Michael A. Caddell (SBN 249469)
mac@caddellchapman.com
Cynthia B. Chapman (SBN 164471)
cbc@caddellchapman.com
Amy E. Tabor (SBN 297660)
aet@caddellchapman.com
CADDELL & CHAPMAN
P.O. Box 1311
Monterey CA 93942
Tel.: (713) 751-0400
Fax: (713) 751-0906

Foster C. Johnson
fjohnson@azalaw.com (SBN 289055)
David Warden (*pro hac vice forthcoming*)
dwarden@azalaw.com
Joseph Ahmad (*pro hac vice forthcoming*)
jahmad@azalaw.com
Nathan Campbell (*pro hac vice forthcoming*)
ncampbell@azalaw.com
AHMAD, ZAVITSANOS, & MENSING, P.C.
1221 McKinney Street, Suite 3460
Houston TX 77010
Tel: (713) 655-1101
Fax: (713) 655-0062

Attorneys for Plaintiff

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF LOS ANGELES

JANE DOE, individually and on behalf of others similarly situated,

Plaintiff,

v.

TORRANCE MEMORIAL MEDICAL CENTER,

Defendant.

CASE NO. 23STCV00395

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Jane Doe, individually and on behalf of all other California citizens similarly situated, brings suit against Defendant Torrance Memorial Medical Center ("Defendant" or "Torrance Memorial"), and upon personal knowledge as to Plaintiff's own conduct and on information and belief as to all other matters based upon investigation by counsel, alleges as follows:

I. SUMMARY OF ALLEGATIONS

1. This case arises from Defendant's systematic violation of the medical privacy rights of patients and users of Defendant's services, resulting in the disclosure of highly sensitive personal information to Facebook without those patients' or users' knowledge or consent.

2. Defendant's "Website Privacy Policy" tells patients and prospective patients that "Your privacy is very important to us."[1] Indeed, Defendant promises patients and prospective patients that "[w]e will not use or disclose your Health Information for marketing purposes without your written authorization."[2] Contrary to these assurances, Defendant does not follow these policies, nor does it follow the law prohibiting such disclosures.

3. Since at least 2017, Defendant has disclosed information about prospective and actual patients—including their status as actual or potential patients, their actual or potential physicians, their actual or potential medical treatments, the hospitals they visited or may visit, and their personal identities—to Facebook and other third parties without their knowledge, authorization, or consent.

4. Defendant discloses this protected health information through the deployment of various digital marketing and automatic rerouting tools embedded on its websites that purposefully and intentionally redirect personal health information to Facebook, who exploits that information for advertising purposes. Defendant's use of these rerouting tools causes personally

[1] https://www.torrancememorial.org/website-privacy-notice/

[2] https://www.tmphysiciannetwork.org/app/files/public/8fa720fb-71e9-47b9-aa4a-68bc32931845/Torrance%20Memorial%20Physician%20Network/Pt%20Privacy/Notice-of-Privacy-Practices-TMPN.pdf

identifiable information and the contents of communications exchanged between actual and prospective patients with Defendant to be automatically redirected to Facebook in violation of those patients' reasonable expectations of privacy, their rights as patients, their rights as citizens of California, and both the express and implied promises of Defendant.

5. Defendant's conduct in disclosing such protected health information to Facebook violates California law, including the California Invasion of Privacy Act ("CIPA"), CAL. PENAL CODE §§ 630, et seq.; the California Confidentiality of Medical Information Act ("CMIA"), CAL. CIVIL CODE §§ 56.06, 56.10, 56.101; the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), CAL. PENAL CODE § 502; and Invasion of Privacy and Violation of the California Constitution, ART. 1, § 1.

6. Plaintiff continues to desire to search for health information on Torrance Memorial's website. Plaintiff will continue to suffer harm if the website is not redesigned. If the website were redesigned to comply with applicable laws, Plaintiff would use the Torrance Memorial website to search for health information in the future.

7. On behalf of herself and all similarly situated persons, Plaintiff seeks an order enjoining Defendant from further unauthorized disclosures of personal information; awarding statutory damages in the amount of at least $5,000 per violation, attorneys' fees and costs; and granting any other preliminary or equitable relief the Court deems appropriate.

II. PARTIES

A. Plaintiff

8. Plaintiff Jane Doe is a resident of Los Angeles County, California.

9. Plaintiff Jane Does has used the Torrance Memorial website to search for Torrance Memorial doctors and medical treatment.

10. Plaintiff Jane Doe's use of the Torrance Memorial website entailed providing Jane Doe's sensitive medical information, such as conditions for which she was seeking treatment.

11. Plaintiff Jane Doe has been a patient at Defendant Torrance Memorial Medical Center.[3]

B. Defendant

12. Defendant Torrance Memorial Medical Center is a California corporation with its principal place of business located at 3300 Lomita Blvd, Torrance, California 90505.

III. JURISDICTION AND VENUE

13. This Court has jurisdiction over Defendant because it regularly conducts business in California, including in Los Angeles County, and has its principal place of business in California.

14. Venue is appropriate in this Court because the injuries giving rise to the alleged causes of action occurred in Los Angeles County and because Plaintiff Jane Doe resided in Los Angeles County at the time the offer of services for personal use was made by Defendant. *See* CAL. C.C.P. §§ 395(a) & 395(b). Venue is also appropriate in this Court because Los Angeles County is the county in which the cause, or some part of the cause, arose for the recovery of a penalty imposed by statute. *See* CAL. C.C.P. § 393(a).

IV. FACTUAL BACKGROUND

15. Plaintiff Jane Doe visited Defendant's website to look for doctors, research treatments, and investigate her insurance options at https://www.torrancememorial.org/. Plaintiff had concerns about a concussion she had suffered and about receiving healthcare to help with her recovery. Plaintiff entered data on Torrance Memorial's website, including sensitive medical information and details about her medical condition. She also searched for a doctor on Torrance Memorial's website to help her with treatment.

16. Unbeknownst to Plaintiff Jane Doe, Torrance Memorial had embedded computer code on its website that took every search term she entered and every page of the site she visited and sent that information directly to Facebook, the largest and most profitable social media

[3] https://www.torrancememorial.org/

company on the planet. Torrance Memorial accomplished this by installing Facebook's "Meta Pixel" tool on almost every page of Torrance Memorial's website. The Meta Pixel worked like a listening device. Each time Plaintiff Jane Doe typed a search term, the Meta Pixel recorded the information she entered and transmitted it to Facebook, along with identifying information that let Facebook know exactly who Jane Doe was. Instantaneously, Facebook knew that Jane Doe was interested in medical treatment for her concussion. Facebook then took this information and added it to all of the other information it keeps about consumers, matching Jane Doe's interest in medical treatment with her Facebook profile, name, address, interests, and other websites she had visited. This information then became available for Facebook's advertisers to use when Facebook sold them targeted advertising services.

