrxtY1jj9lKWnpCg7UAhiJMv; c_user=54€; xs=7%3A_bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AAcVF8I7YyNYaI3bQ3Mo-c1bIjBPIB21upjmYX5TTDf-W; r=0GszWVVFcrn0BxYAH.AWVyw6mXR8D6QhniF3z5qbu_XSo.BkSroG.-f.AAA.0.0.BkSroG.AWXHmKfgepI
:referrer: https://eisenhowerhealth.org/
:sec-ch-ua: "Chromium";v="112", "Google Chrome";v="112", "Not:A-Brand";v="99"
```

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.<sup>7</sup> Finally, continuing to the right on the top line, Defendant is disclosing that the User is visiting the webpage

<sup>7</sup> 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.

1 “eisenhowerhealth.org/resources.”

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

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

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

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

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

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

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

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

17 24. Plaintiffs and Class Members who visited and used Defendant's Web  
18 Properties thought they were communicating with only their trusted healthcare  
19 providers, and reasonably believed that their sensitive and private PHI would be  
20 guarded with the utmost care. In browsing Defendant's Web Properties—be it to  
21 locate and make an appointment with a doctor with a specific specialty, find sensitive  
22 information about their diagnosis, or investigate treatment for their diagnosis—  
23 Plaintiffs and Class Members did not expect that every search (including exact words  
24 and phrases they typed into Defendant's website search bars), extremely sensitive PHI  
25 such as health conditions (*e.g.*, breast cancer), diagnoses (*e.g.*, stroke, arthritis,  
26 COVID-19 or AIDS), procedures sought, treatment status, and/or the names and  
27 locations of their personal and other treating physicians, or even their  
28 access/interactions on Defendant's online Portal would be intercepted, captured and

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

3 25. Plaintiffs continued to have their privacy violated when their Private  
4 Information was used to turn a profit by way of targeted advertising related to their  
5 respective medical conditions and treatments sought.

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

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

12 28. Defendant's actions constitute an extreme invasion of Plaintiffs' and  
13 Class Members' right to privacy and violate federal and state statutory and common  
14 law as well as Defendant's own Privacy Policies that affirmatively and unequivocally  
15 state that any personal information provided to Defendant will remain secure and  
16 protected.<sup>8</sup>

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

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

27 <sup>8</sup> Eisenhower's Privacy Policies (and other affirmative representations) represent to  
28 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).

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.<sup>9</sup>

## 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

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



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

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

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

#### 16 **IV. REPRESENTATIVE PLAINTIFFS' EXPERIENCES**

##### 17 **Plaintiff B.K.**

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

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

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

26 40. Plaintiff B.K. has used and continues to use the same devices to maintain  
27 and access an active Facebook account throughout the relevant period in this case.  
28

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.<sup>10</sup>

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

<sup>10</sup> 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/>.



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

9 46. In July 2020 Plaintiff B.K. felt sick with what she believed to be COVID-  
10 19. As part of her seeking healthcare from Defendant, she utilized the Website to  
11 research COVID-19 symptoms and whether, if she was experiencing severe  
12 symptoms, she needed to go to the hospital and/or the emergency care. On July 9,  
13 2020, Plaintiff B.K. went to Defendant's ER and was diagnosed with COVID-19.

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

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

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

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

13 50. The full scope of Defendant’s interceptions and disclosures of Plaintiff  
14 B.K.’s communications to Meta can only be determined through formal discovery.  
15 However, Defendant intercepted at least the following communications about  
16 Plaintiff B.K.’s patient status, medical knee condition, treatments sought, and  
17 prospective specialized healthcare providers, via the following long-URLs or  
18 substantially similar URLs that were sent to Meta via the Pixel (and which contain  
19 information concerning Plaintiff B.K.’s specific medical conditions, queries, as well  
20 as types of providers and treatments sought):  
21  
22  
23  
24  
25  
26  
27  
28

- 1 • <https://eisenhowerhealth.org/services/orthopedics/conditions/knee-pain-and-injury/>
- 2
- 3 • [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Pain)
- 4 &keywords=Knee%20Pain
- 5
- 6 • [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Arthritis)
- 7 &keywords=Knee%20Arthritis
- 8
- 9 • [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Injections)
- 10 &keywords=Knee%20Injections
- 11
- 12 • [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Replacement)
- 13 &keywords=Knee%20Replacement
- 14
- 15 • [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Gel)
- 16 &keywords=Knee%20Gel
- 17
- 18 • [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Knee%20Pain%20Non-Surgical%20Treatments)
- 19 &keywords=Knee%20Pain%20Non-Surgical%20Treatments
- 20
- 21 • <https://eisenhowerhealth.org/services/orthopedics/>
- 22
- 23 • [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Osteoarthritis)
- 24 &keywords=Osteoarthritis
- 25
- 26 • [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=COVID%20symptoms)
- 27 &keywords=COVID%20symptoms
- 28
- [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Do%20I%20Have%20Covid)
- &keywords=Do%20I%20Have%20Covid
- [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Do%20I%20Have%20To%20Go%20To%20ER%20If%20I%20Have%20Covid)
- &keywords=Do%20I%20Have%20To%20Go%20To%20ER%20If%20I%20Have%20Covid

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

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

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

- 16 • <https://mychart.eisenhowerhealth.org/mychart/Authentication/Login?>
- 17 • <https://eisenhowerhealth.org/resources/mychart/>

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

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

25 56. As described herein, Defendant worked along with Facebook to intercept  
 26 Plaintiff B.K.'s communications, including those that contained her Private  
 27 Information.  
 28

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

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

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

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

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

15           **Plaintiff N.Z.**

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

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

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

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

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

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

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

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

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/>



- <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>

///

///

///

///

///

///

///

///

///

///



- 1 • [https://eisenhowerhealth.org/services/oncology/services/breast-](https://eisenhowerhealth.org/services/oncology/services/breast-center/diagnosis/)
- 2 [center/diagnosis/](https://eisenhowerhealth.org/services/oncology/services/breast-center/diagnosis/)
- 3
- 4 • [https://eisenhowerhealth.org/services/oncology/services/breast-](https://eisenhowerhealth.org/services/oncology/services/breast-center/mammography/)
- 5 [center/mammography/](https://eisenhowerhealth.org/services/oncology/services/breast-center/mammography/)
- 6
- 7 • <https://eisenhowerhealth.org/services/digestive/>
- 8 • [https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-](https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-screening/)
- 9 [screening/](https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-screening/)
- 10
- 11 • [https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-](https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-screening/colorectal-cancer-screening/)
- 12 [screening/colorectal-cancer-screening/](https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-screening/colorectal-cancer-screening/)
- 13
- 14 • [https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-](https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-screening/colorectal-cancer-screening/colonoscopy-and-prep-instructions/)
- 15 [screening/colorectal-cancer-screening/colonoscopy-and-prep-instructions/](https://eisenhowerhealth.org/services/digestive/colorectal-cancer-and-screening/colorectal-cancer-screening/colonoscopy-and-prep-instructions/)
- 16
- 17 • <https://eisenhowerhealth.org/services/digestive/faq/>
- 18
- 19 • [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Suspicious%20Breast%20Mass)
- 20 [&keywords=Suspicious%20Breast%20Mass](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Suspicious%20Breast%20Mass)
- 21
- 22 • [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Suspicious%20Breast%20Cancer)
- 23 [&keywords=Suspicious%20Breast%20Cancer](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Suspicious%20Breast%20Cancer)
- 24
- 25 • [https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Colon%20Polyps)
- 26 [&keywords=Colon%20Polyps](https://www.eisenhowerhealth.org/resources/search/?cache=on&action=list&keywords=Colon%20Polyps)

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

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

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

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

- 12 • <https://mychart.eisenhowerhealth.org/mychart/Authentication/Login?>
- 13 • <https://eisenhowerhealth.org/resources/mychart/>

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

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

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

25 77. As described herein, Defendant enabled Facebook to intercept Plaintiff  
26 N.Z.'s communications, including those that contained her Private Information about  
27 her medical conditions, symptoms, and treatment.  
