RACHELE R. BYRD (190634)
FERDEZA ZEKIRI (335507)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4559
Facsimile: (619) 234-4599
byrd@whafh.com
zekiri@whafh.com
Attorneys for Plaintiff

SUPERIOR COURT OF THE STATE OF CALIFORNIA

IN AND FOR THE COUNTY OF LOS ANGELES

JOHN DOE, on behalf of himself and all others similarly situated,

Plaintiff,

v.

CEDARS-SINAI HEALTH SYSTEM and CEDARS-SINAI MEDICAL CENTER,

Defendants.

Case No. 22STCV41085

CLASS ACTION COMPLAINT FOR:

1. **Violations of the California Invasion of Privacy Act (Cal. Penal Code §§ 630, 631, *et seq.*);**
2. **Violations of the California Invasion of Privacy Act (Cal. Penal Code § 632, *et seq.*);**
3. **Invasion of Privacy/Intrusion Upon Seclusion – California Constitution and Common Law;**
4. **Breach of Implied Contract;**
5. **Breach of Contract -- Third Party Beneficiaries;**
6. **Breach of Implied Covenant of Good Faith and Fair Dealing;**
7. **Negligence;**
8. **Violations of California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq.*);**
9. **Violations of the Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, *et seq.*)**

CLASS ACTION

JURY TRIAL DEMANDED

Plaintiff John Doe ("Plaintiff") brings this class action complaint against Cedars-Sinai Health System and Cedars-Sinai Medical Center (collectively, "Cedars-Sinai" or "Defendant") on behalf of himself and all others similarly situated. Plaintiff alleges, upon personal knowledge as to his own actions and upon his counsel's investigation and information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Defendant Cedars-Sinai is a major healthcare organization based in Los Angeles, California. It maintains a website and a mobile application or "app" (together, the "Website") through which it communicates with its more than one million patients.[1] It encourages patients to use this Website to research their medical symptoms and health issues, identify doctors who can treat their specific conditions, make appointments with those doctors, and take other actions related to their personal health care. When doing this, patients convey highly private information, including medical information, through the Website.

2. Plaintiff and all other members of the proposed class (defined *infra*) are patients who communicated with Cedars-Sinai through its Website. They shared information, including their Protected Health Information ("PHI") and Personally Identifiable Information ("PII"),[2] with the reasonable belief that Cedars-Sinai would take appropriate steps to maintain the privacy of these communications.

3. Instead, Cedars-Sinai took the opposite course. Without these patients' knowledge or consent, Defendant shared their Private Information with unrelated companies including Facebook/Meta,[3] Google, Microsoft Bing, and other marketing and social media platforms or businesses.

---

[1] *See* https://www.cedars-sinai.org/about.html (last visited Dec. 29, 2022). The home page of this Website can be found at https://www.cedars-sinai.org/. Through it, one can reach Cedars-Sinai's patient portal, the home page of which is https://www.cedars-sinai.org/mycslink.html.

[2] This information is collectively and severally referred to as "Private Information."

[3] In October 2021, Facebook, Inc. changed its name to Meta, Inc. Unless otherwise indicated, Facebook, Inc. and Meta, Inc. are referenced collectively herein as "Meta."

4. Cedars-Sinai transmitted to third parties portions of the patients' private communications with it through pieces of tracking code that it embedded in its Website, for the sole purpose of sharing such information with marketing entities. This code served as real time wiretaps on patients' communications.

5. Cedars-Sinai's goal in installing the tracking code was not to provide any benefit to its patients but only to itself. Cedars-Sinai installed the tracking code to obtain insight about how its patients and potential patients use its Website.

6. By installing the tracking code, moreover, Cedars-Sinai enabled the marketing entities to use patients' Private Information to target them with advertising by yet other, unrelated businesses. By way of illustration, if a patient made an appointment with a doctor for treatment of cancer, the tracking code Cedars-Sinai put on its Website conveyed that information to Meta, which in turn allowed Meta to include that patient in marketing target groups that it offered to its other advertising clients who wanted to market to cancer patients.

7. Cedars-Sinai's conduct in sharing patients' health information and other personally identifiable information violates an array of laws and duties. Plaintiff thus sues, on behalf of himself and a class of all persons who used Defendant's Website at any time when tracking code able to share data with third parties for marketing or web-site analytics purposes was present on the Website (the "Class"), seeking remedies for: violations of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631, *et seq.* and the privacy rights protected by California's Constitution and common law; breaches of implied contractual promises by Cedars-Sinai; breach of Cedars-Sinai's contract with Meta, of which Class members are third-party beneficiaries; violation of California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.*; violation of California's Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq.*; and other tortious acts as described herein.

II. JURISDICTION & VENUE

8. This Court has jurisdiction over this action under California Code of Civil Procedure § 410.10. The total amount of damages incurred by Plaintiff and the Class in the

aggregate exceeds the $25,000 jurisdictional minimum of this Court. Further, the amount in controversy as to Plaintiff individually does not exceed $75,000.

9. This Court has jurisdiction over Defendant because it is located within Los Angeles County, California.

10. This action does not qualify for federal jurisdiction under the Class Action Fairness Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies to this action because (1) more than two-thirds of the members of the proposed Class are citizens of the State of California, and (2) Defendant is a citizen of the State of California.

11. Venue is proper in this Court under California Bus. & Prof. Code § 17203 and Code of Civil Procedure §§ 395(a) and 395.5 because Defendant is headquartered within this Court's jurisdiction and because a substantial part of the events giving rise to Plaintiff's claims occurred in this County.

III. PARTIES

12. Plaintiff John Doe is a resident of the City of Los Angeles, California. Plaintiff is a healthcare consumer who used Defendant's Website, https://www.cedars-sinai.org/, including its patient portal available through the Website, My CS-Link, to communicate personal medical information to Defendant. Defendant wrongfully shared Plaintiff's personal information, including private medical information, without Plaintiff's knowledge or consent.

13. Plaintiff Doe is also a Facebook user who has used the "Keep Me Logged In" feature of his Facebook account. He has noticed an increase in the number of health related ads that he has received and he has received ads relating to the condition about which he communicated on Defendant's Website.

14. Defendant Cedars-Sinai Medical Center is a private non-profit healthcare organization headquartered in Los Angeles, California.[4] According to publicly available sources,

[4] Cedars Sinai, ABOUT US, https://www.cedars-sinai.org/about.html?s_kwid=&&origin=sitelink&gclid=CjwKCAjwwdWVBhA4EiwAjcYJECi4Wk4AtxtCGg0bqj7uO8Eh4YM8Iv8sVqvH2Yu6qpyj9q4Bj4--oBoCHQ4QAvD_BwE&gclsrc=aw.ds (last visited Dec. 28, 2022).

it generated over $3.8 billion in revenue in 2020.[5]

15. Defendant Cedars-Sinai Health System is a California non-profit corporation and the parent organization of Cedars-Sinai Medical Center. Cedars-Sinai Health System is the sole corporate member of Cedars-Sinai Medical Center. The Website states that "[t]he Cedars-Sinai Health System ("CSHS") website is owned and operated by Cedars-Sinai Health System."[6]

IV. STATEMENT OF FACTS

A. Cedars-Sinai's Inclusion of Tracking Codes on Its Website

16. Defendant Cedars-Sinai is a Los Angeles health services organization which sees over a million patients per year.[7] One of its primary means of communication with those patients is through its Website. In a brazen violation of law and of its own promises, it embedded code on its Website designed to facilitate eavesdropping by Meta and other unrelated third parties.

17. The home page of Cedars-Sinai's Website provides highly visible links that encourage visitors to "Become a Patient," "Make an appointment," "Find a Doctor," use the "Health Library," log into the patient portal, My CS-Link, and take other actions. Use of these links can require patients to transmit information about: the specialty, gender and location of doctors they are seeking; their own or their family members' medical conditions; and/or take other actions that necessarily transmit significant private information.

18. What was not visible on the Website, although Cedars-Sinai placed it there, was tracking code that transmitted patients' selections and actions on the Website to Meta, Google and other entities that provide marketing services to Cedars-Sinai.

19. Defendant shared patients' communications with at least the following third parties: Meta, Google, Microsoft (Bing), Broadcastmed.innocraft.cloud (a healthcare media company) and Marketo (an automated marketing services entity). On information and belief,

---

[5] ProPublica, CEDARS-SINAI MEDICAL CENTER, https://projects.propublica.org/nonprofits/organizations/951644600 (last visited Dec. 28, 2022).

[6] *See* https://www.cedars-sinai.org/privacy-policy.html#:~:text=The%20Cedars-Sinai%20Health%20System%20%28%22CSHS%22%29%20website%20is,owned%20and%20operated%20by%20Cedars-Sinai%20Health%20System (last visited Dec. 29, 2022).

[7] Cedars Sinai, ABOUT US, https://www.cedars-sinai.org/about.html (last visited Dec. 28, 2022).

each of these offered marketing, rather than any medically-related, services and none had any right to patients' data.

20. At some point between July 6 and July 10, 2022, Cedars-Sinai removed Meta's code from its Website, but the harm has already been done. Moreover, other marketing tracking code from, for example, Google and Microsoft, remains.

21. Plaintiff and Class members never consented, agreed to, authorized, or otherwise permitted Defendant to disclose any of their Private Information to any of these entities.

B. Types of Tracking Code Through Which Defendant Shared Private Patient Information

1. The Meta Pixel

22. In order to increase its advertising revenue, Meta, the world's largest and most profitable social networking company, devises tools to identify which users may be interested in specific products, which allows it to enable its advertising clients to target their advertising to particular groups with those interests. One such tool is the "Meta Pixel" (formerly known as the "Facebook Pixel" and referred to herein as the "Pixel"), a piece of code written by Meta to enable itself and its business customers to track and share data about customer transactions.