17. Plaintiff was surprised and troubled that information she believed was being communicated only to Torrance Memorial for the purpose of obtaining medical treatment had been sent to Facebook and used to target advertisements to her. Plaintiff subsequently learned that thousands of Torrance Memorial patients like her had similarly had their privacy rights violated. Most of these consumers were likely not even aware of this privacy violation, much less able to hire counsel to stop the illegal conduct. Plaintiff therefore now brings these claims to correct Torrance Memorial's privacy violations and obtain relief for herself and thousands of similarly situated consumers.

V. CLASS ACTION ALLEGATIONS

A. Defendant routinely discloses the protected health information of patients and users of its services to Facebook.

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

19. Medical patients and those seeking medical treatment in California such as Jane Doe have a legal interest in preserving the confidentiality of their communications with health

care providers and have reasonable expectations of privacy that their personally identifiable information and communications will not be disclosed to third parties by Defendant without their express written consent and authorization.

20. As a health care provider, Defendant has common law and statutory duties to protect the confidentiality of patient information and communications.

21. Defendant expressly and impliedly promises patients that it will maintain and protect the confidentiality of personally identifiable patient information and communications.

22. Defendant operates websites for current and prospective patients, including https://www.torrancememorial.org/.

23. Defendant's websites are designed for interactive communication with patients and users, including scheduling appointments, searching for physicians, paying bills, requesting medical records, learning about medical issue treatment options, and joining support groups.

24. Notwithstanding prospective and current patients' reasonable expectations of privacy, Defendant's legal duties of confidentiality, and Defendant's express promises to the contrary, Defendant discloses the contents of prospective and current patients' communications and protected healthcare information via automatic re-routing mechanisms embedded in the websites operated by Defendant without patients' knowledge, authorization, or consent.

B. The Nature of Defendant's Unauthorized Disclosure of Patients' Health Care Information

25. Defendant's disclosure of current and prospective patients' personal healthcare information occurs because Defendant intentionally deploys source code on the websites it operates, including https://www.torrancememorial.org, that causes current and prospective patients' personally identifiable information (as well as the exact contents of their communications) to be transmitted to third parties.

26. By design, third parties receive and record the exact contents of these communications before the full response from Defendant has been rendered on the screen of the

patient's or user's computer device and while the communication with Defendant remains ongoing.

27. Websites like those maintained by Defendant are hosted by a computer server through which the businesses in charge of the website exchange and communicate with internet users via their web browsers.

28. The basic command that web browsers use to exchange data and user communications is called a GET request.[4] For example, when a patient types "heart failure treatment" into the search box on Defendant's website and hits 'Enter,' the patient's web browser makes a connection with the server for Defendant's website and sends the following request: "GET search/q=heart+failure+treatment."

29. When a server receives a GET request, the information becomes appended to the next URL (or "Uniform Resource Locator") accessed by the user. For example, if a user enters "respiratory problems" into the query box of a website search engine, and the search engine transmits this information using a GET request method, then the words "respiratory" and "problems" will be appended to the query string at the end of the URL of the webpage showing the search results.

30. The other basic transmission command utilized by web browsers is POST, which is typically employed when a user enters data into a form on a website and clicks 'Enter' or some other form of submission button. POST sends the data entered in the form to the server hosting the website that the user is visiting.

31. In response to receiving a GET or POST command, the server for the website with which the user is exchanging information will send a set of instructions to the web browser and command the browser with source code that directs the browser to render the website's responsive communication.

[4] https://www.w3schools.com/tags/ref_httpmethods.asp

32. Unbeknownst to most users, however, the website's server may also redirect the user's communications to third parties. Typically, users are given no notice that these disclosures are being made. Third parties (such as Facebook and Google) use the information they receive to track user data and communications for marketing purposes.

33. In many cases, third-party marketing companies acquire the content of user communications through a 1x1 pixel (the smallest dot on a user's screen) called a tracking pixel, a web-bug, or a web beacon. These tracking pixels are tiny and are purposefully camouflaged to remain invisible to users.

34. Tracking pixels can be placed directly on a web page by a developer, or they can be funneled through a "tag manager" service to make the invisible tracking run more smoothly. A tag manager further obscures the third parties to whom user data is transmitted.

35. These tracking pixels can collect dozens of data points about individual website users who interact with a website. One of the world's most prevalent tracking pixels, called the Meta Pixel, is provided by Facebook.

36. A web site developer who chooses to deploy third-party source code, like a tracking pixel, on their website must enter the third-party source code directly onto their website for every third party they wish to send user data and communications. This source code operates invisibly in the background when users visit a site employing such code.

C. Tracking pixels provide third parties with a trove of personally identifying data permitting them to uniquely identify the individuals browsing a website.

37. Tracking pixels are lines of source code embedded in websites such as Defendant's. Tracking pixels are particularly pernicious because they result in the disclosure of a variety of data that permits third parties to determine the unique personal identities of website visitors. While most users believe that the internet provides them with anonymity when, for example, they browse a hospital website for treatment information about a medical condition, that is not the case when the hospital website has embedded third party tracking devices, as Defendant has.

38. For example, an IP address is a number that identifies a computer connected to the internet. IP addresses are used to identify and route communications on the internet. IP addresses of individual users are used by internet service providers, websites, and tracking companies to facilitate and track internet communications and content. IP addresses also offer advertising companies like Facebook a unique and semi-persistent identifier across devices—one that has limited privacy controls.[5]

39. Because of their uniquely identifying character, IP addresses are considered protected personally identifiable information. Tracking pixels can (and typically do) collect website visitors' IP addresses.

40. Likewise, internet cookies also provide personally identifiable information. Cookies are small text files that web servers can place on a user's browser and computer when a user's browser interacts with a website server. Cookies are typically designed to acquire and record an individual internet user's communications and activities on websites and were developed by programmers to aid with online advertising.

41. Cookies are designed to operate as a means of identification for internet users. Advertising companies like Facebook and Google have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell targeted advertising that is customized to a user's personal communications and browsing history. To build individual profiles of internet users, third party advertising companies assign each user a unique (or a set of unique) identifiers to each user.