28

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

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

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

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

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

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

## 18                                   V. **FACTUAL BACKGROUND**

### 19           A. ***The Problematic Use of Invisible Tracking Codes to Collect People's*** 20 ***Data for its Advertising Business.***

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

23           85. The Meta Pixel and other third-party tracking tools also collect and  
24 transmit information from Defendant that identifies a Facebook user's status as a  
25 patient and other health information that is protected by federal and state law. This  
26 occurs through tools that Facebook encourages its healthcare Partners to use,  
27 including uploading patient lists to Facebook for use in its advertising systems.  
28

1           86. Meta associates the information it obtains via the Meta Pixel with other  
 2 information regarding the User, using personal identifiers that are transmitted  
 3 concurrently with other information the Pixel is configured to collect. For Facebook  
 4 account holders, these identifiers include the “c\_user” cookie IDs, which allow Meta  
 5 to link data to a particular Facebook account. For both Facebook account holders and  
 6 users who do not have a Facebook account, these identifiers also include cookies that  
 7 Meta ties to their browser.

8           87. Realizing the value of having direct access to millions of consumers, in  
 9 2007, Facebook began monetizing its platform by launching “Facebook Ads,”  
 10 proclaiming it to be a “completely new way of advertising online” that would allow  
 11 “advertisers to deliver more tailored and relevant ads.”<sup>11</sup>

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

14           89. Ad Targeting has been extremely successful due, in large part, to  
 15 Facebook’s ability to target people at a granular level. “Among many possible target  
 16 audiences, Facebook offers advertisers, [for example,] 1.5 million people ‘whose  
 17 activity on Facebook suggests that they’re more likely to engage with/distribute  
 18 liberal political content’ and nearly seven million Facebook users who ‘prefer high-  
 19 value goods in Mexico.’”<sup>12</sup>

20           90. The Meta Pixel is a free and publicly available “piece of code” that third-  
 21 party web developers can install on their website to “measure, optimize and build  
 22 audiences for ... ad campaigns.”<sup>13</sup>

23  
 24  
 25 <sup>11</sup>*Facebook Unveils Facebook Ads*, META (Nov. 6, 2007),  
<https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/>.

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

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

1           91. Meta describes the Pixel as “a snippet of Javascript code” that “relies on  
2 Facebook cookies, which enable [Facebook] to match ... website visitors to their  
3 respective Facebook User accounts.”<sup>14</sup>

4           92. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers  
5 the Pixel “can help you better understand the effectiveness of your advertising and  
6 the actions people take on your site, like visiting a page or adding an item to their  
7 cart.”<sup>15</sup>

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

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

12           B. “Create Custom Audiences from website visitors” and create  
13 “[d]ynamic ads [to] help you automatically show website  
14 visitors the products they viewed on your website—or related  
15 ones.”<sup>16</sup>

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

25 \_\_\_\_\_  
26 <sup>14</sup> *Meta Pixel*, META, <https://developers.facebook.com/docs/meta-pixel/> (last  
27 visited Apr. 19, 2024).

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

<sup>16</sup> *Id.*



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<sup>17</sup> for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website.<sup>18</sup>

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.

<sup>17</sup> 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).

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

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

6           99. Healthcare providers like Defendant encourage Plaintiffs and Class  
7 Members to access and use various digital tools via its Web Properties to, among  
8 other things, receive healthcare services, in order to gain additional insights into its  
9 Users, improve its return on marketing dollars and, ultimately, increase its revenue.

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

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

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

26  
27  
28



1           103. Thus, the Meta “pixel allows Facebook to be a silent third-party watching  
2 whatever you’re doing,”<sup>19</sup> which in this case included the content of Defendant’s  
3 patients’ communications with its Web Properties, including their PHI.

4           104. For Facebook, the Pixel acts as a conduit of information, sending the  
5 information it collects to Facebook through scripts running in the User’s internet  
6 browser, via data packets labeled with PII, including the User’s IP address, the  
7 Facebook c\_user cookie and third-party cookies allowing Facebook to link the data  
8 collected by Meta Pixel to the specific Facebook user.<sup>20</sup>

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

13           106. David Holtzman, a health privacy consultant was “deeply troubled” by  
14 the results of The Markup’s investigation and indicated “it is quite likely a HIPAA  
15 violation” by the hospitals, such as Defendant.<sup>22</sup>

16           107. Facebook’s access to use even only some of these data points—such as  
17 just a “descriptive” webpage URL—is problematic. As Laura Lazaro Cabrera, a legal  
18 officer at Privacy International, explained: “Think about what you can learn from a  
19 URL that says something about scheduling an abortion’ . . . ‘Facebook is in the  
20  
21

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

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

28 <sup>21</sup> See Feathers, *et al.*, *supra* note 4.

<sup>22</sup> *Id.*



1 business of developing algorithms. They know what sorts of information can act as a  
2 proxy for personal data.”<sup>23</sup>

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

10 109. This data can be used not only to provide personalized and targeted  
11 content and advertising, but also for more nefarious purposes, such as tracking and  
12 surveillance. Moreover, the misuse of this data could potentially lead to the spread of  
13 false or misleading information, which could have serious consequences, particularly  
14 in the case of health-related information.

15 110. As pointed out by the Office for Civil Rights (OCR) at the U.S.  
16 Department of Health and Human Services (HHS), impermissible disclosures of such  
17 data in the healthcare context “may result in identity theft, financial loss,  
18 discrimination, stigma, mental anguish, or other serious negative consequences to the  
19 reputation, health, or physical safety of the individual or to others identified in the  
20 individual’s PHI . . . This tracking information could also be misused to promote  
21 misinformation, identity theft, stalking, and harassment.”<sup>24</sup> As anticipated by the  
22 OCR and HHS, Plaintiffs here, as a result of Defendant’s impermissible disclosure of  
23

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

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

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

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

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

10 112. Healthcare entities collecting and disclosing Users' Private Information  
11 face significant legal exposure under the Health Insurance Portability and  
12 Accountability Act of 1996 ("HIPAA"), which applies specifically to healthcare  
13 providers, health insurance providers and healthcare data clearinghouses.<sup>27</sup>

14 113. The HIPAA Privacy Rule sets forth policies to protect all individually  
15 identifiable health information ("IIHI") that is held or transmitted.<sup>28</sup> This is  
16 information that can be used to identify, contact, or locate a single person or can be  
17 used with other sources to identify a single individual.

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

21 <sup>25</sup> The Markup reported that 33 of the largest 100 hospital systems in the country  
22 utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked  
23 a button to schedule a doctor's appointment. Todd Feathers, *Facebook Is Receiving*  
*Sensitive Medical Information from Hospital Websites*, *supra*, note 6.

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

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

28 <sup>28</sup> 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.

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

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

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

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

23 ///

24 ///

25 \_\_\_\_\_  
 26 <sup>29</sup> *Guidance Regarding Methods for De-identification of Protected Health*  
 27 *Information in Accordance with the Health Insurance Portability and Accountability*  
 28 *Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVICES,  
[https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html)  
[identification/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html) (last visited Apr. 19, 2024).