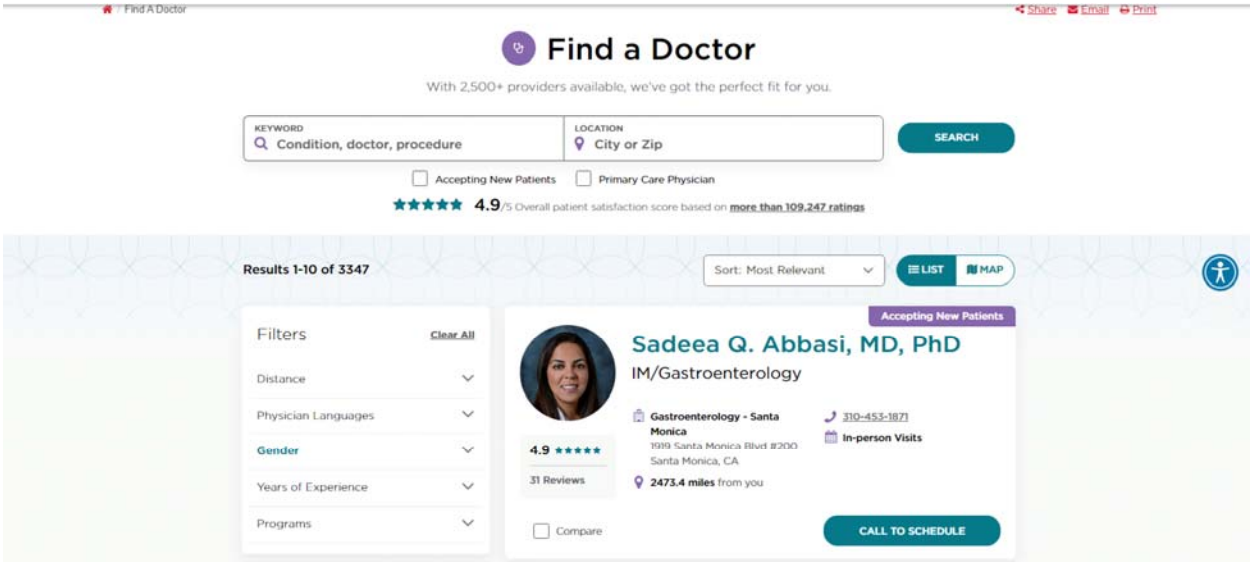
23. Cedars-Sinai chose to include the Pixel on its Website.

24. While the Pixel was on the Website, when a patient entered the following information, the information would simultaneously be shared with Meta:

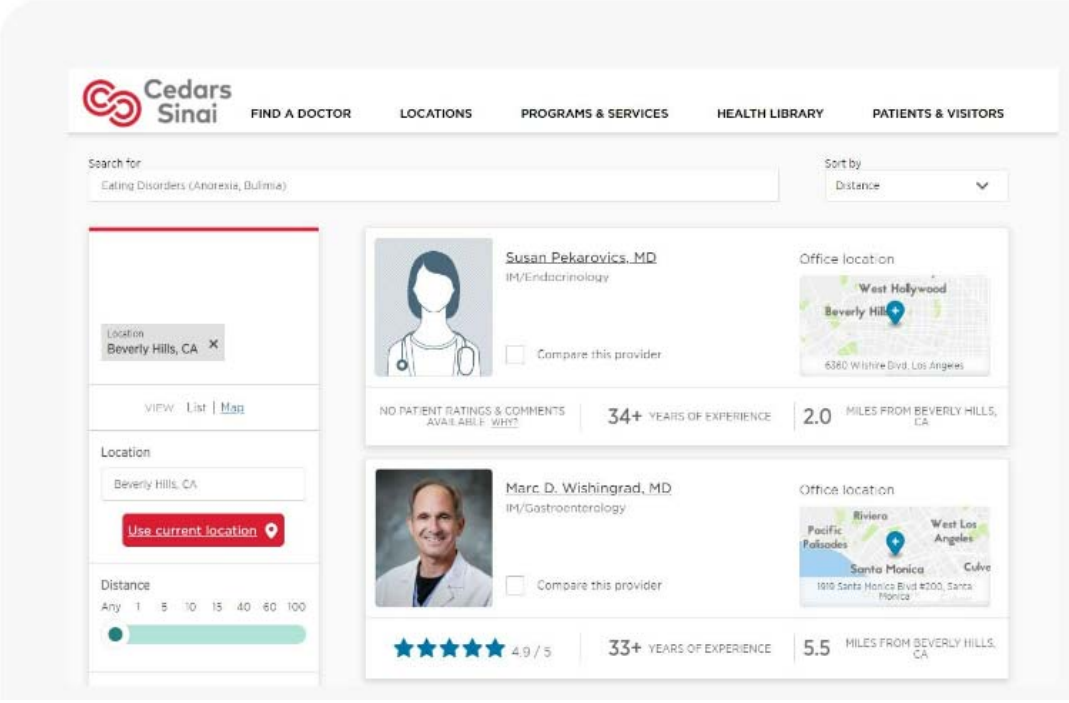
- The types of medical treatment the patient sought;
- The name, gender, language, and specialty of the physician(s) that the patient specified when seeking treatment;
- The patient's searches relating to COVID-19 information and treatment;
- The locations where the patient sought treatment; and
- That a patient clicked to make a telephone call in order to schedule an appointment through the site.

25. By way of illustration, if a patient selected the "Find a Doctor" button on the main page of Defendant's Website, they would be directed to a page where they could search for

doctors by using keywords such as condition, specialty, or by name, gender, location and language, among other things, as shown below.



26. As the patient submitted their search, the terms of the search would be simultaneously transmitted to Meta. The patient would then be directed to a search results page, like the one shown below:



27. When the patient then selected a doctor on this page by clicking on the link for that doctor, the fact of that selection was simultaneously transmitted to Meta.

28. If the patient then clicked on a button to call the doctor's office and make an appointment, because of the Pixel, Meta would immediately receive notification of that click, before the transmission of the communication to Defendant was complete.

29. Meta's own documentation makes clear just how much tracking of private information the Pixel does. It describes the Pixel as code that Meta's business customers can put on their website to "[m]ake sure your ads are shown to the right people. ***Find … people who have visited a specific page or taken a desired action on your website***." (Emphasis added.)[8]

30. Meta instructs such business customers that:

> 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 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***.[9]

31. Of course, in the healthcare context, it is medical specialists that users "add to their shopping cart." They make doctor's appointments rather than making purchases.

32. The Pixel code enables Meta not only to help Cedars-Sinai with advertising to its own patients outside the Cedars-Sinai Website, but also to include individual patients among groups targeted by ***other*** Meta advertisers relating to the conditions about which patients communicated on Cedars-Sinai's Website.

33. In other words, Meta sells advertising space by highlighting its ability to target users.[10] Meta can target users so effectively because it surveils user activity both on and off its

---

[8] Meta, ABOUT META PIXEL https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Dec. 28, 2022).

[9] *Id*. (Emphasis added.)

[10] Meta, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706 (last visited Dec. 28, 2022).

site.[11] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[12]

34. Meta's Business Help Center explains:

> Meta ***uses marketing data to show ads to people who are likely to be interested in them***. One type of marketing data is website events, which are ***actions that people take on your website***.[13]

35. Meta's Terms and Conditions for Data Processing instructs businesses like Cedars-Sinai that Meta may correlate the data business customers provide with individual Facebook users:

> You may provide Event Data to improve ad targeting and delivery optimization of your ad campaigns. ***We may correlate that Event Data to people who use Facebook Company Products*** to support the objectives of your ad campaign, improve the effectiveness of ad delivery models, and determine the relevance of ads to people. ***We may use Event Data to personalize the features and content (including ads and recommendations) that we show people on and off our Facebook Company Products.***[14]

36. One service that Meta provides using the data obtained through the Pixel is "Core Audiences." This allows advertisers to select highly specific filters and parameters, such as demographics, behavior and interests, which Meta will use in directing their targeted advertisements.[15]

---

[11] Meta, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Dec. 29, 2022).

[12] Meta, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Dec. 29, 2022).

[13] Meta, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (emphasis added) (last visited Dec. 29, 2022).

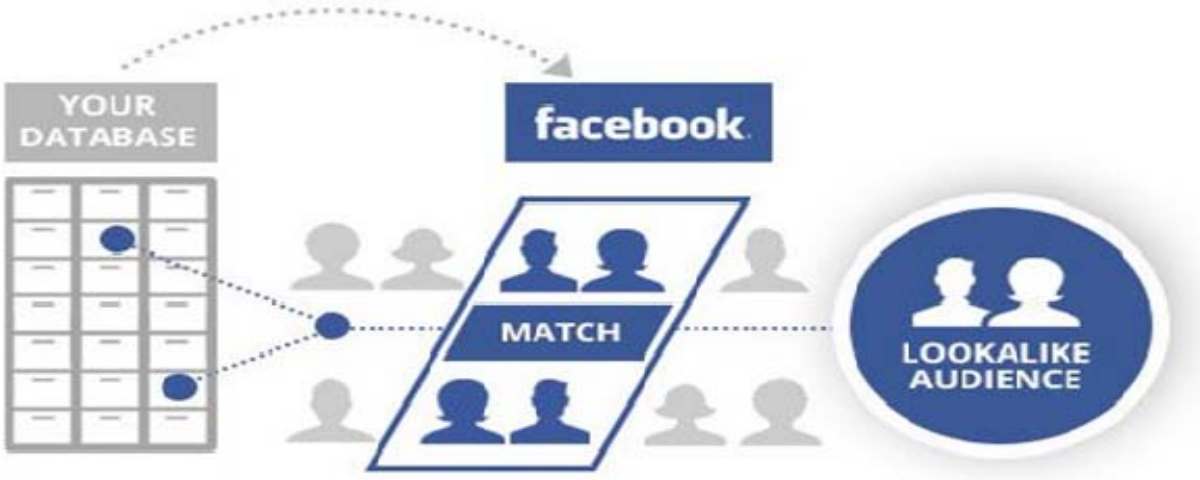
[14] Facebook, FACEBOOK BUSINESS TOOLS TERMS, https://m.facebook.com/legal/technology_terms?locale=ne_NP&_rdr (emphasis added) (last visited Dec. 29, 2022).