42. Cookies are considered personal identifiers, and tracking pixels can collect cookies from website visitors.

[5] https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/

43. A third type of personally identifying information is what data companies refer to as a "browser-fingerprint." A browser-fingerprint is information collected about a computing device that can be used to identify the specific device.

44. These browser-fingerprints can be used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked and can provide a wide variety of data. As Google explained, "With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."[6] The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it employs much more subtle techniques.[7] Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.[8]

45. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.[9]

46. Browser-fingerprints are considered personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors.

47. A fourth kind of personally identifying information is the unique user identifier (such as Facebook's "Facebook ID") that permits companies like Facebook to quickly and automatically identify the personal identity of its user across the internet whenever the identifier is encountered. A Facebook ID is a number string that is connected to a user's Facebook profile.[10] Anyone with access to a user's Facebook ID can locate a user's Facebook profile.[11]

[6] https://www.blog.google/products/chrome/building-a-more-private-web/

[7] https://pixelprivacy.com/resources/browser-fingerprinting/

[8] https://www.blog.google/products/chrome/building-a-more-private-web/

[9] https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/

[10] https://www.facebook.com/help/211813265517027

[11] https://smallseotools.com/find-facebook-id/

48. Unique personal identifiers such as a person's Facebook ID are likewise capable of collection through pixel trackers.

D. Facebook's Business Model: Exploiting User Data to Sell Advertising

49. Facebook, a social media platform founded in 2004 and today operated by Meta Platforms, Inc., was originally designed as a social networking website for college students.

50. Facebook describes itself as a "real identity" platform.[12] This means that users are permitted only one account and must share "the name they go by in everyday life."[13] To that end, Facebook requires users to provide their first and last names, along with their birthday, telephone number and/or email address, and gender, when creating an account.[14]

51. In 2007, realizing the value of having direct access to millions of consumers, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming this service to be a "completely new way of advertising online," that would allow "advertisers to deliver more tailored and relevant ads."[15] Facebook has since evolved into one of the largest advertising companies in the world.[16] Facebook can target users so effectively because it surveils user activity both on and off its website through the use of tracking pixels.[17] This allows Facebook to make inferences about users based on their interests, behavior, and connections.[18]

52. Today, Facebook provides advertising on its own social media platforms, as well as other websites through its Facebook Audience Network. Facebook has more than 2.9 billion users.[19]

---

[12] https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701#:~:text=Facebook%20said%20in%20its%20most,of%20them%20than%20developed%20ones.

[13] https://transparency fb.com/policies/community-standards/account-integrity-and-authentic-identity/

[14] https://www.facebook.com/help/406644739431633

[15] https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/

[16] https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/

[17] https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[18] https://www.facebook.com/business/ads/ad-targeting

[19] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

53. Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications. These profiles are associated with personal identifiers, including IP addresses, cookies, and other device identifiers. Facebook also tracks non-users across the web through its internet marketing products and source code. Facebook employs algorithms, powered by machine learning tools, to determine what advertisements to show users based on their habits and interests, and utilizes tracking software such as the Meta Pixel to monitor and exploit users' habits and interests.

54. Tracking information about users' habits and interests is a critical component of Facebook's business model because it is precisely this kind of information that allows Facebook to sell advertising to its customers.

55. Facebook offers several advertising options based on the type of audience that an advertiser wants to target. Those options include targeting "Core Audiences," "Custom Audiences," "Look Alike Audiences," and even more granulated approaches within audiences called "Detailed Targeting." Each of Facebook's advertising tools allows an advertiser to target users based, among other things, on their personal data, including geographic location, demographics (e.g., age, gender, education, job title, etc.), interests, (e.g., preferred food, movies), connections (e.g., particular events or Facebook pages), and behaviors (e.g., purchases, device usage, and pages visited). This audience can be created by Facebook, the advertiser, or both working in conjunction.

56. Ad Targeting has been extremely successful due to Facebook's ability to target individuals at a granular level. For example, among many possible target audiences, "Facebook offers advertisers 1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"[20] Aided by highly granular data used to target specific

[20] https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings html

users, Facebook's advertising segment quickly became Facebook's most successful business unit, with millions of companies and individuals utilizing Facebook's advertising services.

E. Facebook's Meta Pixel tool allows Facebook to track the personal data of individuals across a broad range of third-party websites.

57. To power its advertising business, Facebook uses a variety of tracking tools to collect data about individuals, which it can then share with advertisers. These tools include software development kits incorporated into third-party applications, its "Like" and "Share" buttons (known as "social plug-ins"), and other methodologies, which it then uses to power its advertising business.

58. One of Facebook's most powerful tools is called the "Meta Pixel." Once a third-party like Defendant installs the Meta Pixel on its website, by default it begins sending user information to Facebook automatically.[21]

59. The Meta Pixel is a snippet of code embedded on a third-party website that tracks users' activities as users navigate through a website.[22] Once activated, the Meta Pixel "tracks the people and type of actions they take."[23] Meta Pixel can track and log each page a user visits, what buttons they click, as well as specific information that users input into a website.[24] The Meta Pixel code works by sending Facebook a detailed log of a user's interaction with a website such as clicking on a product or running a search via a query box. The Meta Pixel also captures information such as what content a user views on a website or how far down a web page they scrolled.[25]

60. When someone visits a third-party website page that includes the Meta Pixel code, the Meta Pixel code is able to replicate and send the user data to Facebook through a separate (but

[21] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector

[22] https://developers.facebook.com/docs/meta-pixel/

[23] https://www.facebook.com/business/goals/retargeting

[24] https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[25] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector

simultaneous) channel in a manner that is undetectable by the user.[26] The information sent to Facebook includes a referrer header (or "URL"), which includes significant information regarding the user's browsing history, including the identity of the individual internet user and the web server, as well as the name of the web page and the search terms used to find it.[27] These search terms and the resulting URLs divulge a user's personal interests, queries, and habits on third-party websites operating outside of Facebook's own platform. In this manner, Facebook tracks users' browsing histories on third-party websites and compiles these browsing histories into personal profiles which are sold to advertisers to generate revenue.[28]

61. For example, if Meta Pixel is incorporated on a shopping website, it may log what searches a user performed, which items of clothing a user clicked on, whether they added an item to their cart, as well as what they purchased. Along with this data, Facebook also receives personally identifying information like IP addresses, Facebook IDs, and other data that allow Facebook to identify the user. All this personally identifying data is included each time the Meta Pixel forwards a user's interactions with a third-party website to Facebook's servers. Once Facebook receives this information, Facebook processes it, analyzes it, and assimilates it into datasets like its Core Audiences and Custom Audiences. Facebook can then sell this information to companies who wish to display advertising for products similar to what the user looked at on the original shopping website.