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

2 119. As the OCR reminded entities regulated under HIPAA (like Defendant)  
3 in its recently issued *Use of Online Tracking Technologies by HIPAA Covered*  
4 *Entities and Business Associates* bulletin:

5 Regulated entities are not permitted to use tracking technologies  
6 in a manner that would result in impermissible disclosures of PHI  
7 to tracking technology vendors or any other violations of the  
8 HIPAA Rules. ***For example, disclosures of PHI to tracking  
technology vendors for marketing purposes, without  
individuals' HIPAA-compliant authorizations, would  
constitute impermissible disclosures.***<sup>30</sup>

9 120. The OCR makes it clear that information that is routinely collected by  
10 vendors on public-facing websites may be PHI, including unique identifiers such as  
11 IP addresses, device IDs, or email addresses.<sup>31</sup>

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

16 This is because, when a regulated entity collects the individual's  
17 IHHI through its website or mobile app, the information connects  
18 the individual to the regulated entity (*i.e.* it is indicative that the  
19 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.<sup>32</sup>

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

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

24 <sup>30</sup> *Use of Online Tracking Technologies by HIPAA Covered Entities and Business*  
25 *Associates, supra*, note 27 (emphasis added) (updated Mar.18, 2024) (last visited Apr.  
19, 2024).

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

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

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.<sup>33</sup>

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.

<sup>33</sup> *Id.* (emphasis added).



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

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

7 127. Recognizing the distinct privacy dangers third party tracking tools  
 8 present, the Federal Trade Commission ("FTC") joined HHS in warning HIPAA-  
 9 covered entities and non-HIPAA covered entities alike that unauthorized disclosure  
 10 of sensitive health information is through online tracking technology must be  
 11 prevented.<sup>34</sup>

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

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

19 "When consumers visit a hospital's website or seek telehealth services, they  
 20 should not have to worry that their most private and sensitive health information  
 21 may be disclosed to advertisers and other unnamed, hidden third parties," said  
 22 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

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

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

everything in our powers to protect consumers' health information from potential misuse and exploitation."<sup>36</sup>

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.<sup>37</sup>

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."<sup>38</sup>

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

<sup>36</sup> *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, *supra*, note 40.

<sup>37</sup> *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).

<sup>38</sup> *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, *supra*, note 40.

<sup>39</sup> 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>.

<sup>40</sup> 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>.

<sup>41</sup> *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

1 bulletin<sup>42</sup> concerning the privacy risks resulting from the use of tracking  
2 technologies like Meta Pixel.

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

5 “If you are a covered entity or business associate (“regulated entities”) under  
6 HIPAA, you **must** comply with the HIPAA Privacy, Security, and Breach  
7 Notification Rules (HIPAA Rules), with regard to protected health information  
(PHI) that is transmitted or maintained in electronic or any other form or  
medium.

8 The HIPAA Rules apply when the information that a regulated entity collects  
9 through tracking technologies or discloses to third parties (e.g., tracking  
10 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  
11 tracking technologies by HIPAA regulated entities provides a general overview  
12 of how the HIPAA Rules apply.[] This bulletin discusses what tracking  
13 technologies are and reminds regulated entities of their obligations to comply  
with the HIPAA Rules when using tracking technologies.”<sup>43</sup>

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

19 135. Defendant’s purposeful violation of HIPAA despite clear warnings is  
20 emblematic of systemic privacy issues at Eisenhower medical facilities in particular.  
21 ProPublica even identified Defendant as the #1 hospital-culprit in California with the  
22

---

23 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  
24 Dkt. No. C-4747 (June 22, 2021), <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc>.

25 <sup>42</sup> *Use of Online Tracking Technologies by HIPAA Covered Entities and Business  
26 Associates, supra*, note 27 (updated March 18, 2024) (last visited Apr. 19, 2024).

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



1 most privacy-related deficiencies from 2012 to 2015—riddled with HIPAA violations  
2 and unauthorized disclosures of PHI.<sup>44</sup>

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

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

9 137. Source Code is a set of instructions that commands the website visitor’s  
10 browser to take certain actions when the web page first loads or when a specified  
11 event triggers the code. Source Code is designed to be readable by humans and  
12 formatted in a way that developers and other users can understand.

13 138. In addition to controlling a website’s Markup, Source Code executes a  
14 host of other programmatic instructions including the ability to command a website  
15 user’s browser to send data transmissions to third parties like Facebook, via the Meta  
16 Pixel.<sup>45</sup>

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

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

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

<sup>45</sup> 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.

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

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

- 8 a. The exact search terms entered by a User on the Website,  
 9 including searches for the User's medical symptoms and  
 10 conditions, specific medical providers and their specialty,  
 11 and treatments sought;
- 12 b. descriptive URLs that describe the categories of the  
 13 Website, categories that describe the current section of the  
 14 Website, and the referrer URL that caused navigation to  
 the current page;
- 15 c. the communications a User exchanges through  
 16 Defendant's Web Properties by clicking and viewing  
 17 webpages, including communications about providers  
 18 and specialists, conditions, and treatments, along with the  
 19 timing of those communications, including, upon  
 20 information and good faith belief, whether they are made  
 21 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;
- 22 d. when a User sets up or schedules an appointment;
- 23 e. information that a User clicks on in an appointment form;
- 24 f. when a User clicks a button to call the provider from a  
 25 mobile device directly from Defendant's Website;
- 26 g. when a User clicks to register for the Patient Portal, clicks  
 27 to log into the Portal, and/or accesses other patient-  
 28 dedicated web pages; and

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

4 143. Thus, Defendant is, in essence, handing patients a tapped device and once  
5 one of its webpages is loaded into the User's browser, the software-based wiretap is  
6 quietly waiting for private communications on the webpage to trigger the tap, which  
7 intercepts those communications—intended only for Defendant—and transmits those  
8 communications to unauthorized third parties such as Facebook.

9 144. For example, when a patient visits [www.eisenhowerhealth.org](http://www.eisenhowerhealth.org) and enters  
10 “heart disease,” “diabetes” or “stroke rehabilitation” into the search bar, their browser  
11 automatically sends an HTTP request to Eisenhower's web server. Eisenhower's web  
12 server automatically returns an HTTP response, which loads the Markup for that  
13 particular webpage.

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

16 146. In reality, Defendant's Source Code and underlying HTTP Requests and  
17 Responses share the patient's personal information with Facebook, including the fact  
18 that a User was looking for treatment for their heart disease, diabetes, or stroke  
19 diagnosis — along with the User's unique personal identifiers.  
20  
21  
22  
23  
24  
25  
26  
27  
28

▼ Request Headers

*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.*

The screenshot shows two parts of a web browser. On the left is the 'Patient Resources' page, which has a blue header and lists several links under the heading 'Title':

- [Diabetes Education Services](#)
- [Diabetes Education Services - Spanish](#)
- [Diabetes Prevention Program](#)
- [Hechos Sobre la Diabetes](#)

On the right is the Chrome DevTools Network tab. It shows a request for 'icon\_facebook-128.png'. The 'Query String Parameters' section is expanded, displaying the following details:

- id: 665385720738429
- ev: PageView
- dl: https://eisenhowerhealth.org/services/diabetes/#resource
- rl: https://eisenhowerhealth.org/services/diabetes-endocrinology/
- if: false
- ts: 16820965243962
- sw: 1664

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

1 <https://www.eisenhowerhealth.org> to look for medical treatments for her knee pain,  
 2 her exact search terms (including “knee pain,” “knee arthritis,” “knee osteoarthritis,”  
 3 “knee injections,” “knee replacement,” and “non-surgical treatments for knee pain”) were transmitted by Defendant’s Pixel to Meta, disclosing her specific medical  
 4 conditions.  
 5

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

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

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

22 152. For example, a diabetes patient in search for diabetes services can search  
 23 for various diabetes treatment options and information, from “endocrinology clinic”  
 24 and “diabetes prevention” to resources intended to help patients.<sup>46</sup>  
 25  
 26

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



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.