[15] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting#:~:text=Core%20AudiencesDefine%20an%20audience,your%20business%2C%20online%20or%20off (last visited Dec. 29, 2022).

37. Another of the services that Meta offers to companies that pay it for advertising is "Lookalike Audiences." That service relies on information that Meta obtains about end users, like Class members, based on their usage of websites, like Defendant's Website, where advertising customers, like Defendant, install Meta's code. As Oberlo explains:

> One of the great things about Meta advertising is "Lookalike Audiences." You can design Lookalike Audiences to reflect the characteristics of your best customers.
>
> ***The code knows who did what on your website, and the Facebook platform can use that data to identify people who share similar traits as your visitors***. So if your "Big spenders" segment is full of 25-35 year old females who live in urban areas, ***Facebook can create a Lookalike Audience of other*** 25-35 year old females who live in urban areas and ***who Facebook thinks might be interested in your products***.[16]

The process has been illustrated as follows:[17]



38. Again, in the healthcare context, instead of tracking customers, the Pixel tracks patients, and instead of shopping preferences it tracks medical concerns.

---

[16] Oberlo, A COMPLETE GUIDE TO FACEBOOK TRACKING FOR BEGINNERS, https://www.oberlo.com/blog/facebook-pixel (emphasis added) (last visited Dec. 29, 2022).

[17] Instapage, WHAT IS THE META PIXEL AND WHAT DOES IT DO?, https://instapage.com/blog/meta-pixel (last visited Dec. 29, 2022).

39. The foregoing all demonstrates that Meta can and does use unique patient information to facilitate the targeting of individuals like Plaintiff and all other Class members, whose personal information is sent to Meta – as Cedars-Sinai sent it – through the Pixel.

40. The ready availability of this information on Meta's business pages also demonstrates that Defendant knew or was reckless in not knowing about this transmission and information before it installed the Pixel on its Website.

41. In terms of technology, the Pixel is JavaScript code that sends Meta a collection of data whenever a person interacts in certain ways with a website. When a user selects a URL or clicks a button on a website, the browser sends a "GET Request" to the server, requesting that a particular webpage be loaded. When a user accesses a website hosting the Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Website—Defendant's own code, and Facebook's embedded code that Defendant placed there.

42. Again, an example illustrates the point. Take an individual who navigates to Defendant's Website and clicks on a tab for eating disorder information. When that tab is clicked, the individual's browser sends a GET request to Defendant's server requesting that server to load the particular webpage. Because Cedars-Sinai utilizes the Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual that this is happening. Facebook causes the browser to secretly duplicate the communication with Cedars-Sinai, transmitting it to Facebook's servers, alongside additional information that transcribes the key elements of the communication's content and the individual's identity.

43. After collecting and intercepting this information, Meta processes it, analyzes it, and assimilates it into datasets including Core Audiences and Lookalike Audiences.

44. Moreover, for any user that was a Facebook member and used Facebook on the same browser as they used the Website and had not logged out from Facebook, or used the commonly used "Keep Me Logged In" feature, the Pixel would transmit that individual's "c_user" number to Meta. A "c_user" number includes the user's unique Facebook identification number, which Meta uses to link an individual's activities and communications, including those on other websites like Cedars-Sinai's, to the user's identity and Meta account.[18]

45. Here, when a patient transacted with Defendant's Website, due to the Pixel, an HTTP single communication session would be sent automatically from the patient's device to Meta. That communication revealed the provider information the patient is searching for, along with the patient's Facebook identification (c_user field).

46. It is alarmingly easy to identify a person by their user identification number. Facebook states that the user ID can, "[a]llow someone with the ID to see your profile, including any public information."[19] Indeed, as detailed on the website Techwalla, "if you have someone's ID number and want to map it to a profile, you can go to www.facebook.com/[id-number], replacing "id-number" with the person's Facebook ID. When you have access to the profile, you'll see the profile page including the person's name they used when registering with Facebook."[20]

47. That means that the private medical information a person enters onto Defendant's Website that is transferred with their c_user code can be easily linked to the person themselves.

48. For example, when someone searches on Defendant's Website for a doctor who specializes in eating disorders, who is male, who is located near Beverly Hills, code is generated

---

[18] Medium, Seralahthan, FACEBOOK COOKIES ANALYSIS, https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a#:~:text=browser%20session%20ends.-,%E2%80%9Cc_user%E2%80%9D,after%2090%20days%20of%20inactivity ("The c_user cookie contains the user ID of the currently logged in user.") (last visited Dec. 29, 2022).

[19] Facebook, HOW USERNAMES AND USER IDS ARE USED ON FACEBOOK PROFILES, https://www.facebook.com/help/211813265517027 (last visited Dec. 29, 2022).

[20] Techwalla, HOW TO FIND A PERSON FROM THEIR FACEBOOK ID, https://www.techwalla.com/articles/how-to-find-a-person-from-their-facebook-id (last visited Dec. 29, 2022).

that transmits to Facebook: the doctor's name, the search terms "Eating disorders," "anorexia" and "bulimia," and the patient's unique Meta identifier, the c_user number.

49. The code generated by such a search also includes the "fbp" cookie, which can be an indicator that the Facebook Pixel is present on the Website.

50. The code generated by such a search also includes a "datr" cookie. This is a cookie that Meta uses to identify the web browser through which the user is communicating. It is a unique identifier and thus another means to identify individual users.

51. The search code also reflects an "fr" cookie. This is a Meta identifier that is an encrypted combination of the c_user and datr cookies.

52. By incorporating the code into its Website, Defendant facilitated this eavesdropping by Meta on patient communications.

53. On information and belief, Defendant also included the Pixel on its password protected portal, My CS-Link.

54. Cedars-Sinai included the Pixel on its Website despite knowing that it would allow Meta to identify individual users' communications containing PII and PHI.

2. Google Analytics Tracking Code

55. Cedars-Sinai also uses "Google Analytics," a web analytics service that allows website owners to track visitor actions on the Website and target them with personalized advertisements. The code for Google Analytics is still on Defendant's Website as of the filing of this Complaint. The code is both on the main pages and on those accessed after a user enters a user name and password. Google tracking code is also present when a person performs the same functions through Cedars-Sinai's smartphone app, as well as through the Website.

56. Google's Analytics Help pages instruct health care providers like Defendant:

> Google does not intend uses of Google Analytics to create obligations under the Health Insurance Portability and Accountability Act, as amended, ("HIPAA"), and makes no representations that Google Analytics satisfies HIPAA requirements. ***If you are (or become) a Covered Entity or Business Associate***

under HIPAA, you may not use Google Analytics for any purpose or in any manner involving Protected Health Information.[21]

57. Despite the above warning, Defendant embedded Google Analytics code on is Website.

58. Google Analytics collects IP addresses of individual Internet users to facilitate and track Internet communications. It also collects various cookie-related user identifiers that allow it to link transactions on websites to individual users for the purpose of targeted advertising.

59. The data is connected to the user's IP address, which is a unique address that identifies a device on the internet. IP addresses constitute personally identifiable information.

60. For example, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") characterizes IP addresses as "direct identifiers," 45 C.F.R. § 164.514(e)(2)(B)(2)(xiv), and provides that "[a] covered entity may determine that health information is not individually identifiable health information if; … (2)(i) [t]he following identifiers of the individual or of relatives, employers, or household members of the individual, are removed: … (O) Internet Protocol (IP) address numbers." 45 C.F.R. § 164.514(b)(2)(i)(O). The only alternative to the removal of such information is that: "[a] person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) [a]pplying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (ii) [d]ocuments the methods and results of the analysis that justify such determination." *Id.* at 45 C.F.R. § 164.514(b). On information and belief, these standards were not met here.

[21] Google, ANALYTICS HELP, BEST PRACTICES TO AVOID SENDING PERSONALLY IDENTIFIABLE INFORMATION (PII), https://support.google.com/analytics/answer/6366371?hl=en#zippy=%2Cin-this-article (emphasis added) (last visited Dec. 29, 2022).

61. Google offers an IP Anonymization tool for entities (like Defendant) using Google Analytics, so that end users (like Plaintiff and the Class members) will not have their full IP address reported and stored. Google's website explains, "The IP-masking feature in Universal Analytics sets the last octet of IPv4 user IP addresses and the last 80 bits of IPv6 addresses to zeros in memory shortly after being sent to Google Analytics. The full IP address is never written to disk in this case."[22] Google further states, "This feature is designed to help site owners comply with their own privacy policies or, in some countries, recommendations from local data protection authorities, which may prevent the storage of full IP address information."[23]

62. Defendant does not use Google's IP Anonymization tool.

63. As a result of Defendant's decision not to use the IP anonymization feature, Defendant transmits patients' full IP addresses to Google, meaning that communications are not anonymous, regardless of whether Google also placed ID cookies on the user's device.