62. These communications with Facebook happen silently, without users' knowledge. By default, the transmission of information to Facebook's servers is invisible. Facebook's Meta Pixel allows third-party websites to send users' personal information to match them with Facebook or Instagram profiles, even if they are not logged into Facebook at the time.[29]

[26] *See, e.g., In re Facebook, Inc. Internet Tracking Litigation,* 956 F.3d 589, 596 (9th Cir. 2020) (explaining functionality of Facebook software code on third-party websites).

[27] *In re Facebook*, 956 F.3d at 596.

[28] *In re Facebook*, 956 F.3d at 596.

[29] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector

63. In exchange for installing its Meta Pixel, Facebook provides website owners like Defendant with analytics about the ads they've placed on Facebook and Instagram and tools to target people who have visited their website.[30]

64. Facebook shares analytic metrics with the website host, while at the same time sharing the information it collects with third-party advertisers who can then target users based on the information collected and shared by Facebook.

65. Facebook touted Meta Pixel (which it originally called "Facebook Pixel") as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website."[31] According to Facebook, the Meta Pixel is an analytics tool that allows business to measure the effectiveness of their advertising by understanding the actions people take on their websites."[32]

66. Facebook warns web developers that its Pixel is a personal identifier because it enables Facebook "to match your website visitors to their respective Facebook User accounts."[33]

67. Facebook recommends that its Meta Pixel code be added to the base code on every website page (including the website's persistent header) to reduce the chance of browsers or code from blocking Pixel's execution and to ensure that visitors will be tracked.[34]

68. Once Meta Pixel is installed on a business's website, the Meta Pixel tracks users as they navigate through the website and logs which pages are visited, which buttons are clicked, the specific information entered in forms (including personal information), as well as "optional values" set by the business website.[35] Meta Pixel tracks this data regardless of whether a user is

[30] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

[31] https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/

[32] https://www.oviond.com/understanding-the-facebook-pixel

[33] https://developers.facebook.com/docs/meta-pixel/get-started

[34] https://developers.facebook.com/docs/meta-pixel/get-started

[35] https://developers.facebook.com/docs/meta-pixel/

logged into Facebook.[36] It is unclear how Facebook exploits the data collected from nonusers, but when asked by Congress about Facebook's business practices, Mark Zuckerberg conceded that company maintains "shadow profiles" on nonusers of Facebook.[37]

69. For Facebook, the Meta Pixel tool embedded on third-party websites acts as a conduit for information, sending the information it collects to Facebook through scripts running in a user's internet browser, similar to how a "bug" or wiretap can capture audio information. The information is sent in data packets, which include personally identifying data such as a user's IP address.

70. For example, the Meta Pixel is configured to automatically collect "HTTP Headers" and "Pixel-specific data."[38] HTTP headers collect data including "IP addresses, information about the web browser, page location, document, referrer and person using the website."[39] Pixel-specific data includes such data as the "Pixel ID and the Facebook Cookie."[40]

71. Meta Pixel takes the information it harvests and sends it to Facebook with personally identifiable information, such as a user's IP address, name, email, phone number, and specific Facebook ID, which identifies an individual's Facebook user account. Anyone who has access to this Facebook ID can use this identifier to quickly and easily locate, access, and view a user's corresponding Facebook profile. Facebook stores this information on its servers, and, in some instances, maintains this information for years.[41]

72. Facebook has a number of ways to uniquely identify the individuals whose data is being forwarded from third-party websites through the Meta Pixel.

---

[36] https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients

[37] https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/

[38] https://developers.facebook.com/docs/meta-pixel/

[39] https://developers.facebook.com/docs/meta-pixel/

[40] https://developers.facebook.com/docs/meta-pixel/

[41] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

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

74. Alternatively, Facebook can link the data to a user's Facebook account through the "Facebook Cookie."[42] The Facebook Cookie is a workaround to recent cookie-blocking applications used to prevent websites from tracking users.[43]

75. Facebook can also link user data to Facebook accounts through identifying information collected through Meta Pixel through what Facebook calls "Advanced Matching." These are two forms of Advanced Matching: manual matching and automatic matching.[44] Manual matching requires the website developer to manually send data to Facebook so that users can be linked to data. Automatic matching allows Meta Pixel to scour the data it receives from third-party websites to search for recognizable fields, including names and email addresses that correspond with users' Facebook accounts.

76. While the Meta Pixel tool "hashes" personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent *Facebook* from using the data.[45] In fact, Facebook explicitly uses the hashed information it gathers to link pixel data to Facebook profiles.[46]

77. Facebook also receives personally identifying information in the form of user's unique IP addresses that stay the same as users visit multiple websites. When browsing a third-party website that has embedded Facebook code, a user's unique IP address is forwarded to

[42] https://clearcode.cc/blog/facebook-first-party-cookie-adtech/

[43] https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/

[44] https://www.facebook.com/business/help/611774685654668?id=1205376682832142

[45] https://www.facebook.com/business/help/611774685654668?id=1205376682832142

[46] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

Facebook by GET requests, which are triggered by Facebook code snippets. The IP address enables Facebook to keep track of the website page visits associated with that address.

78. Facebook also places cookies on visitors' computers. It then uses these cookies to store information about each user. For example, the "c_user" cookie is a unique identifier that identifies a Facebook user's ID. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user has one—and only one—unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

79. The data supplied by the c_user cookie allows Facebook to identify the Facebook account associated with the cookie. One simply needs to log into Facebook, and then type www.facebook.com/#, with the c_user identifier in place of the "#." For example, the c_user cookie for Mark Zuckerberg is 4. Logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

80. Similarly, the "lu" cookie identifies the last Facebook user who logged in using a specific browser. Like IP addresses, cookies are included with each request that a user's browser makes to Facebook's servers. Facebook employs similar cookies such as "datr," "fr," "act," "presence," "spin," "wd," "xs," and "fbp" cookies to track users on websites across the internet.[47] These cookies allow Facebook to easily link the browsing activity of its users to their real-world identities, as well as such highly sensitive data as medical information, religion, and political preferences.[48]

81. Facebook also uses browser fingerprinting to uniquely identify individuals. Web browsers have several attributes that vary between users, like the browser software system, plugins that have been installed, fonts that are available on the system, the size of the screen, color depth, and more. Together, these attributes create a fingerprint that is highly distinctive. The

[47] https://techexpertise medium.com/facebook-cookies-analysis-e1cf6ffbdf8a#:~:text=browser%20session%20ends.-,%E2%80%9Cdatr%E2%80%9D,security%20and%20site%20integrity%20features.