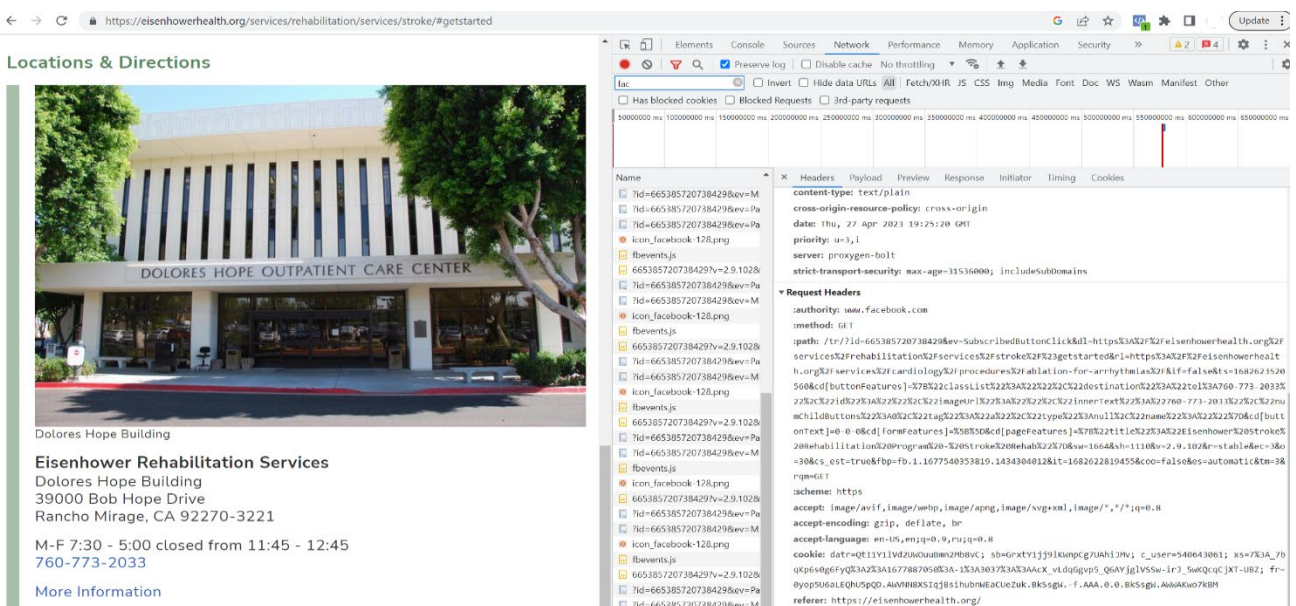
154. The transmission identifies the User as a patient: (i) seeking medical care from Defendant via www.eisenhowerhealth.org; (ii) who has diabetes; and (iii) who is searching for diabetes services.

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*:







1 163. For Plaintiff B.K., Defendant would have disclosed that starting in May  
 2 2018 she was looking up procedures to treat knee pain (including knee replacement),  
 3 including but not limited to sharing the descriptive URL  
 4 [https://eisenhowerhealth.org/services/orthopedics/conditions/knee-pain-and-](https://eisenhowerhealth.org/services/orthopedics/conditions/knee-pain-and-injury/#procedures)  
 5 [injury/#procedures](https://eisenhowerhealth.org/services/orthopedics/conditions/knee-pain-and-injury/#procedures) that she visited on Defendant's Website.

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

8 164. As described herein, Defendant's Meta Pixel (and other third-party  
 9 trackers) sent sensitive Private Information to Facebook, including but not limited to  
 10 Plaintiffs' and Class Members': (i) status as medical patients; (ii) health conditions;  
 11 (iii) sought treatments or therapies; (iv) terms and phrases entered into Defendant's  
 12 search bar; (v) the specialty and location of personal, treating, and other physicians  
 13 and providers sought together with any medical specialties; (vi) selected locations or  
 14 facilities for treatment; and (vii) web pages viewed.

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

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

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

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

3 168. The "datr" cookie identifies the patient's specific web browser from  
4 which the patient is sending the communication. It is an identifier that is unique to the  
5 patient's specific web browser and is therefore a means of identification for Facebook  
6 users.

7 169. The "fr" cookie is a Facebook identifier that is an encrypted combination  
8 of the c\_user and datr cookies.<sup>47</sup> Facebook, at a minimum, uses the fr cookie to  
9 identify Users.<sup>48</sup>

10 170. At each stage, Defendant Eisenhower also utilized the \_fbp cookie, which  
11 attaches to a browser as a first-party cookie, and which Facebook uses to identify a  
12 browser and a User.<sup>49</sup>

13 171. The fr cookie expires after ninety (90) days unless the User's browser  
14 logs back into Facebook.<sup>50</sup> If that happens, the time resets, and another ninety (90)  
15 days begins to accrue.

16 172. The \_fbp cookie expires after ninety (90) days unless the User's browser  
17 accesses the same website.<sup>51</sup> If that happens, the time resets, and another ninety (90)  
18 days begins to accrue.

19 173. The Facebook Meta Pixel uses both first- and third-party cookies. A first-  
20 party cookie is "created by the website the user is visiting"—i.e., Defendant.<sup>52</sup>

23 <sup>47</sup> Gunes Acar et al., *Facebook Tracking Through Social Plug-ins*, BELGIAN PRIVACY  
24 COMMISSION, (Mar. 27, 2015),  
[https://securehomes.esat.kuleuven.be/~gacar/fb\\_tracking/fb\\_pluginsv1.0.pdf](https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf).

25 <sup>48</sup> *Cookies Policy*, META, <https://www.facebook.com/policy/cookies/> (last visited  
26 Apr. 19, 2024).

26 <sup>49</sup> *Id.*

27 <sup>50</sup> *Id.*

27 <sup>51</sup> *Id.*

28 <sup>52</sup> This is confirmable by using developer tools to inspect a website's cookies and  
track network activity.

1 174. A third-party cookie is “created by a website with a domain name other  
2 than the one the user is currently visiting”—i.e., Facebook.<sup>53</sup>

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

6 176. Facebook, at a minimum, uses the fr, \_fbp, and c\_user cookies to link to  
7 FIDs and corresponding Facebook profiles.

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

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

13 179. Plaintiffs were never provided with any written notice that Defendant  
14 disclosed its Website Users’ Private Information nor were they provided any means  
15 of opting out of such disclosures.

16 180. Despite this, Defendant knowingly and intentionally disclosed Plaintiffs’  
17 Private Information to Facebook.

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

20 181. Beyond Defendant’s legal obligations to protect the confidentiality of  
21 individuals’ Private Information, Defendant’s privacy policies and online  
22 representations affirmatively and unequivocally state that any personal information  
23 provided to Defendant will remain secure and protected.<sup>54</sup>

24 182. Further, Defendant represents to Users that it will only disclose Private  
25 Information provided to them under certain circumstances, **none of which apply**  
26

27 <sup>53</sup> This is confirmable by tracking network activity.

28 <sup>54</sup> *Privacy Policy*, EISENHOWER HEALTH, <https://eisenhowerhealth.org/about/privacy/>  
(last visited Apr. 19, 2024).

1 *here*.<sup>55</sup> Defendant's privacy policies do **not** permit Defendant to use and disclose  
2 Plaintiffs' and Class Members' Private Information for marketing purposes.

3 183. In fact, Defendant acknowledges in its Notice of Privacy Practices that it  
4 "will not sell, trade or rent your personal information to other people or businesses  
5 unless we have your consent."<sup>56</sup>

6 184. Moreover, Defendant represents that it will disclose Users' PHI when  
7 required to in limited circumstances. Defendant represents that it may transfer or share  
8 User's PHI "to successors in title to our business (third parties who by our company  
9 or the relevant part of the business)" or to "comply with lawful requests to disclose  
10 personal information to certain authorities."<sup>57</sup>

11 185. Further, Defendant's Privacy Policy represents:

12 "We are committed to protecting the privacy of your medical  
13 information. We are required by law to maintain the confidentiality  
14 of information that identifies you and the care you receive."