64. Like Meta's Lookalike Audiences, Google offers "Similar Audiences." Google explains on its website:

> To find similar segments, Google Ads looks at the millions of people searching on Google. …
>
> A similar segments list is created from a remarketing list or Customer Match list with at least 1,000 cookies ***with enough similarity in search behavior to create a corresponding similar segment***.
>
> Website tag and rule-based remarketing lists, as well as Customer Match lists built from email addresses, mailing addresses, and/or phone numbers, can be used to generate similar segments.….[24]

(Emphasis added.)

---

[22] Google, ANALYTICS HELP, IP MASKING IN UNIVERSAL ANALYTICS, https://support.google.com/analytics/answer/2763052?hl=en (last visited Dec. 29, 2022).

[23] *Id.*

[24] Google Ads Help, ABOUT SIMILAR SEGMENTS FOR SEARCH, https://support.google.com/google-ads/answer/7151628?hl=en#:~:text=To%20find%20similar%20audiences%2C%20Google,visitors%20on%20the%20original%20list (last visited Dec. 29, 2022).

65. Google explains, for its marketing and developer clients:

> In order for Google Analytics to determine that two distinct hits belong to the same user, a unique identifier, associated with that particular user, must be sent with each hit.
>
> The analytics.js library accomplishes this via the Client ID field, a unique, randomly generated string that gets stored in the browsers cookies, so subsequent visits to the same site can be associated with the same user.
>
> By default, analytics.js uses a single, first-party cookie named _ga to store the Client ID, but the cookie's name, domain, and expiration time can all be customized. Other cookies created by analytics.js include _gid, AMP_TOKEN and _gac_<property-id>. These cookies store other randomly generated ids and campaign information about the user.[25]

66. For example, when a patient clicks on a link to a particular doctor, the code that is generated related to Google Analytics shows: the doctor's name, and various "cookies" that Google uses to track individual users. The doctor's specialty is readily available on Defendant's website, so conveying this information Google Analytics makes it easy to identify the medical condition for which the user is seeking a doctor. The Google Analytics cookies in the code generated by the search include strings beginning with "gid" and "cid" (Google Analytics' "Client ID") cookie, followed by strings of unique numbers Google uses to identify to the user's device.

67. On the portions of the Website that are reached after a patient enters their password, Google tracking code that Defendant embedded similarly informs Google of each page that a patient clicks on, including those displaying doctor's names.

68. This disclosure of patient information was unwarranted and improper.

3. Microsoft Bing Tracking Software

69. Defendant also placed tracking code created by Microsoft, called bat.bing, on its Website. bat.bing collects a Microsoft's Machine Unique Identifier (MUID cookie) from users.

---

[25] Google Analytics, COOKIES AND USER IDENTIFICATION, https://developers.google.com/analytics/devguides/collection/analyticsjs/cookies-user-id (last visited Dec. 29, 2022).

This cookie is a unique user identifier and remains active for one year. It is used for advertising, site analytics, and other operational purposes. Similar to Google Analytics, when a user clicks on a doctor's name, bringing them to that doctor's page, bat.bing passes the name, along with the MUID, to Microsoft.

4. Additional Marketing Entities That Were Sent Patient Communications

70. Defendant also placed code on its website that transmitted information regarding the patients' activity on the Cedars-Sinai website to the following marketing related entities. Again, the name of the hospital and doctor are transferred through the tracking code to the marketing partner.

(a) Broadcastmed.innocraft.cloud

71. According to its website: "BroadcastMed is a groundbreaking healthcare media company that plans, produces, and promotes engaging healthcare content in the clinical setting using data-driven solutions to optimize marketing initiatives."[26] Like the other marketing entities to which Cedars-Sinai transmitted patient communications, Broadcastmed is focused on use of patient information to drive marketing decisions. Its website further explains, "[t]he company's proprietary AI-driven data yields unrivaled healthcare industry insights to guide future marketing strategies and decisions for their clients." Transferring Patient information to such and entity would not be done for the patient's benefit, but for the marketer's.

72. When a person clicks on a particular doctor on Defendant's Website, Broadcastmed's tracking code passes the doctor's name back to Broadcastmed.

(b) Mktoresp.com

73. Defendant also had tracking code on its website identified as "mktoresp.com." This appears to be a part of Marketo, which is a marketing automation service associated with Adobe.[27]

---

[26] Broadcastmed, ABOUT US, https://www.broadcastmed.com/about-us (last visited Dec. 29, 2022).

[27] Adobe Experience Cloud, THE DEFINITIVE GUIDE TO MARKETING AUTOMATION, https://www.marketo.com/definitive-guides/marketing-automation/ (last visited Dec. 29, 2022).

74. As with the tracking codes for Google, Microsoft, and Broadcastmed, this code transferred the name of the doctor that the patient clicked on to a third party, along with the user's IP address, without the patient's knowledge or consent. Marketo's default setting is to not anonymize IP addresses. On information and belief, Cedars-Sinai did not change the setting to anonymize the IP addresses. Cedars-Sinai had no legitimate reason for sharing such patient communications with this entity.

C. Class Members Had Multiple Bases for Reasonable Expectations of Privacy

75. Plaintiff and Class members, as patients of Cedars-Sinai, had numerous reasons to expect that their communications with Defendant would be kept private. First, Cedars-Sinai never obtained their consent to share their Private Information for purposes unrelated to services that the patients requested.

76. Moreover, Cedars-Sinai never disclosed that it was doing so. The tracking code is designed to be invisible to a normal website user.

77. In addition, as detailed herein, an array of policies, state and federal statutes, and common understandings give rise to such reasonable expectations.

D. Many Policies and Regulations Demonstrate the Impropriety of Defendant's Sharing of Patient Information

78. By sharing patient data with third parties, Defendant violated its own and Meta's privacy policies as well as government standards and regulations. Defendant knew of its responsibility to protect patient communications and ignored it to further its advertising goals.

1. Defendant's Violation of Its Privacy Policy

79. Cedars-Sinai had a Privacy Policy through which it assured Class members that that their information would be protected and not shared for purposes unnecessary to services specifically requested by the patients.[28] This policy shows that Defendant knew it had a responsibility to protect patient information, rather than share it unnecessarily.

80. Defendant's Website's Privacy Policy states:

[28] Cedars Sinai, PRIVACY POLICY, https://www.cedars-sinai.org/privacy-policy.html (last visited Dec. 29, 2022).

> Personally identifiable information is information you provide that lets us know specific facts about you ***so that we can respond to your requests***. Depending on the portion of the website you visit and the information you provide, this information could range from your name, address and ZIP code, which you provide in order to receive information from us about certain services, to specific health information that you provide to us on an admission form. ***Personal information collected on our site is used only to allow us to fulfill your request for services.*** For instance, if you use our online physical system to locate a specialist in your area, we use the information you provide to put you in touch with a physician. Similarly, if you complete an admission form that you download from our site and submit it to us, we use the information contained in your admission form for the purposes of admitting you to CSHS and to thereafter providing the services your physician prescribes. Another example relates to our gift shop. We collect personal information from you in order to complete transactions you request The information you provide may be furnished to a third party ***in order to facilitate the transaction***. Or, you may submit personal information to us in response to an employment opportunity. ***In each case, we use your personal information only for the purpose it is submitted to us***, which may include providing it to third parties with whom we have relationships ***to deliver the information or services you request***.[29]

(Emphasis added.)

81. This was demonstrably untrue, given that Defendant routinely and automatically transmitted and continues to transmit patients' data to third parties for marketing purposes. Such transmission is unnecessary to "fulfill [patients'] requests for services."

82. Defendant's Privacy Policy also states:

> ***We also do everything reasonably possible to protect user information we collect. All of our users' information, not just the sensitive information, is restricted in our offices***. Only individuals who need the information to perform a specific job are granted access to personal information. Access to this information is password protected. Furthermore, all personnel having access to your personal information are kept up-to-date on our security and privacy practices.[30]

83. Again, this was demonstrably false given the extent to which Defendant has unnecessarily shared patient communications with third parties.

84. As to cookies, Defendant's Privacy Policy states:

---

[29] *Id.*

[30] *Id.*

> We may place small data files, called "cookies," in your browser's file storage area of your computer's hard drive. Cookies are a standard Internet technology that allow us to both store and retrieve login information on a user's system. A cookie is a small text file that is stored on a site visitor's computer to gather and keep track of information related to you. These cookies automatically identify your browser ***to our server*** whenever you interact with a service provided on our website. Cookies can store your preferences through a password you select to access a web site. Cookies also help us review website traffic patterns and improve our site. Most browsers automatically accept these cookies, but you usually can change your browser setting to prevent the acceptance of cookies, but this may prevent you from using some of the features of our website. ***Information collected through cookies is not linked to any personally identifiable information***.[31]

85. This is not true given that some of the cookies relating to tracking code on Defendant's Website can be linked to individual identities.

86. As to log files, the Privacy Policy states:

> We collect and log IP addresses in order to analyze site visitation trends and administer the website. An IP address is a number automatically assigned to your computer whenever you access the Internet. IP addresses allow computers and servers to recognize and communicate with one another. IP address information allows us to properly administer our system and gather ***aggregate*** information on visitors to our website help diagnose problems with our servers, and how our site is being used, including the pages visitors are viewing in the ***aggregate***. This ***aggregate*** information may be shared with third parties, such as our physicians, our suppliers and other businesses. ***To maintain your anonymity, we do not associate IP addresses with records containing personal information. In other words, IP addresses are not linked to personally identifiable information***.[32]

87. The foregoing promises of confidentiality and anonymity were false and misleading given Defendant's incorporation into its website of code that shared patients' communications with Meta and other third parties. However, they gave Class members a reasonable expectation of privacy.