[48] https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf

likelihood that two browsers have the same fingerprint is at least as low as 1 in 286,777, and the accuracy of the fingerprint increases when combined with cookies and the user's IP address. Facebook recognizes a visitor's browser fingerprint each time a Facebook button is loaded on a third-party website page. Using these various methods, Facebook can identify individual users, watch as they browse third-party websites like https://www.adventisthealth.org/, and target users with advertising based on their web activity.

F. Defendant has discreetly embedded the Meta Pixel tool on its website, resulting in the capture and disclosure of patients' and users' protected health information to Facebook.

82. A third-party website that incorporates Meta Pixel benefits from the ability to analyze a user's experience and activity on the website to assess the website's functionality and traffic. The third-party website also gains information from its customers through Meta Pixel that can be used to target them with advertisements, as well as to measure the results of advertising efforts.

83. Facebook's intrusion into the personal data of visitors to third-party websites incorporating the Meta Pixel is both significant and unprecedented. When Meta Pixel is incorporated into a third-party website, unbeknownst to users and without their consent, Facebook gains the ability to surreptitiously gather every user interaction with the website ranging from what the user clicks on to the personal information entered on a website search bar. Facebook aggregates this data against all websites.[49] Facebook benefits from obtaining this information because it improves its advertising network, including its machine-learning algorithms and its ability to identify and target users with ads.

84. Facebook provides websites using Meta Pixel with the data it captures in the "Meta Pixel page" in Events Manager, as well as tools and analytics to reach these individuals through future Facebook ads.[50] For example, websites can use this data to create "custom audiences" to

[49] https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[50] https://www.facebook.com/business/help/742478679120153?id=1205376682832142

target the specific Facebook user, as well as other Facebook users who match "custom audience's" criteria.[51] Businesses that use Meta Pixel can also search through Meta Pixel data to find specific types of users to target, such as men over a certain age.

85. Meta Pixel is wildly popular with businesses and embedded on millions of websites. Shockingly, Meta Pixel is incorporated on many websites that are used to store and convey sensitive medical information, which by law must be kept private. Recently, investigative journalists have determined that Meta Pixel is embedded on the websites of many of the top hospitals in the United States.[52] This results in sensitive medical information being collected and then sent to Facebook when a user interacts with these hospital websites. For example, when a user on many of these hospital websites clicks on a "Schedule Online" button next to a doctor's name, Meta Pixel sends the text of the button, the doctor's name, and the search term (such as "cardiology") used to find the doctor to Facebook. If the hospital's website has a drop-down menu to select a medical condition in connection with locating a doctor or making an appointment, that condition is also transmitted to Facebook through Meta Pixel.

86. Facebook has designed the Meta Pixel such that Facebook receives information about patient activities on hospital websites as they occur in real time. Indeed, the moment that a patient takes any action on a webpage that includes the Meta Pixel—such as clicking a button to create an appointment—Facebook code embedded on that page redirects the content of the patient's communications to Facebook while the exchange of information between the patient and hospital is still occurring.

87. Defendant is among the hospital systems who have embedded Meta Pixel on their websites. When a prospective or actual patient enters their personal information through Defendant's websites that incorporate Meta Pixel, such as to locate a doctor or make an appointment, this information, including what the patient is being treated for, is immediately and

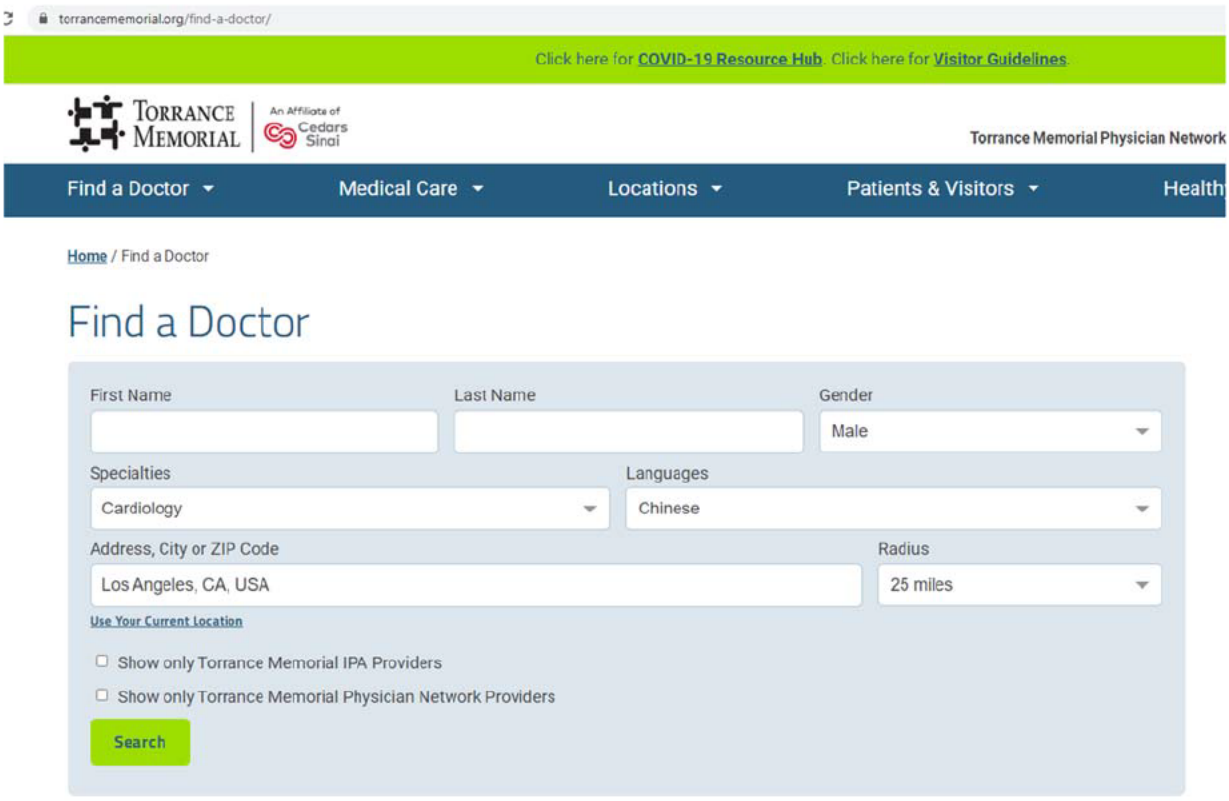
[51] https://developers.facebook.com/docs/marketing-api/reference/custom-audience/