15 "We ensure, to the best of our ability, that our systems are secure so  
16 as to protect your personal information from misuse."

17 "For example, like many web sites, we use cookies, log files and  
18 links to tell us how you use our site, but we do not collect or store  
19 personally identifiable information."<sup>58</sup>

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

22 187. Defendant acknowledges that, "We will not sell, trade or rent your  
23 personal information to other people or businesses unless we have your consent."<sup>59</sup>

24 188. Defendant failed to issue a notice that Plaintiffs' and Class Members'  
25 Private Information had been impermissibly disclosed to an unauthorized third party.  
26 In fact, Defendant **never** disclosed to Plaintiffs or Class Members that it shared their

27 <sup>55</sup> *See id.*

28 <sup>56</sup> *See id.*

<sup>57</sup> *See id.*

<sup>58</sup> *Privacy Policy*, EISENHOWER HEALTH, <https://eisenhowerhealth.org/about/privacy/>  
(last visited Apr. 19, 2024).

<sup>59</sup> *See id.*

1 sensitive and confidential communications, data, and Private Information with  
2 Facebook and other unauthorized third parties.<sup>60</sup>

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

13 190. Even non-Facebook users can be individually identified via the  
14 information gathered on the Digital Platforms, like an IP address or personal device  
15 identifying information. This is precisely the type of information for which HIPAA  
16 requires the use of de-identification techniques to protect patient privacy.<sup>61</sup>

17 191. In fact, in an action currently pending against Facebook related to use of  
18 their Pixel on healthcare provider web properties, Facebook explicitly stated it  
19 requires Pixel users to "post a prominent notice on every page where the Pixel is  
20

21 <sup>60</sup> In contrast to Defendant, in recent months several medical providers which have  
22 installed the Meta Pixel on its Web Properties have provided its patients with notices  
23 of data breaches caused by the Pixel transmitting PHI to third parties. *See, e.g.,*  
24 *Cerebral, Inc. Notice of HIPAA Privacy Breach*, [https://cerebral.com/static/hippa\\_privacy\\_breach-](https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf)  
25 [4000c6eb21449c2ecd8bd13706750cc2.pdf](https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf); Annie Burky, *Advocate Aurora says 3M*  
26 *patients' health data possibly exposed through tracking technologies*, FIERCE  
27 HEALTHCARE (Oct. 20, 2022), [https://www.fiercehealthcare.com/health-](https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3)  
28 [tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-](https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3)  
information-3; *Novant Health Notifies Patients of Potential Data Privacy Incident*,  
PR NEWswire (Aug. 19, 2022), [https://www.prnewswire.com/news-releases/novant-](https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html)  
health-notifies-patients-of-potential-data-privacy-incident-301609387.html.

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

1 embedded and to link from that notice to information about exactly how the Pixel  
2 works and what is being collected through it, so it is not invisible.”<sup>62</sup> Defendant did  
3 not post such a notice, further underscoring the purposefulness of its HIPAA and other  
4 violations alleged.

5 192. Facebook further stated that “most providers [...] will not be sending  
6 [patient information] to Meta because it violates Meta’s contracts for them to be doing  
7 that.”<sup>63</sup>

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

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

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

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

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

23  
24  
25  
26 <sup>62</sup> See Transcript of the Argument on Plaintiff’s Motion for Preliminary Injunction in  
27 *In re Meta Pixel Healthcare Litig.*, Case No. CV-22-03580-WHO (N.D. Cal. Nov. 9,  
28 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).

<sup>63</sup> *Id.* at 7:20-8:11.



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

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

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

12 199. Plaintiffs and Class Members did not realize that tracking Pixels exist  
13 because they are invisibly embedded within Defendant's web pages that users might  
14 interact with.<sup>64</sup> Patients and Users of Defendant's Web Properties do not receive any  
15 alerts during their uses of Defendant's Web Properties stating that Defendant tracks  
16 and shares sensitive medical data with Facebook, allowing Facebook and other third  
17 parties to subsequently target all users of Defendant's website for marketing purposes.

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

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

26  
27 <sup>64</sup> FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel*  
28 *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>.



1 privacy and uses of their Private Information. Furthermore, any person visiting a  
2 health website has a reasonable understanding that medical providers must adhere to  
3 strict confidentiality protocols and are bound not to share any medical information  
4 without their consent.

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

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

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

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

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

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.<sup>65</sup> 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.<sup>66</sup>

<sup>65</sup> 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)

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

**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

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

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

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

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

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

17 216. For example, a recent study by Consumer Reports shows that 92% of  
 18 Americans believe that internet companies and websites should be required to obtain  
 19 consent before selling or sharing consumers' data, and the same percentage believe  
 20 internet companies and websites should be required to provide consumers with a  
 21 complete list of the data that has been collected about them.<sup>67</sup> Moreover, according to  
 22 a study by Pew Research Center, a majority of Americans, approximately 79%, are  
 23 concerned about how data is collected about them by companies.<sup>68</sup>

24 <sup>67</sup> *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New*  
 25 *Survey Finds*, CONSUMER REPORTS (May 11, 2017),  
 26 [https://www.consumerreports.org/consumer-reports/consumers-less-confident-](https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/)  
[about-healthcare-data-privacy-and-car-safety/](https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/).

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

1           217. Users act consistent with these preferences. Following a new rollout of  
2 the iPhone operating software—which asks users for clear, affirmative consent before  
3 allowing companies to track users—85% of worldwide users and 94% of U.S. users  
4 chose not to share data when prompted.<sup>69</sup>

5           218. Medical data is particularly even more valuable because unlike other  
6 personal information, such as credit card numbers which can be quickly changed,  
7 medical data is static. This is why companies possessing medical information, like  
8 Defendant, are intended targets of cyber-criminals.<sup>70</sup>

9           219. Patients using Defendant’s Web Properties must be able to trust that the  
10 information they input including their physicians, their health conditions and courses  
11 of treatment will be protected. Indeed, numerous state and federal laws require this.  
12 And these laws are especially important when protecting individuals with particular  
13 medical conditions such as HIV or AIDS that can and do subject them to regular  
14 discrimination. Furthermore, millions of Americans keep their health information  
15 private because it can become the cause of ridicule and discrimination. For instance,  
16 despite the anti-discrimination laws, persons living with HIV/AIDS are routinely  
17 subject to discrimination in healthcare, employment, and housing.<sup>71</sup>

18           220. The concern about sharing medical information is compounded by the  
19 reality that advertisers view this type of information as particularly high value.  
20 Indeed, having access to the data women share with their healthcare providers allows  
21 advertisers to obtain data on children before they are even born. As one article put it:  
22 “the datafication of family life can begin from the moment in which a parent thinks

23  
24 <sup>69</sup> Margaret Taylor, *How Apple Screwed Facebook*, WIRED (May 19, 2021),  
<https://www.wired.co.uk/article/apple-ios14-facebook>.

25 <sup>70</sup> Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than*  
26 *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>.

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



1 about having a baby.”<sup>72</sup> The article continues, “[c]hildren today are the very first  
 2 generation of citizens to be datafied from before birth, and we cannot foresee — as  
 3 yet — the social and political consequences of this historical transformation. What is  
 4 particularly worrying about this process of datafication of children is that companies  
 5 like . . . Facebook . . . are harnessing and collecting multiple typologies of children’s  
 6 data and have the potential to store a plurality of data traces under unique ID  
 7 profiles.”<sup>73</sup>

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

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

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

22 223. Meta advertises its’ Pixel as a piece of code “that can help you better  
 23 understand the *effectiveness of your advertising* and the actions people take on your  
 24

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

27 <sup>73</sup> *Id.*

28 <sup>74</sup> 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>.