2. Meta's Policies

88. Meta's own policies were another source of assurance to Class members that Cedars-Sinai would not be sharing their data and another clear warning to Defendant that it

---

[31] *Id*. (Emphasis added.)

[32] *Id*. (Emphasis added.)

should not have shared its patients' data as it did. To begin, Meta's privacy policy states that "[w]e require Partners [*e.g.*, advertisers, like Cedars-Sinai, who send Meta information through Meta Business Tools] to have the right to collect, use and share your information before giving it to us."[33]

89. In addition, Meta's contract with businesses that, like Cedars-Sinai, use its Business Tools, including the Pixel, requires that such businesses "represent and warrant that [they] (and any data provider that [they] may use) have all of the necessary rights and permissions and a lawful basis (in compliance with all applicable laws, regulations and industry guidelines) for the disclosure and use of Business Tool Data."[34] Here, for the reasons discussed herein, Cedars-Sinai did not have the necessary legal rights and permissions to share the patient data that it did.

90. The Facebook Business Tool Terms also provide, at Section 1(h), "***You will not share Business Tool Data with us that you know or reasonably should know*** is from or about children under the age of 13 ***or that includes health***, financial information or other categories of sensitive information." Of course, Defendant did just that.

91. In addition, the Facebook Business Tool Terms requires of businesses like Cedars-Sinai to:

> [R]epresent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage that includes, at a minimum: i. For websites, a clear and prominent notice on each web page where our pixels are used that links to a clear explanation (a) that third parties, including Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from your websites and elsewhere on the Internet and use that information to provide measurement services and target ads.

---

[33] Meta, PRIVACY POLICY, https://mbasic.facebook.com/privacy/policy/printable/ (last visited Dec. 29, 2022).

[34] Facebook, FACEBOOK BUSINESS TOOLS TERMS, Section 1(e), https://www.facebook.com/legal/businesstech?paipv=0&eav=Afb8lVB3IDvB3rFEMJQmgdaS2iOzEGlLXfl8Q71xM21q28VqYCBGQeF3XUqAnbXgoGU&_rdr (last visited Dec. 29, 2022).

92. Cedars-Sinai did not give "robust" or "sufficiently prominent" notice that it would be using cookies or tracking code to share patients' Private Information with third parties, including Facebook, for marketing purposes.

93. The various statements on Meta's website was one of the reasons that Class members had a strong expectation that the information they provided to Cedars-Sinai would not be provided to Facebook.

94. The above policies are part of Meta's contract with Cedars-Sinai. Class members are the intended third party beneficiaries of this contract.

3. Google's Policies Provided Additional Assurance of Confidentiality

95. Google's Privacy Disclosure Statement is yet another reason that Defendant knew or should have known that its sharing data was improper.

96. The Google Privacy Disclosure Policy provides:

> When you use Google Analytics on your site or application, you must disclose the use of Google Analytics and how it collects and processes data.[35]

97. Defendant does not expressly mention "Google Analytics" on its website or make proper disclosure of the data that Defendant provides to Google through coding, and what that data is used for.

98. Google's rules for advertisers also provide:

> We understand that users don't want to see ads that exploit their personal struggles, difficulties, and hardships, so we don't allow personalized advertising based on these hardships. Such personal hardships include health conditions, treatments, procedures, personal failings, struggles, or traumatic personal experiences. You also can't impose negativity on the user.[36]

99. Google's rules for advertisers further state that the following should not be used in advertising:

---

[35] Google, PRIVACY DISCLOSURES POLICY, https://support.google.com/analytics/answer/7318509?hl=en#:~:text=When%20you%20use%20Google%20Analytics,Safeguarding%20your%20data (last visited Dec. 29, 2022).

[36] Google, ADVERTISING POLICIES HELP, PERSONALIZED ADVERTISING https://support.google.com/adspolicy/answer/143465?hl=en (last visited Dec. 29, 2022).

Personal health content, which includes:

- Physical or mental health conditions, including diseases, sexual health, and chronic health conditions, which are health conditions that require long-term care or management.
- Products, services, or procedures to treat or manage chronic health conditions, which includes over-the-counter medications and medical devices.
- Any health issues associated with intimate body parts or functions, which includes genital, bowel, or urinary health.
- Invasive medical procedures, which includes cosmetic surgery.
- Disabilities, even when content is oriented toward the user's primary caretaker.
    - **Examples**: Treatments for chronic health conditions like diabetes or arthritis, treatments for sexually transmitted diseases, counseling services for mental health issues like depression or anxiety, medical devices for sleep apnea like CPAP machines, over-the-counter medications for yeast infections, information about how to support your autistic child[.][37]

100. Google's policies in this regard are indicative of a broader general public policy against using medical information for advertising, and are another reason that Plaintiff and Class members would reasonably expect Defendant to maintain the privacy of their information. Of course, if Defendant did not intend to advertise to patients based on their having health conditions that cause them to be patients, it would have had no reason to include Google Analytics on its Website at all.

4. Federal Warning on Tracking Codes on Healthcare Websites.

101. Beyond Defendant's own policies, and those of Meta and Google, the government has issued guidance warning that tracking code like Meta Pixel and Google Analytics may come up against federal privacy law when installed on healthcare websites. The statement, titled USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES

[37] *Id.*

(the "Bulletin"), was recently issued by the Department of Health and Human Services' Office for Civil Rights ("OCR").[38]

102. Healthcare organizations regulated under the Health Insurance Portability and Accountability Act (HIPAA) may use third-party tracking tools, such as Google Analytics or Meta Pixel, in a limited way, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' protected health information to these vendors. The Bulletin explains:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures***.[39]

103. The bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI***. Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment***. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***[40]

104. Plaintiff and Class members face just the risks about which the government expresses concern. Defendant has passed along Plaintiff's and Class members' search terms about health conditions for which they seek doctors; their contacting of doctors to make

---

[38] HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Dec. 29, 2022).

[39] *Id.* (Emphasis added.)

[40] *Id.* (Emphasis added.)

appointments; the names of their doctors; the frequency with which they take steps relating to obtaining healthcare for certain conditions; and where they seek medical treatment. This information is, as described by the OCR in its bulletin, "highly sensitive."

105. The Bulletin goes on to make clear how broad the government's view of protected information is. It explains:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code***.[41]

106. Crucially, that paragraph in the government's Bulletin continues:

> ***All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.*** This is because, ***when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care***.[42]

107. This is further evidence that the data that Defendant chose to share is protected Personal Information. The sharing of that information was a violation of Class members' rights.

5. Defendant's Violation of HIPAA

108. Defendant's disclosure of Plaintiff's and Class members' Private Information to entities like Facebook and Google also violated HIPAA. HIPAA provided Plaintiff and Class members with another reason to believe that the information they communicated to Defendant through its Website would be protected, rather than shared with third-parties for marketing purposes. Moreover, Defendant's violation of HIPAA is a violation of law that forms the one of the bases of its violation of California's Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq*.

---

[41] *Id*. (Emphasis added.)

[42] *Id*. (Emphasis added.)

109. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

110. HIPAA prohibits health care providers from "us[ing] or disclos[ing] 'protected health information' except as permitted or required by" the HIPAA Privacy Rule. 45 C.F.R. § 164.502.

111. "A covered entity may determine that health information is not individually identifiable health information only if" either "a person with appropriate knowledge of and experience with generally accepted statistical and scientific methods for rendering information not individually identifiable: a) applying such principles" determines that the risk is "very small" that the information could be used alone, or in combination with other information, to identify individuals, and documents the methods that justifies such a determination, or identifiers are removed that include: Internet Protocol (IP) address numbers; account numbers; URLs, device identifiers, and "any other unique identifying number, characteristic or code," except codes assigned by the healthcare organization to allow itself to reidentify information from which it has removed identifying information.

112. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be Protected Health Information. The Department of Health and Human Services has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data:

> If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[43]

113. Consistent with this restriction, the HHS has issued marketing guidance that provides that:

> With limited exceptions, the [Privacy] Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.[44]

114. Here, Defendant provided patient information to third parties in violation of this rule.

115. Commenting on a June 2022 report discussing the use of the Meta Pixel by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it … ***It is quite likely a HIPAA violation.***"[45]

116. Defendant's placing of the third-party tracking code on its Website is a violation of Class members' privacy rights under federal law. While Plaintiff does not bring a claim under HIPAA itself, this violation evidences Defendant's wrongdoing as relevant to other claims.

E. Plaintiff's and Class Members' Private Information Had Financial Value

117. Plaintiff's private data has economic value. Indeed, Meta's, Google's and others' practices of using such information to package groups of people as "Lookalike Audiences" and

---

[43] HHS.gov, GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Dec. 29, 2022).

[44] HHS.gov, MARKETING, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (last visited Dec. 29, 2022).

[45] Advisory Board, 'DEEPLY TROUBLED': SECURITY EXPERTS WORRY ABOUT FACEBOOK TRACKERS ON HOSPITAL SITES, https://www.advisory.com/daily-briefing/2022/06/17/data-trackers (emphasis added) (last visited Dec. 29, 2022).

similar groups and selling those packages to advertising clients demonstrates the financial worth of that data.

118. Data harvesting is the fastest growing industry in the nation. As software, data mining, and targeting technologies have advanced, the revenue from digital ads and the consequent value of the data used to target them have risen rapidly.