[52] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

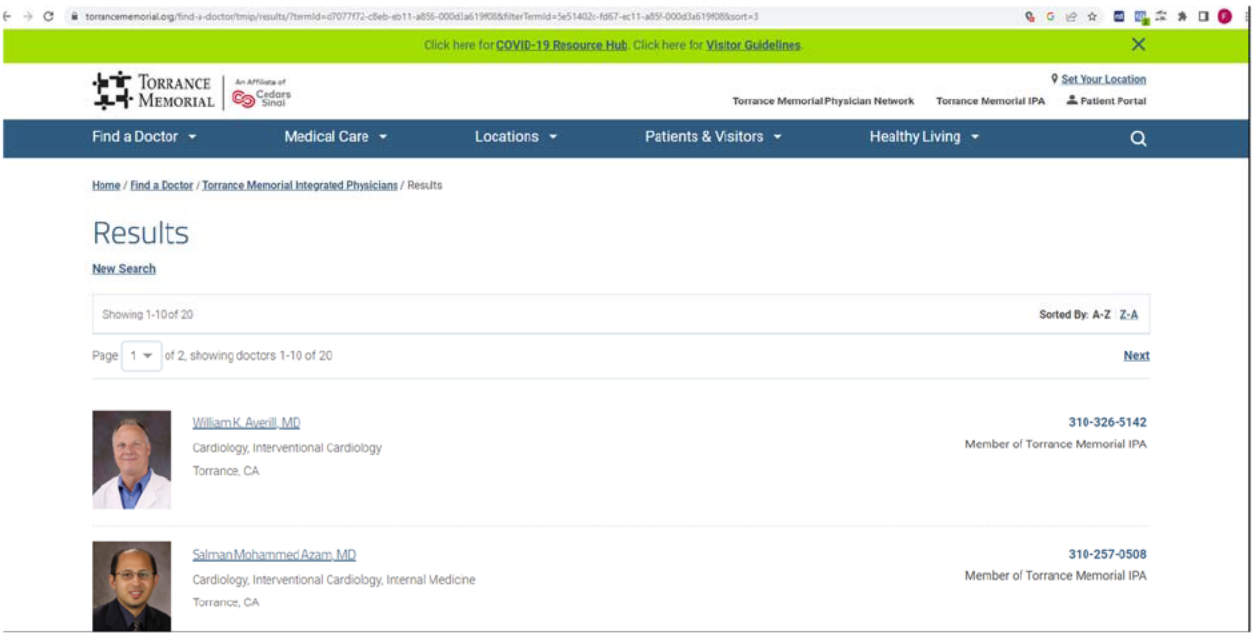
instantaneously transmitted to Facebook via the Meta Pixel. The acquisition and disclosure of these communications occurs contemporaneously with the transmission of these communications by patients.

88. This data, which can include health conditions (e.g., addiction, heart disease, cancer), diagnoses, procedures, test results, the treating physician, medications, and other personally identifying information ("Personal Health Information"), is obtained and used by Facebook, as well as other parties, for the purpose of targeted advertising.

89. For example, a visitor searching for a doctor on Defendant's website is asked to provide a variety of information to filter the various physicians available to treat various medical conditions, including the doctor's specialty and the prospective or actual patient's location:



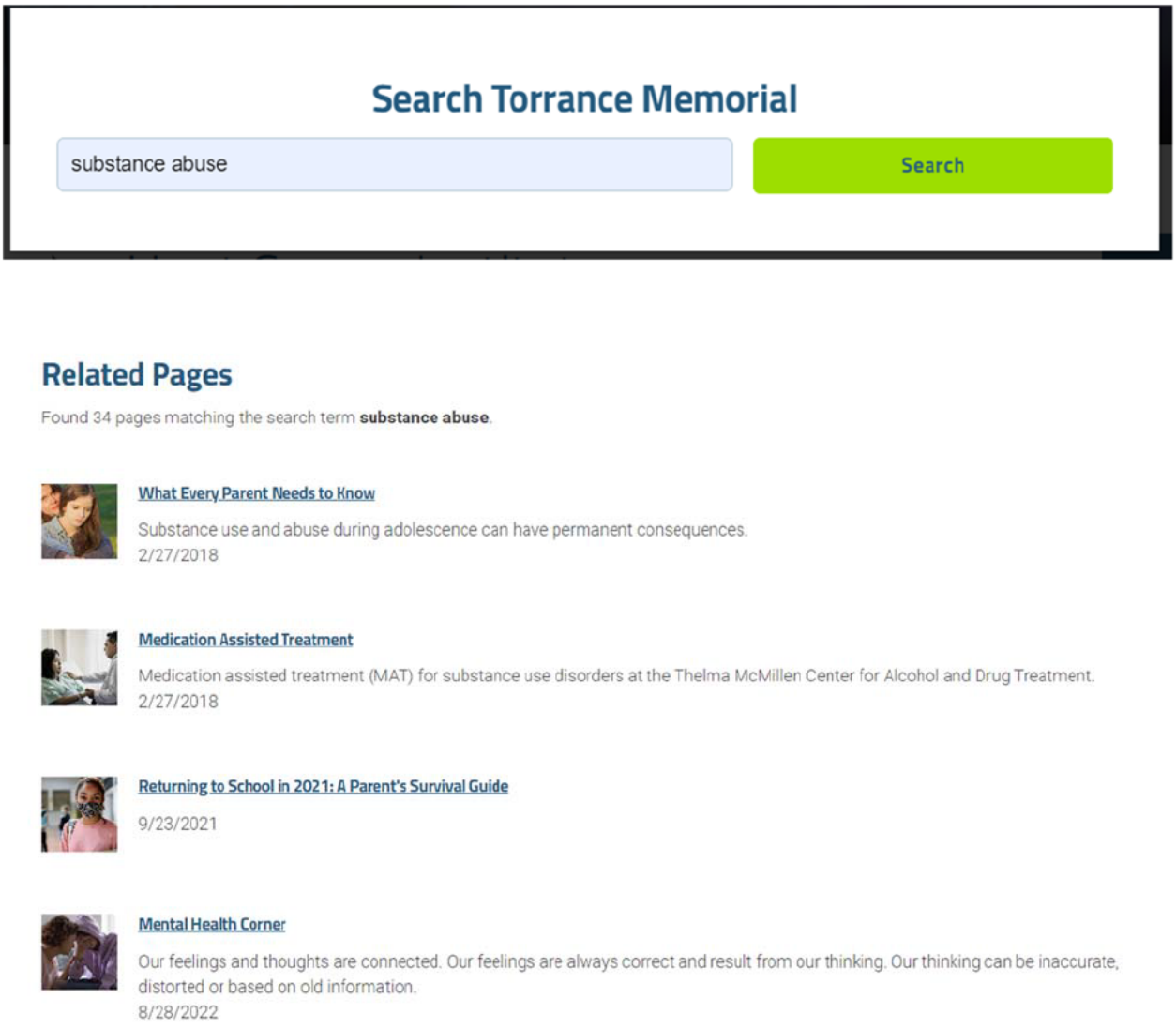
90. When a patient clicks on the "search" button, Defendant's website generates a list of providers that a patient can review and choose from:



91. All the data about patients' interactions with Defendant's website is disclosed to Facebook simultaneously in real time as visitors transmit their information, such as the doctor they choose for treatment, the doctor's specialty, the patient's location, and the patient's language and gender preferences. Along with other data, Defendant also discloses patients' unique Facebook IDs, which are captured by the c_user cookie, which allows Facebook to link this information to patients' unique Facebook accounts. Defendant also discloses other personally identifying information to Facebook, such as patient and user IP addresses, cookie identifiers, browser-fingerprints, and device identifiers.

92. Likewise, Defendant allows patients to search for information about "Medical Care" organized by specialty, such as "Cancer," "Heart Health," "Orthopedics, and "Maternal and Child." A patient searching for information about cancer treatment or pregnancy, however, not only shares their personal data with Defendant but also unknowingly shares their personal data with Facebook.

93. Defendant discloses such personally identifying information and sensitive medical information even when patients or users are searching for doctors to assist them with conditions such as substance abuse and addiction:



94. As the above demonstrates, knowing what information a patient is reviewing on Defendant's website can reveal deeply personal and private information. A simple search for "pregnancy" on Defendant's website tells Facebook that the patient is likely pregnant. Indeed, Facebook might know that the patient is pregnant before the patient's close family and friends. Likewise, most patients would not want it made public that they were seeking treatment for substance abuse. But there is nothing visible on Defendant's website that would indicate to patients that, when they use Defendant's search function, their personally identifiable data and the precise content of their communications with Defendant are being automatically transmitted

to Facebook for advertising purposes—even when patients search for treatment options for sensitive medical conditions such as cancer or substance abuse.

95. Defendant also discloses prospective and actual patient information from other sections of its website including (but not limited to) communications that are captured by the website's search bar, communications that are captured when a patient searches for classes and services offered by Defendant, and communications made when patients are researching specific medical conditions. The information that Facebook receives from Defendant includes a full-string, detailed URL, which contains such information as the name of the website, the pages patients are viewing, and search terms that patients have entered. Along with patients' communications, Defendant's website also causes the transmission of personally identifying data to Facebook, including patients' IP addresses, cookie identifiers, browser fingerprints, and device identifiers.

96. By compelling visitors to their websites to disclose personally identifying data and sensitive medical information to Facebook, Defendant knowingly disclosed information that allows Facebook and other advertisers to link patients' and visitors' Personal Health Information to their private identities and target them with advertising (or do whatever else Facebook may choose to do with this data, including running "experiments" on its customers by manipulating the information they are shown on their Facebook pages).[53] Defendant intentionally shares the Personal Health Information of its patients with Facebook in order to gain access to the benefits of the Meta Pixel tool.

97. For example, Plaintiff Jane Doe is an individual with a Facebook account who has also been a patient at Torrence Memorial Hospital. Plaintiff Jane Doe visited Defendant's website at www.torrencememorial.org approximately seven times and entered data, including sensitive medical information, such as details about her medical condition and search for a doctor. The

[53] https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/

information that Plaintiff Jane Doe transmitted included queries about treatment for a concussion that she had suffered.

98. Defendant knew that by embedding Meta Pixel—a Facebook advertising tool—it was permitting Facebook to collect, use, and share Plaintiff's and the Class Members' Personal Health Information, including sensitive medical information and personally identifying data. Defendant was also aware that such information would be shared with Facebook simultaneously with patients' interactions with its websites. Defendant made the decision to barter its patients' Personal Healthcare Information to Facebook because it wanted access to the Meta Pixel tool. While that bargain may have benefited Defendant and Facebook, it also betrayed the privacy rights of Plaintiff and Class Members.

G. Plaintiff and the Class Members did not consent to the interception and disclosure of their protected health information.

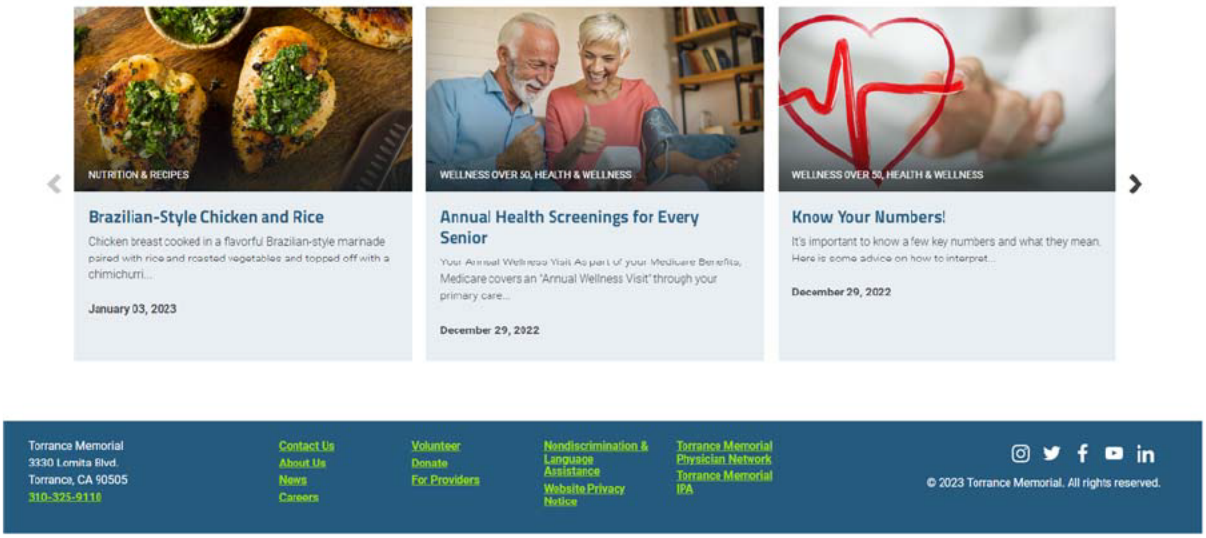
99. Plaintiff and Class Members had no idea when they interacted with Defendant's websites that their personal data, including sensitive medical data, was being collected and simultaneously transmitted to Facebook. That is because, among other things, the Meta Pixel tool is seamlessly and secretly integrated into Defendant's websites and is invisible to patients visiting those websites.