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

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

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

14 226. Through this process, the Meta Pixel loads and captures as much data as  
 15 possible when a User loads a healthcare website that has installed the Pixel. The  
 16 information the Pixel captures, “includes URL names of pages visited, and actions  
 17 taken - all of which could be potential examples of health information.”<sup>77</sup>

18 227. In exchange for disclosing the Private Information of their patients,  
 19 Eisenhower is compensated by Facebook and likely other third parties in the form of  
 20 enhanced advertising services and more cost-efficient marketing on their platform.  
 21  
 22  
 23  
 24

25 <sup>75</sup> *What is the Meta Pixel?*, META, [https://www.facebook.com/business/tools/meta-](https://www.facebook.com/business/tools/meta-pixel)  
 26 [pixel](https://www.facebook.com/business/tools/meta-pixel) (emphasis added) (last visited Apr. 19, 2024).

27 <sup>76</sup> Louis Meletiou, *The complex world of healthcare retargeting*, MEDICO DIGITAL  
 28 (Jul. 10, 2023) [https://www.medicodigital.com/the-complicated-world-of-healthcare-](https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/)  
[retargeting/](https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/).

<sup>77</sup> *Id.*



1           228. But companies have started to warn about the potential HIPAA violations  
2 associated with using pixels and tracking technologies because many are not HIPAA-  
3 complaint or are only HIPAA-compliant if certain steps are taken.<sup>78</sup>

4           229. For example, Freshpaint a healthcare marketing vendor, cautioned that  
5 “Meta isn’t HIPAA-compliant”, and “If you followed the Facebook (or other general)  
6 documentation to set up your ads and conversion tracking using the Meta Pixel,  
7 remove the Pixel now.”<sup>79</sup>

8           230. Medico Digital also warns that “retargeting requires sensitivity, logic and  
9 intricate handling. When done well, it can be a highly effective digital marketing tool.  
10 But when done badly, it could have serious consequences.”<sup>80</sup>

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

13           ***M. Plaintiffs’ & Class Members’ Private Information Has Substantial***  
14           ***Value.***

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

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

---

25           <sup>78</sup> *The guide to HIPAA compliance in analytics*, PIWIK PRO,  
26 [https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-](https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf)  
27 [compliance-in-analytics.pdf](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-  
28 compliant) (last visited Apr. 19, 2024).

<sup>79</sup> *Id.*

<sup>80</sup> *The complex world of healthcare retargeting*, *supra*, note 76.

234. The robust market for Internet user data has been analogized to the “oil” of the tech industry.<sup>81</sup> A 2015 article from TechCrunch accurately noted that “Data has become a strategic asset that allows companies to acquire or maintain a competitive edge.”<sup>82</sup> 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.<sup>83</sup>

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

---

<sup>81</sup> *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>.

<sup>82</sup> Pauline Glikman and Nicolas Gladly, *What’s The Value Of Your Data?*, TECHCRUNCH (Oct. 13, 2015) <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>.

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

1 providers that they must de-identify data and that purchasers and sellers of “such data  
2 should ensure it is priced at fair market value to mitigate any regulatory risk.”<sup>84</sup>

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

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

12 241. Similarly, CNBC published an article in 2019 in which it observed that  
13 “[d]e-identified patient data has become its own small economy: There’s a whole  
14 market of brokers who compile the data from providers and other health-care  
15 organizations and sell it to buyers.”<sup>87</sup>

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

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

24 <sup>85</sup> *Hackers, breaches, and the value of healthcare data*, IMPRIVATA (Jun. 30, 2021)  
25 <https://www.imprivata.com/blog/healthcare-data-new-prize-hackers> (citing *The*  
26 *Value of Data*, [https://www.infopoint-](https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf)  
27 [security.de/media/TrustwaveValue\\_of\\_Data\\_Report\\_Final\\_PDF.pdf](https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf)).

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

<sup>87</sup> 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>.

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

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

6                           **VI. TOLLING, CONCEALMENT & ESTOPPEL**

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

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

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

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

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

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

## 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.

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

6           257. The requirements of Federal Rules of Civil Procedure 23(a), 23(b)(2), and  
7 23(b)(3) are met in this case.

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

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

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

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

23          262. **Adequate Representation:** Plaintiffs will fairly and adequately represent  
24 and protect the interests of the Class Members. Plaintiffs' claims are made in a  
25 representative capacity on behalf of the Class Members. Plaintiffs have no interests  
26 antagonistic to the interests of the other Class Members. Plaintiffs have retained  
27 competent counsel to prosecute the case on behalf of Plaintiffs and the Class.  
28



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

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

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

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

- i. Whether Defendant's acts and practices violated California's Constitution, Art. 1, § 1;
- ii. Whether Defendant's acts and practices violated California's Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*;
- iii. Whether Defendant's acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;
- iv. Whether Defendant's unauthorized disclosure of Users' Private Information was negligent;
- v. Whether Defendant owed a duty to Plaintiffs' and Class Members not to disclose their Private Information to unauthorized third parties;
- vi. Whether Defendant breached its duty to Plaintiffs and Class Members not to disclose their Private Information to unauthorized third parties;
- vii. Whether Defendant represented to Plaintiffs and the Class that it would protect Plaintiff's and the Class Members' Private Information;
- viii. Whether Defendant violated Plaintiffs' and Class Members' privacy rights;
- ix. Whether Defendant's practices violated California's Confidentiality of Medical Information Act, Civ. Code §§ 56, *et seq.*;
- x. Whether Defendant's practices violated California's Constitution, Art. 1, § 1;
- xi. Whether Plaintiffs and Class Members are entitled to actual damages, enhanced damages, statutory damages, and other monetary remedies provided by equity and law;

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

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

1 providers only for the limited purpose of providing access to its  
2 services;

- 3 c. Whether Defendant misrepresented that it had in place contractual  
4 and technical protections that limit third-party use of User  
5 information and that it would seek User consent prior to sharing  
6 Private Information with third parties for purposes other than  
7 provision of its services;
- 8 d. Whether Defendant misrepresented that any information it receives  
9 is stored under the same guidelines as any health entity that is subject  
10 to the strict patient data sharing and protection practices set forth in  
11 the regulations propounded under HIPAA;
- 12 e. Whether Defendant misrepresented that it complied with HIPAA's  
13 requirements for protecting and handling Users' PHI;
- 14 f. Whether Defendant shared the Private Information that Users  
15 provided to Defendant with advertising platforms, including  
16 Facebook, without adequate notification or disclosure, and without  
17 Users' consent, in violation of health privacy laws and rules and its  
18 own privacy policy;
- 19 g. Whether Defendant integrated third-party tracking tools, consisting  
20 of automated web beacons ("**Pixels**") in its website that shared  
21 Private Information and User activities with third parties for  
22 unrestricted purposes, which included advertising, data analytics,  
23 and other commercial purposes;
- 24 h. Whether Defendant shared Private Information and activity  
25 information with Facebook using Facebook's Pixels on its Web  
26 Properties without Users' consent;
- 27  
28

- 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.

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

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

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

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

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

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



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

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

## 7 **COUNT TWO**

### 8 **VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT**

#### 9 **("ECPA")**

#### 10 **18 U.S.C. § 2511(1), et seq.**

#### 11 **Unauthorized Interception, Use, and Disclosure**

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

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

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

16 281. 18 U.S.C. § 2520(a) provides a private right of action to any person whose  
17 wire or electronic communications are intercepted, disclosed, or intentionally used in  
18 violation of Chapter 119.

19 282. The transmissions of Plaintiffs' PII and PHI to Defendant's Web  
20 Properties qualify as "communications" under the ECPA's definition of 18 U.S.C. §  
21 2510(12).