119. Consumer data is so valuable that some have proclaimed that data is the new oil. Between 2016 and 2018, the value of information mined from Americans increased by 85% for Facebook and 40% for Google. Overall, the value internet companies derive from Americans' personal data increased almost 54%. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user. In 2022, that value is expected to be $200 billion industry wide, or $434 per user, also a conservative estimate.

120. As to health data specifically, as detailed in an article in Canada's National Post:

> As part of the multibillion-dollar worldwide data brokerage industry, health data is one of the most sought-after commodities. De-identified data can be re identified (*citing* https://www.nature.com/articles/s41467-019-10933-3/) and brazen decisions to release records with identifiable information (citing https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200?mod=hp_lista_pos3) are becoming commonplace).[46]

121. Further demonstrating the financial value of Class members' medical data, CNBC has reported that hospital executives have received a growing number of bids for user data:

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

[46] National Post, IRIS KULBATSKI: THE DANGERS OF ELECTRONIC HEALTH RECORDS, February 26, 2020, https://nationalpost.com/opinion/iris-kulbatski-the-dangers-of-electronic-health-records (last visited Dec. 29, 2022).

> "It's all the time," he said via phone. "Often, once a day or more."
>
> * * *
>
> [H]ealth systems administrators say [the data] could also be used in unintended or harmful ways, like being cross-referenced with other data to identify individuals at higher risk of diseases and then raise their health premiums, or to target advertising to individuals.[47]

122. The CNBC article also explained:

> De-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers. Just one company alone, IQVIA, said on its website that it has access to more than 600 million patient records globally that are nonidentified, much of which it accesses through provider organizations. The buyers, which include pharma marketers, will often use it for things like clinical trial recruiting
>
> But hospital execs worry that this data may be used in unintended ways, and not always in the patient's best interest.
>
> * * *
>
> Tech companies are also under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own needs. For instance, the health data Google collects could eventually help it micro-target advertisements to people with particular health conditions. Policymakers are proactively calling for a revision and potential upgrade of the health privacy rules known as HIPAA, out of concern for what might happen as tech companies continue to march into the medical sector.[48]

123. Time Magazine similarly, in an article titled, HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY, referenced the "growth of the big health data bazaar," in which patients' health information is sold. It reported that:

> [T]the secondary market in information unrelated to a patient's direct treatment poses growing risks, privacy experts say. That's because clues in anonymized patient dossiers make it possible for outsiders to determine your identity, especially as computing power advances in the future.[49]

---

[47] CNBC, HOSPITAL EXECS SAY THEY ARE GETTING FLOODED WITH REQUESTS FOR YOUR HEALTH DATA, https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Dec. 29, 2022).

[48] *Id.*

[49] Time, HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY, https://time.com/4588104/medical-data-industry/ (last visited Dec. 29, 2022).

124. Cedars-Sinai gave away Plaintiff's and Class members' communications and transactions on its Website without permission. The unauthorized access to Plaintiff's and Class members' private and Personal Information has diminished the value of that information, resulting in harm to Defendant's Website users.

V. CLASS ACTION ALLEGATIONS

125. Plaintiff brings this action on his own behalf and as a class action, pursuant to California Code of Civil Procedure Section 382, on behalf of the following class:

> All persons residing in California who used Defendant's Website at any time when tracking code able to share data for marketing or website analytics purposes was present.

126. This action is properly maintainable as a class action.

127. Plaintiff reserves the right under California Rules of Court, rule 3.765 to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

128. Numerosity: The Class is so numerous that joinder of all members would be impracticable. While Plaintiff does not know the exact number of Class members, Cedars-Sinai represents that it sees over 1 million patients per year, and on, information and belief, a significant proportion of those patients use Defendant's Website.

129. Commonality and Predominance: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, are the following:

- Whether Defendant had a duty not to share the PHI/PII of Plaintiff and Class members with unauthorized third parties;
- Whether Defendant had a duty not to use the PHI/PII of Plaintiff and Class members for non-healthcare purposes;
- Whether information that Defendant shared with third parties like Meta constituted PHI and/or PII;

- Whether Defendant disclosed to Plaintiff and Class members that their PHI/PII would be shared with third parties unrelated to services that they specifically requested;
- Whether Defendant engaged in unfair, unlawful, or deceptive acts or practices by sharing the PHI/PII of Plaintiff and Class members with unrelated third parties such as Meta;
- Whether Plaintiff and Class members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;
- Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's sharing of their PHI/PII with unrelated third parties such as Meta;
- Whether Defendant's disclosure of Plaintiff's and Class members' PHI/PII constituted an intrusion upon seclusion;
- Whether Defendant's disclosure of Plaintiff's and Class members' PHI/PII was unfair, deceptive and/or unlawful and thus a violation of California's statutory prohibition of unfair competition.
- Whether and the extent to which Defendant's conduct harmed Plaintiff and Class members.

130. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other member, was exposed to virtually identical conduct and now suffers from the same violations of the law as other members of the Class.

131. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate. Defendant's policies and practices challenged herein apply to and affect Class members uniformly and

Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

132. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class members. Plaintiff seeks no relief that is antagonistic or adverse to the Class members and the infringement of the rights and the damages they have suffered are typical of other Class members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

133. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against a large corporation, like Defendant. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

134. The nature of this action and the nature of laws available to Plaintiff and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

135. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

136. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

137. Unless a Class-wide injunction is issued, Defendant may continue to illegally provide the PHI/PII of its patients to unrelated third parties.

138. The prosecution of separate actions by individual members of the Class would create the risk of inconsistent or varying adjudications and would establish incompatible standards of conduct for the Defendant. The Defendant has acted, or has refused to act, on grounds generally applicable to the Class, making final injunctive relief on behalf of the Class as a whole appropriate.

139. Questions of law and fact common to the members of the Class predominate over any questions affecting any individual member, and a class action is superior to all other available methods for the fair and efficient adjudication of the controversy.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
Violation of the California Invasion of Privacy Act
(Cal. Penal Code §§ 630, 631, *et seq.* ("CIPA"))

140. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

141. California's Invasion of Privacy Act, California Penal Code 631(a) provides a remedy against, *inter alia*:

> ***Any person who*** … ***intentionally taps*****, or** ***makes any unauthorized*** connection, ***whether*** physically, ***electrically***, …, or otherwise, with any telegraph or telephone wire, line, cable, or instrument … ***or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads***, or attempts to read, or to learn the contents or meaning of any message, report, or communication ***while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state***; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, ***or who aids, agrees with, employs, or***

conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section,

142. Defendant is a person for the purposes of this law.

143. Here, Defendant "intentionally tap[ped] … **or *ma[de] [an] unauthorized*** connection" with respect to Class members' communications by placing third party tracking code on its Website, without "the consent of all parties" including Plaintiff, and thereby violated CIPA.

144. Defendant also "***aid[ed], agree[d] with, employ[d], or conspire[d] with*****"** Meta, Google, and other third parties providing marketing services by placing their third-party tracking code on its Website, and allowing such entities; to "tap" communications on its website without "the consent of all parties" including Plaintiff, and thereby violated CIPA.

145. Defendant facilitated the interception and simultaneous transmission to Meta, Google, and others of Plaintiff's and other Class members' PII and PHI while the information was "in transit." As a patients typed communications into Defendant's website, as a result of the Meta Pixel and other tracking codes that Defendant placed there, their requests were simultaneously redirected to Facebook while they were still on their way to Defendant.

146. The information communicated between patients and Cedars-Sinai, a Los Angeles healthcare system, was transmitted to or from the state of California. The information was wiretapped "***while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state*****."**

147. Redirection of data as a result of tracker coding before that data reaches its originally intended recipient (here, Cedars-Sinai) does not constitute a separate communication for the purposes of exclusion from CIPA coverage.

148. Cedars-Sinai enabled non-parties to the communications to "read" the communications for the purposes of the statute. For example, Meta could see which individual searched for doctors with particular specialties, what conditions they researched, and when and where they made appointments.

149. Cedars-Sinai facilitated this communication "without authorization" of Class members because it did not give Class members any hint that the transmission was happening. Indeed, Cedars-Sinai's own privacy policy stated that "personal information" would only be used "for the purpose it is submitted to us, ***which may include providing it to third parties with whom we have relationships to deliver the information or services you request***."[50] (Emphasis added.) Class members did not *request* that Defendant and third parties target them with advertising that might be related to their health conditions.

150. Cal. Penal Code § 637.2(a) provides:

> Any person who has been injured by a violation of this chapter [including Penal Code §§ 630 and 631] may bring an action against the person who committed the violation for the greater of the following amounts:
>
> (1) Five thousand dollars ($5,000) per violation.
> (2) Three times the amount of actual damages, if any, sustained by the plaintiff.

151. Cal. Penal Code § 637.2(b) provides that "[a]ny person may . . . bring an action to enjoin and restrain any violation of this chapter, and may in the same action seek damages as provided by subdivision (a)."

152. Cal. Penal Code § 637.2(c) provides, "It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

153. Defendant is therefore liable to Plaintiff and the Class for, at a minimum, statutory damages of $5,000 per violation, and Plaintiff and Class members are also entitled to injunctive relief.

SECOND CAUSE OF ACTION
Violation of the California Invasion of Privacy Act
(Cal. Penal Code § 632, *et seq.* ("CIPA"))

154. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

155. Cal. Penal Code § 632 provides, in relevant part, that it is unlawful to "intentionally and without the consent of all parties to a confidential communication," "use[] [a]

[50] *See* https://www.cedars-sinai.org/privacy-policy.html (last visited Dec. 29, 2021).

recording device to … record the confidential communication." As used in the statute "'confidential communication' means any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto."

156. The written transmission of information about Plaintiff's and Class members' searches and clicks on its Website as described above is a recording of those communications. The code is a "recording device."

157. Defendant did not have Plaintiff's or other Class members' consent to record their communications.

158. Cal. Penal Code § 637.2(a) provides:

> Any person who has been injured by a violation of this chapter [including Penal Code § 632] may bring an action against the person who committed the violation for the greater of the following amounts:
>
> (1) Five thousand dollars ($5,000) per violation.
> (2) Three times the amount of actual damages, if any, sustained by the plaintiff.

159. Cal. Penal Code § 637.2(b) provides that "[a]ny person may . . . bring an action to enjoin and restrain any violation of this chapter, and may in the same action seek damages as provided by subdivision (a)."

160. Cal. Penal Code § 637.2(c) provides, "It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

161. Defendant is therefore liable to Plaintiff and the Class for, at a minimum, statutory damages of $5,000 per violation, and Plaintiff and Class members are also entitled to injunctive relief.

THIRD CAUSE OF ACTION
Invasion of Privacy/Intrusion upon Seclusion in Violation of California Common Law and the California Constitution, Art. 1, § 1

162. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

163. Plaintiff and Class members have a legally protected privacy interest in the PHI and PII that they enter into Defendant's Website and are entitled to the protection of their information and property against unauthorized access.

164. Plaintiff and Class members reasonably expected that their Private Information would be protected and secure from unauthorized parties, and that it would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

165. Defendant unlawfully invaded the privacy rights of Plaintiff and Class members by: (a) disclosing their private, and personal information to unauthorized parties in a manner that is highly offensive to a reasonable person; and (b) disclosing their private and personal information to unauthorized parties without the informed and clear consent of Plaintiff and Class members, including but not limited to including the Meta Pixel and other tracking code on its Website that transfer information entered and records of actions taken by patients on Defendant's Website to unrelated entities. This invasion into the privacy interest and seclusion of Plaintiff and Class members is serious and substantial.

166. In willfully sharing Plaintiff's and Class members' Personal Information, Defendant acted in reckless disregard of their privacy rights.

167. Defendant violated Plaintiff's and Class members' right to privacy under California law, including, but not limited to California common law and Article 1, Section 1 of the California Constitution and the California Consumer Privacy Act.

168. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiff's and Class members' private, personal, and confidential information has been accessed or is at imminent risk of being accessed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff and proposed Class members have suffered injuries as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

169. Plaintiff and Class members are entitled to injunctive relief as well as actual and punitive damages.

FOURTH CAUSE OF ACTION
Breach of Implied Contract

170. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

171. Defendant offered use of its Website to Plaintiff and members of the Class. In exchange, Defendant received benefits in the form of patients making appointments with Defendant's doctors, obtaining treatment at Defendant's hospitals and/or other valuable consideration, *e.g.*, access to their private and personal data.

172. Defendant acknowledged these benefits and accepted or retained them.

173. In using Defendant's Website, Plaintiff and Class members continually provide Defendant with their valuable private and personal information.

174. By providing that information, and upon Defendant's acceptance of that information, Plaintiff and Class members, on the one hand, and Defendant, on the other, entered into implied contracts, separate and apart from Defendant's terms of service, under which Defendant agreed to and was obligated to take reasonable steps to secure and safeguard that sensitive information.

175. All parties understood that such security was essential to Defendant's line of business—the provision of medical information and services.

176. Under those implied contracts, Defendant was obligated to provide Plaintiff and Class members with a Website that was suitable for its intended purpose of exchanging sensitive and other healthcare information rather than a Website that provided patient information to third parties including Meta and that tracks its users' personal data for commercial purposes.

177. Without such implied contracts, Plaintiff and Class members would not have used Defendant's Website and would not have conferred benefits on Defendant.

178. Plaintiff and Class members fully performed their obligations under these implied contracts.

179. As described throughout, Defendant did not take reasonable steps to safeguard Plaintiff's and Class members' private information. In fact, Defendant willfully violated those privacy interests by placing third party tracking code on its Website.

180. Because Defendant failed to take reasonable steps to safeguard Plaintiff's private information, Defendant breached its implied contracts with Plaintiff and Class members.

181. Accordingly, Plaintiff, on behalf of himself and Class members, seeks an order declaring that Defendant's conduct constitutes breach of implied contract, and awarding them damages in an amount to be determined at trial.

FIFTH CAUSE OF ACTION
Breach of Contract – Third-Party Beneficiaries

182. Plaintiff incorporates the foregoing allegations as if set forth fully herein.

183. Defendant entered into an agreement (the "Facebook Business Tools Agreement") with Meta when it placed the Pixel on its website.

184. The Facebook Business Tools Agreement is a valid and enforceable express contract between Defendant and Meta for the benefit of Defendant's customers. Under the Facebook Business Tools Agreement, Defendant gave Meta access to its patients' private information and in exchange Meta provided data analytic tools for use on Defendant's Website.

185. In Connection with that Agreement, Defendant agreed to follow Meta's policies, which require businesses, like Cedars-Sinai, that use its Business Tools, including the Pixel, to represent that they have the legal rights to share the data, that they will not disclose medical data, and that they will give "robust" and "sufficiently prominent" notice that they would be sharing patients' Private Data, including medical data, with Meta for advertising purposes.

186. The above policies are part of Meta's contract with Cedars-Sinai. Class members are the intended third party beneficiaries of this contract.

187. While Plaintiff and the Class are not parties to the Facebook Business Tools Agreement, given the purpose of and the services to be provided under the Facebook Business Tools Agreement, and the surrounding circumstances, including Defendant's and Meta's public statements about their duties to protect Private Information, Plaintiff and the Class are intended third party beneficiaries of the Facebook Business Tools Agreement.

188. The benefits that Plaintiff and the Class were to receive as intended third party beneficiaries of the Facebook Business Tools Agreement were not incidental to that Agreement.

189. As a direct and proximate result of Defendant's breaches of the Facebook Business Tools Agreement, Plaintiff and the Class, as intended third party beneficiaries of Facebook Business Tools Agreement, sustained actual losses and damages as described in detail above in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
Breach of Implied Covenant of Good Faith and Fair Dealing

190. Plaintiff incorporates the foregoing allegations as if fully set forth here.

191. There is a covenant of good faith and fair dealing implied in every implied contract. This implied covenant requires each contracting party to refrain from doing anything to injure the right of the other to receive the benefits of the agreement. To fulfill its covenant, a party must give at least as much consideration to the interests of the other party as it gives to its own interests.

192. Under the implied covenant of good faith and fair dealing, Defendant is obligated to, at a minimum: (a) implement proper procedures to safeguard the PHI and PII of Plaintiff and other Class members; (b) refrain from disclosing, without authorization or consent, the PHI and PII of Plaintiff and other Class members to any third parties; and (c) and promptly and accurately notify Plaintiff and other Class members of any unauthorized disclosure of, access to, and use of their Private Information.

193. Defendant breached the implied covenant of good faith and fair dealing by, among other things:

- disclosing Plaintiff's and other Class members' Private Information to unauthorized outside entities, including Facebook and Google;
- allowing outside entities to access the Private Information of Plaintiff and other Class members;
- failing to implement and maintain adequate security measures to safeguard users' Private Information; and
- failing to timely notify Plaintiff and other Class members of the unlawful disclosure of their Private Information;

194. As a direct and proximate result of Defendant's breaches of the implied covenant of good faith and fair dealing, Plaintiff and other Class members have suffered actual losses and damages in an amount to be determined at trial.

SEVENTH CAUSE OF ACTION
Negligence

195. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

196. Defendant offered its Website to Plaintiff and Class members with full knowledge of the purposes for which the Website was being used, as well as the highly sensitive nature of the information the Website involved.

197. Defendant owed a duty to Plaintiff and Class members arising from the sensitivity of Plaintiff's and Class members' information, and the privacy rights the Website was supposed to secure and protect, to exercise reasonable care in safeguarding such information and privacy rights. Defendant's duties included refraining from sharing patients' sensitive PII and PHI with unauthorized parties without users' informed and clear consent.

198. Defendant breached its duties by, among other things, knowingly placing code on its Website that would divert customers' Private Information to outside entities including Meta for analytics and marketing purposes without adequate disclosure to and consent from its customers.

199. Defendant's misconduct is inconsistent with industry regulations and standards.

200. But for Defendant's breaches of its duties, Plaintiff's and Class members' PII and PHI would have been protected from unauthorized access and would not have been compromised or obtained by third parties without consent.

201. Plaintiff and Class members were foreseeable victims of Defendant's wrongful conduct complained of herein. Defendant knew or should have known that its enabling of third-party access to customers' Private Information would cause damages to Plaintiff and Class members.

202. As a result of Defendant's negligent and/or willful failures, Plaintiff and Class members suffered injury, including unauthorized release of Private Information to third parties,

and exposure to a heightened, imminent risk of unauthorized access to their private and personal data.

203. The damages to Plaintiff and Class members were a proximate, reasonably foreseeable result of Defendant's breaches of its duties.

204. Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

EIGHTH CAUSE OF ACTION
Violation of California's Confidentiality of Medical Information Act
(Cal. Civ. Code § 56, *et seq.*)

205. Plaintiff incorporates the foregoing allegations as if set forth fully herein.

206. The short title of the California Confidentiality of Medical Information Act, California Civil Code § 56, *et seq.* (hereinafter referred to as the "CMIA") states:

> The Legislature hereby finds and declares that persons receiving health care services have a right to expect that the confidentiality of individual identifiable medical information derived by health service providers be reasonably preserved. It is the intention of the Legislature in enacting this act, to provide for the confidentiality of individually identifiable medical information, while permitting certain reasonable and limited uses of that information."