22 283. **Electronic Communications**. The transmission of PII and PHI between  
23 Plaintiffs and Class Members and Defendant's Web Properties with which they chose  
24 to exchange communications are "transfer[s] of signs, signals, writing,...data, [and]  
25 intelligence of [some] nature transmitted in whole or in part by a wire, radio,  
26 electromagnetic, photoelectronic, or photooptical system that affects interstate  
27 commerce" and are therefore "electronic communications" within the meaning of 18  
28 U.S.C. § 2510(2).

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

4           285. Defendant’s intercepted communications include, but are not limited to,  
5 communications to/from Plaintiffs and Class Members regarding PII and PHI,  
6 diagnosis of certain conditions, treatment/medication for such conditions, and  
7 scheduling of appointments, including annual mammograms, surgeries, ER visits, lab  
8 work, and scans. Furthermore, Defendant intercepted the “contents” of Plaintiffs’  
9 communications in at least the following forms:

- 10           a. The parties to the communications;
- 11           b. The precise text of patient search queries;
- 12           c. Personally, identifying information such as patients’ IP addresses,  
13 Facebook IDs, browser fingerprints, and other unique identifiers;
- 14           d. The precise text of patient communications about specific doctors;
- 15           e. The precise text of patient communications about specific medical  
16 conditions;
- 17           f. The precise text of information generated when patients requested or  
18 made appointments,
- 19           g. The precise text of patient communications about specific  
20 treatments;
- 21           h. The precise text of patient communications about scheduling  
22 appointments with medical providers;
- 23           i. The precise text of patient communications about billing and  
24 payment;
- 25           j. The precise text of specific buttons on Defendant’s Web Properties  
26 that patients click to exchange communications, including Log-Ins,  
27 Registrations, Requests for Appointments, Search, and other  
28 buttons;

- k. The precise dates and times when patients click to Log-In on Defendant's Web Properties;
- l. The precise dates and times when patients visit Defendant's Web Properties;
- m. Information that is a general summary or informs third parties of the 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).

1           289. Specifically, Defendant intercepted Plaintiffs’ and Class Members’  
2 electronic communications via the Pixel, which tracked, stored, and unlawfully  
3 disclosed Plaintiffs’ and Class Members’ Private Information to third parties such as  
4 Facebook.

5           290. Defendant’s intercepted communications include, but are not limited to,  
6 communications to/from Plaintiffs and Class Members regarding PII and PHI,  
7 treatment, medication, and scheduling.

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

12           292. By intentionally disclosing or endeavoring to disclose the electronic  
13 communications of Plaintiffs and Class Members to affiliates and other third parties,  
14 while knowing or having reason to know that the information was obtained through  
15 the interception of an electronic communication in violation of 18 U.S.C. §  
16 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

17           293. By intentionally using, or endeavoring to use, the contents of the  
18 electronic communications of Plaintiffs and Class Members, while knowing or having  
19 reason to know that the information was obtained through the interception of an  
20 electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated  
21 18 U.S.C. § 2511(1)(d).

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

26           295. The ECPA provides that a “party to the communication” may liable where  
27 a “communication is intercepted for the purpose of committing any criminal or  
28

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

3 296. Defendant is not a party for purposes to the communication based on its  
4 unauthorized duplication and transmission of communications with Plaintiffs and the  
5 Class. However, even assuming Defendant is a party, Defendant’s simultaneous,  
6 unknown duplication, forwarding, and interception of Plaintiffs’ and Class Members’  
7 Private Information does not qualify for the party exemption.

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

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

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

25 299. Defendant’s conduct violated 42 U.S.C. § 1320d-6 in that it: Used and  
26 caused to be used cookie identifiers associated with specific patients without patient  
27 authorization; and disclosed individually identifiable health information to Facebook  
28 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.

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,



1 healthcare providers and locations, medications and treatments, and  
 2 health insurance and medical bills) for commercial purposes has  
 3 caused Plaintiffs and the Class Members to suffer emotional  
 4 distress;

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

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

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

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

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

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

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

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

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

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

- 11           A. the false and misleading statements and omissions in its privacy  
12 policy set forth above, including the statements and omissions  
13 recited in the claims below;
- 14           B. the placement of the 'fbp' cookie on patient computing devices  
15 disguised as a first-party cookie on Defendant's Website rather than  
16 a third-party cookie from Facebook.

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

- 19           A. property rights to the confidentiality of Private Information and their  
20 right to determine whether such information remains confidential  
21 and exclusive right to determine who may collect and/or use such  
22 information for marketing purposes; and
- 23           B. property rights to determine who has access to their computing  
24 devices.

25          313. In sending and in acquiring the content of Plaintiffs' and Class Members'  
26 communications relating to the browsing of Defendant's Web Properties, Defendant's  
27 purpose was tortious, criminal, and designed to violate federal and state legal  
28

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,

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

3 C. “uses, or attempts to use, in any manner, or for any purpose, or to  
4 communicate in any way, any information so obtained,” or

5 D. **aids, agrees with, employs, or conspires with any person or persons**  
6 **to unlawfully do, or permit, or cause to be done any of the acts or**  
7 **things mentioned above in this section**” (emphasis added).

8 318. Section 631(a) is not limited to phone lines, but also applies to “new  
9 technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*,  
10 2016 WL 8200619, at \*21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new  
11 technologies” and must be construed broadly to effectuate its remedial purpose of  
12 protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at \*5-6 (N.D. Cal.  
13 Dec. 22, 2006) (CIPA governs “electronic communications”); *In re Facebook, Inc.*  
14 *Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of  
15 CIPA and common law privacy claims based on Facebook’s collection of consumers’  
16 Internet browsing history).

17 319. Defendant’s Web Properties are a “machine, instrument, contrivance, or  
18 . . . other manner” used to engage in the prohibited conduct at issue here.

19 320. At all relevant times, Defendant entered into contracts with Facebook, in  
20 order to track certain activities on its Web Properties. Defendant allowed Facebook  
21 to intercept and otherwise track Users’ clicks, communications, searches, and other  
22 User activities.

23 321. Defendant activated Facebook Pixel tracking tools, allowing Facebook to  
24 intentionally tap, and make unauthorized connections with, the lines of internet  
25 communication between Plaintiffs and California Subclass Members on the one hand,  
26 and Defendant’s Web Properties on the other hand, without consent of all parties to  
27 the communication.  
28

1           322. At all relevant times, by using the Facebook Pixel, Facebook willfully  
2 and without the consent of Plaintiffs and California Subclass Members, read or  
3 attempted to learn the contents or meaning of electronic communications of Plaintiffs  
4 and putative California Subclass Members on Defendant's Web Properties. This  
5 occurred while the electronic communications were in transit or passing over any  
6 wire, line, or cable, or were being sent from or received at any place within California.  
7 Facebook intercepted Plaintiffs' and California Subclass Members' communications  
8 – including the very terms and phrases they typed into the search bar – without their  
9 authorization or consent.

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

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

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

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

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

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

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

- 9 a. The parties to the communications;
- 10 b. The precise text of patient search queries;
- 11 c. Personally identifying information such as patients' IP addresses,  
12 Facebook IDs, browser fingerprints, and other unique identifiers;
- 13 d. The precise text of patient communications about specific doctors;
- 14 e. The precise text of patient communications about specific medical  
15 conditions;
- 16 f. The precise text of information generated when patients requested  
17 or made appointments;
- 18 g. The precise text of patient communications about specific  
19 treatments;
- 20 h. The precise text of patient communications about scheduling  
21 appointments with medical providers;
- 22 i. The precise text of patient communications about billing and  
23 payment;
- 24 j. The precise text of specific buttons on Defendant's Webs  
25 Properties that patients click to exchange communications,  
26 including Log-Ins, Registrations, Requests for Appointments,  
27 Search, and other buttons;
- 28



- 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

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

1 protection and limitation on the use of the Private Information. Meanwhile, Defendant  
2 was collecting and sharing Plaintiffs' and Nationwide Class Members' Private  
3 Information without their authorization or knowledge to profit off of the information,  
4 and deliver targeted advertisements to Plaintiffs and Nationwide Class Members,  
5 among other unlawful purposes.