207. The CMIA provides, at Section 56.10(a), that "a provider or health care … shall not disclose medical information regarding a patient … without first obtaining an authorization."

208. Moreover, at all times relevant, Defendant was and is a "provider of health care" within the meaning of Civil Code § 56.05(m).

209. Plaintiff and Class members are patients within the meaning of Civil Code § 56.05(k).

210. At all relevant times, Defendant obtained medical information from its patients through its Website.

211. The statute defines "medical information" as:

> [A]ny individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the

> patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual.

Cal. Civ. Code § 56.05(i).

212. Here, tracking code made possible the linking of a Website user and their identity. The information exchanged, including the contents of searches and the act and substance of making appointments with doctors, reveals information about patients' "physical condition or history."

213. As a provider of health care, a contractor, and/or other authorized recipient of medical information as defined by Civil Code § 56.05(j), Defendant is required by the CMIA to ensure that medical information regarding patients is not disclosed, disseminated or released without patients' authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

214. As provider of health care, a contractor, and/or other authorized recipient of medical information as defined by Civil Code § 56.05(j), Defendant is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization[51] under Civil Code §§ 56.10, 56.13, 56.245 and 56.26.

---

[51] An "authorization" is defined under the CMIA as obtaining permission in accordance with Civil Code § 56.11. Under Civil Code § 56.11, an authorization for the release of medical information is valid only if it:

> (a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.
>
> (b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.
>
> (c) Is signed and dated by one of the following:
>
> > (1) The patient. A patient who is a minor may only sign an authorization for the release of medical information obtained by a provider of health care, health care service plan, pharmaceutical company, or contractor in the course of furnishing services to which the minor could lawfully have consented under Part 1 (commencing with Section 25) or Part 2.7 (commencing with Section 60).
> >
> > (2) The legal representative of the patient, if the patient is a minor or an incompetent. However, authorization may not be given under this subdivision for the disclosure of medical information obtained by the provider of health care,

(continued…)

215. As a provider of health care, a contractor, and/or other authorized recipient of personal and confidential medical information, Defendant is required by the CMIA to create, maintain, preserve, and store medical records in a manner that preserves the confidentiality of the information contained therein under Civil Code § 56.101(a).

216. At all relevant times, as a provider of healthcare a contractor, and/or other authorized recipient of personal and confidential medical information within the meaning of the CMIA, Defendant maintains medical information as defined by Civil Code § 56.05(j) of the Plaintiff and Class members.

217. Plaintiff and Class members provided their medical information as defined by Civil Code § 56.05(j) to Defendant or their medical information as defined by Civil Code § 56.05(j) was provided to Defendant by other providers of health care, contractors, and/or other authorized recipients.

(…continued)

health care service plan, pharmaceutical company, or contractor in the course of furnishing services to which a minor patient could lawfully have consented under Part 1 (commencing with Section 25) or Part 2.7 (commencing with Section 60).

(3) The spouse of the patient or the person financially responsible for the patient, where the medical information is being sought for the sole purpose of processing an application for health insurance or for enrollment in a nonprofit hospital plan, a health care service plan, or an employee benefit plan, and where the patient is to be an enrolled spouse or dependent under the policy or plan.

(4) The beneficiary or personal representative of a deceased patient.

(d) States the specific uses and limitations on the types of medical information to be disclosed.

(e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.

(f) States the name or functions of the persons or entities authorized to receive the medical information.

(g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.

(h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.

(i) Advises the person signing the authorization of the right to receive a copy of the authorization.

218. Section 56.10(a) of the Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization."

219. As a result of the tracking code on its Website, Defendant has released, disclosed, and/or negligently allowed third parties to access and view Plaintiff's and Class members' medical information without their written authorization as required by the provisions of Civil Code § 56, *et seq*.

220. As a further result of the Defendant's actions, the confidential nature of the Plaintiff's and Class members' medical information was breached due to Defendant's negligence or affirmative decisions.

221. Defendant's release and/or disclosure of medical information regarding Plaintiff and the Class members constitutes a violation of Civil Code §§ 56.06, 56.10, 56.11, 56.13, 56.26, 56.36, 56.101 and 56.245.

222. By disclosing Plaintiff's and the Class members' medical information without their written authorization, Defendant violated the CMIA and its legal duty to protect the confidentiality of such information.

223. Defendant also violated § 56.101(a) of the CMIA, which prohibits the negligent release of Plaintiff's and the Class members' medical information.

224. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff's and Class members' medical information as defined by Civil Code § 56.05(j) was viewed by, released to, and disclosed to third parties without Plaintiff's and Class members' written authorization and Plaintiff and the Class are entitled to recover, "against any person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: (1) ... nominal damages of one thousand dollars ($1,000). In order to recover under this paragraph, it shall not be necessary that the

plaintiff suffered or was threatened with actual damages. (2) The amount of actual damages, if any, sustained by the patient."

225. As a direct and proximate result of Defendant's above–described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CMIA, Plaintiff and the Class members are entitled to and hereby seek: (i) actual damages suffered, according to proof, for each violation under Civil Code § 56.36(b)(2); (ii) nominal damages of $1,000 for each violation under Civil Code § 56.36(b)(1); (iii) punitive damages under Civil Code § 56.35; and (iv) attorneys' fees, litigation expenses, and court costs under Civil Code § 56.35.

NINTH CAUSE OF ACTION
Violation of the California Unfair Competition Law
(Cal. Bus. & Prof. Code § 17200, *et seq.*)

226. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

227. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

228. Defendant engaged in unfair, fraudulent, and unlawful business practices in connection with its provision of Plaintiff's and other Class members' PHI and PII to unrelated third parties, including Meta, in violation of the UCL.

229. As alleged herein, Defendant expressly represented to consumers such as Plaintiff and Class members, among other things: that information they entered onto Defendant's website would not be used for purposes other than those specifically requested by Plaintiff, such as finding a doctor within Defendant's system or the researching, on Defendant's system, of patients' medical conditions. Defendant also omitted or concealed the material fact of that it had installed internet eavesdropping devices, including the Meta Pixel, on its webpages. It thus failed to disclose to Plaintiff and Class members that it failed to meet legal and industry standards for the protection of PHI and PII and consequently, its customers' private property and information.

230. The acts, omissions, and conduct of Defendant as alleged herein constitute "business practices" within the meaning of the UCL.

231. Defendant violated the "unlawful" prong of the UCL by violating, *inter alia*, Plaintiff's and Class members' constitutional rights to privacy, state and federal privacy statutes, and state consumer protection statutes, such as The Children's Online Privacy Protection Act, 16 C.F.R. § 312.5 ("COPPA"), The Online Privacy Protection Act, California Business and Professions Code §§ 22575-22579 ("CalOPPA"), the California Invasion of Privacy Act ("CIPA"), California Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA"), and The Health Insurance Portability and Accountability Act ("HIPAA").

232. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct, as alleged herein, offended public policy (including the aforementioned federal privacy statutes, and state consumer protection statutes, such as COPPA, CalOPPA, CIPA, CDAFA, and HIPAA) and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and Class members.

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

234. By exposing, compromising, and willfully sharing and/or selling Plaintiff's and Class members' private property and personal information without authorization, Defendant engaged in a fraudulent business practice that is likely to deceive a reasonable consumer.

235. A reasonable person would not have agreed interact with Defendant's website had he or she known the truth about Defendant's practices alleged herein. By withholding material information about its practices, Defendant was able to convince customers to use its website and to entrust their highly personal information to Defendant.

236. As a result of Defendant's violations of the UCL, Plaintiff and Class members are entitled to injunctive relief.

237. As a result of Defendant's violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost money or property, including but not limited to payments to Defendant and/or other valuable consideration, *e.g.*, access to their private and personal data. The unauthorized access to Plaintiff's and Class members' private and personal data also has diminished the value of that information.

238. In the alternative to those claims seeking remedies at law, Plaintiff and Class members allege that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful, unfair, and fraudulent practices. Further, no legal remedy exists under COPPA, CalOPPA, and HIPAA. Therefore, Plaintiff and members of the proposed Class are entitled to equitable relief to restore Plaintiff and Class members to the position they would have been in had Defendant not engaged in unfair competition, including an order enjoining Defendant's wrongful conduct, restitution, and disgorgement of all profits paid to Defendant as a result of its unlawful and unfair practices.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, requests that this Court:

A. Certify the Class as a class action pursuant to Code of Civil Procedure Section 382, designating Plaintiff as the Class Representative and naming the undersigned as Class Counsel;

B. Award compensatory damages, including all applicable statutory damages, for damages caused by Defendant's wrongdoing;

C. Award punitive damages for the purpose of deterring Defendant from committing similar wrongdoing in the future.

D. Permanently enjoin the Defendant from further sharing communications made on its Website with third parties without the Website's users' knowledge and consent;

E. Award pre-judgment interest to Plaintiff and Class members to the fullest extent allowed by law;

F. Award Plaintiff and the members of the Class the costs of bringing this action, including the payment of reasonable attorneys' fees and administrative and litigation costs and expenses; and

G. Grant such other relief as the Court deems just and proper.

JURY DEMAND

Plaintiff demands a trial by jury.

DATED: December 29, 2022

Respectfully submitted,

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

By: Rachele R. Byrd
RACHELE R. BYRD

RACHELE R. BYRD
FERDEZA ZEKIRI
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4559
Facsimile: (619) 234-4599
byrd@whafh.com
zekiri@whafh.com

Attorneys for Plaintiff

29015v5

ClassAction.org