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

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

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

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

23 342. As a result of Defendant's unlawful conduct, Plaintiffs and Nationwide  
24 Class Members suffered an injury, including violation to their rights of privacy, loss  
25 of value and privacy of their Private Information, loss of control over their sensitive  
26 personal information, and suffered embarrassment and emotional distress as a result  
27 of this unauthorized sharing of information.  
28

**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

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

3 351. Defendant's acts, omissions and conduct also violate the unfair prong of  
4 the UCL because those acts, omissions and conduct offended public policy (including  
5 the aforementioned federal and state privacy statutes and state consumer protection  
6 statutes, such as HIPAA), and constitute immoral, unethical, oppressive, and  
7 unscrupulous activities that caused substantial injury, including to Plaintiffs and  
8 Nationwide Class Members.

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

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

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

27 ///

28 ///

**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.



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

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

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

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

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

18           366. Plaintiffs and California Subclass Members are also entitled to punitive  
19 damages resulting from the malicious, willful, and intentional nature of the  
20 Defendant’s conduct, injuring Plaintiffs and California Subclass Members in  
21 conscious disregard of their rights.

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

25 ///

26 ///

27 ///

28 ///

**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.

1           374. Defendant’s privacy policy specifically provides, “We will not sell, trade  
2 or rent your personal information to other people or businesses unless we have your  
3 consent.”<sup>88</sup>

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

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

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

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

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

26 ///

27 ///

28           <sup>88</sup> *Notice of Privacy Policy, supra* note 40.

**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

1 made these false representations. Defendant profited directly from these sales,  
2 including through payment for these services, and from the Private Information  
3 disclosed and intercepted.

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

## 8 **COUNT EIGHT**

### 9 **LARCENY/RECEIPT OF STOLEN PROPERTY (VIOLATION OF**

#### 10 **CALIFORNIA PENAL CODE § 496(a) and (c)**

#### 11 ***(On behalf of Plaintiffs and the California Subclass)***

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

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

25 390. Cal. Penal Code §496(c) permits "any" person who has been injured by  
26 a violation of section 496(a) to recover three times the amount of actual damages,  
27 costs of suit and attorney's fees in a civil suit.  
28

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

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

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

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

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

18           395. Defendant violated the second ground for liability of section  
19 496(a) because it:

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

25           396. As a direct and proximate result of the acts and omissions described  
26 above, Plaintiffs and California Subclass Members were injured by the Defendant’s  
27 violations of section 496(a).  
28



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

## BREACH OF CONFIDENCE

6

7  
8

9  
10

11  
12  
13

14  
15  
16

17  
18  
19  
20

21  
22

23  
24  
25

26  
27  
28

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

- 5           a. Sensitive and confidential information that Plaintiffs and Class  
6 Members intended to remain private is no longer private;
- 7           b. Defendant eroded the essential confidential nature of the provider-  
8 patient relationship;
- 9           c. Defendant took something of value from Plaintiffs and Class  
10 Members and derived benefit therefrom without Plaintiffs' and Class  
11 Members' knowledge or informed consent and without  
12 compensating Plaintiffs and Class Members for the data;
- 13           d. Plaintiffs and Class Members did not get the full value of the medical  
14 services for which they paid, which included Defendant's duty to  
15 maintain confidentiality;
- 16           e. Defendant's actions diminished the value of Plaintiffs' and Class  
17 Members' Private Information; and
- 18           f. Defendant's actions violated the property rights Plaintiffs and Class  
19 Members have in their Private Information.

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

## 24           **COUNT TEN**

### 25           **BREACH OF FIDUCIARY DUTY**

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

27           408. Plaintiffs repeat the allegations contained in the paragraphs above as if  
28 fully set forth herein.

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

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

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

15           412. As a direct and proximate result of Defendant' breach of its fiduciary  
16 duties, Plaintiffs and Class Members have suffered and will continue to suffer injury  
17 and are entitled to compensatory, nominal, and/or punitive damages, and  
18 disgorgement of profits, in an amount to be proven at trial.

19                           **COUNT ELEVEN**

20                           **UNJUST ENRICHMENT**

21                           ***(On behalf of Plaintiffs and Nationwide Class)***

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

24           414. Plaintiffs and Class Members personally and directly conferred a benefit  
25 on Defendant by paying Defendant for health care services, which included  
26 Defendant's obligation to protect Plaintiffs' and Class Members' Private Information.  
27 Defendant was aware of Plaintiffs' privacy expectations, and in fact, promised to  
28 maintain Plaintiffs' Private Information confidential and not to disclose to third

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

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

12 416. Plaintiffs and Class Members would not have used Defendant's Web  
13 Properties had they known that Defendant would collect, use, and disclose this  
14 information to Facebook, Google, and other third parties. The services that Plaintiffs  
15 and Class Members ultimately received in exchange for the monies paid to Defendant  
16 were worth quantifiably less than the services that Defendant promised to provide,  
17 which included Defendant's promise that any patient communications with  
18 Defendant would be treated as confidential and would never be disclosed to third  
19 parties for marketing purposes without the express consent of patients.

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

26 418. By virtue of the unlawful, unfair and deceptive conduct alleged herein,  
27 Defendant knowingly realized hundreds of millions of dollars in revenue from the use  
28 of the Private Information of Plaintiffs and Classes Members for profit by way of

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

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

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

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

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

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

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

## 23 **VIII. PRAYER FOR RELIEF**

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

26 A. That this Action be maintained as a Class Action, that Plaintiffs be  
27 named as Class Representative of the Class, that the undersigned be  
28

1 named as Lead Class Counsel of the Class, and that notice of this Action  
2 be given to Class Members;

3 B. That the Court enter an order:

- 4 a. Preventing Defendant from sharing Plaintiffs' and Class  
5 Members' Private Information among other third parties;
- 6 b. Requiring Defendant to alert and/or otherwise notify all users  
7 of its websites and portals of what information is being  
8 collected, used, and shared;
- 9 c. Requiring Defendant to provide clear information regarding  
10 its practices concerning data collection from the users/patients  
11 of Defendant's Web Properties, as well as uses of such data;
- 12 d. Requiring Defendant to establish protocols intended to  
13 remove all personal information which has been leaked to  
14 Facebook and/or other third parties, and request  
15 Facebook/third parties to remove such information;
- 16 e. Requiring Defendant to provide an opt out procedures for  
17 individuals who do not wish for their information to be  
18 tracked while interacting with Defendant's Web Properties;
- 19 f. Mandating the proper notice be sent to all affected individuals,  
20 and posted publicly;
- 21 g. Requiring Defendant to delete, destroy, and purge the Private  
22 Information of Users unless Defendant can provide reasonable  
23 justification for the retention and use of such information  
24 when weighed against the privacy interests of Users;
- 25 h. Requiring all further and just corrective action, consistent with  
26 permissible law and pursuant to only those causes of action so  
27 permitted.  
28



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

17 **IX. JURY TRIAL DEMANDED**

18 Plaintiffs demand a jury trial on all triable issues.

19  
20 DATED: April 22, 2024

**CLARKSON LAW FIRM, P.C.**

21 /s/ Yana Hart  
22 Ryan Clarkson, Esq.  
23 Yana Hart, Esq.  
24 Tiara Avanness, Esq.

**ALMEIDA LAW GROUP LLC**

25 /s/ John R. Parker, Jr.  
26 John R. Parker, Jr. (SBN 257761)  
27  
28