100. For example, when Plaintiff Jane Doe visited Defendant's website at https://www.torrancememorial.org/, there was no indication that Meta Pixel was embedded on that website or that it would collect and transmit her sensitive medical data to Facebook.

101. Plaintiff and fellow Class Members could not consent to Defendant's conduct when there was no indication that their sensitive medical information would be collected and transmitted to Facebook in the first place.

102. While Defendant purports to have a "Privacy Notice," that Privacy Notice is effectively hidden from patients, concealed at the bottom of Defendant's homepage in type so small as to be unreadable to many visitors[54]:

[54] https://www.torrancememorial.org/



103. Moreover, Defendant's "Website Privacy Notice" gives no indication to patients that Defendant routinely allows Facebook to capture and exploit patients' and users' Personal Health Information. Indeed, Defendant expressly promised in its "Website Privacy Notice" that "Your privacy is very important to us" and that Defendant "will not sell or otherwise provide the information that we collect to outside third parties for the purpose of direct or indirect mass email marketing."[55] These statements are false and misleading because Defendant in fact discloses patients' Personal Health Information to Facebook so that Facebook can solicit patients with advertising.

104. Defendant also promised in its "Website Privacy Notice" that it would "follow generally accepted industry standards to protect the information submitted to us, both during transmission and once we receive it."[56] This statement is also false and misleading because hospital systems who comply with generally accepted industry standards for protecting patients' Personal Health Information do not deploy source code on their websites that results in patients' Personal Health Information being disclosed to third-party advertising companies.

[55] https://www.torrancememorial.org/website-privacy-notice/

[56] https://www.torrancememorial.org/website-privacy-notice/

105. Defendant also falsely promises patients in its "Website Privacy Policy" that its policy "will inform you of the information that we, Torrance Memorial, may collect from you, and how it is used." This statement is false and misleading because Defendant nowhere discloses in its "Website Privacy Policy" that patients' Personal Health Information is routinely disclosed to Facebook when patients interact with Defendant's website.

106. Similarly, while disclosing that its website contains "cookies," Defendant falsely promises that "[u]sage of a cookie is in no way linked to any personally identifiable information on our site."[57] Contrary to that promise, Defendant's website automatically transmits personally identifying information to Facebook via multiple cookies, including the c_user cookie (i.e., the "Facebook cookie") which permits Facebook to link users' website queries to their Facebook profiles.

107. Even if a visitor stumbled upon Defendant's carefully hidden "Website Privacy Notice," nothing in that notice would be understood by any reasonable prospective or current patient to mean that Defendant is bartering its patients' Personal Health Information in return for access to Facebook's Meta Pixel tool. Indeed, Defendant expressly promises that it will not sell or otherwise provide the information it collects to outside third parties. Accordingly, Patients visiting Defendant's website likely feel assured that their communications about medical conditions such as addiction, cancer, and pregnancy will remain private, not realizing that Defendant has already transmitted this private information to Facebook, so that Facebook can monetize this information by sending targeted content and advertisements to patients.

108. Defendant's promises are unsurprising. Defendant does not have a legal right to share Plaintiff's and Class Members' Protected Health Information with Facebook, because this information is protected from such disclosure by law. *See, e.g.*, CAL. CIV. CODE §§ 56 *et seq.*; 45 C.F.R. § 164.508. Defendant is not permitted to disclose patients' Protected Health Information to

[57] https://www.torrancememorial.org/website-privacy-notice/

an advertising and marketing company like Facebook without express written authorization from patients.

109. Defendant failed to obtain a valid written authorization from Plaintiff or any of the Class Members to allow the capture and exploitation of their personally identifiable information and the contents of their communications by third parties for their own direct marketing uses. Moreover, no *additional* privacy breach by Facebook is necessary for harm to have accrued to Plaintiff and Class Members; the secret disclosure by Defendant of its patients' Personal Health Information to Facebook means that a significant privacy injury has *already occurred.*

110. Likewise, a prospective or current patient's reasonable expectation that their health care provider will not share their information with third parties for marketing purposes is not subject to waiver via an inconspicuous privacy policy hidden away on a company's website. Such "Browser-Wrap" statements do not create an enforceable contract against consumers. Further, Defendant expressly promised that it would not sell, rent, license, or trade their personally identifiable information for marketing purposes without express authorization.

111. Neither Plaintiff nor Class Members knowingly consented to Defendant's disclosure of their Personal Health Information to Facebook. Nowhere in Defendant's privacy policy is it disclosed that Defendant routinely transmits patients' Personal Health Information to third party advertising companies like Facebook so that those companies can monetize and exploit patients' health data. Without disclosing such practices, Defendant cannot have secured consent from Plaintiff and Class Members for the disclosure of their Personal Health Information to Facebook and other third-party advertising companies.

112. Accordingly, Defendant lacked authorization to intercept, collect, and disclose Plaintiff's and Class Members' Personal Health Information to Facebook or aid in the same.

H. The disclosures of personal patient data to Facebook are unnecessary.

113. There is no information anywhere on the websites operated by Defendant that would alert patients that their most private information (such as their identifiers, their medical

conditions, and their medical providers) is being automatically transmitted to Facebook. Nor are the disclosures of patient Personal Health Information to Facebook necessary for Defendant to maintain their healthcare website or provide medical services to patients.

114. For example, it is possible for a healthcare website to provide a doctor search function without allowing disclosures to third-party advertising companies about patient sign-ups or appointments. It is also possible for a website developer to utilize tracking tools without allowing disclosure of patients' Personal Healthcare Information to companies like Facebook. Likewise, it is possible for Defendant to provide medical services to patients without sharing their Personal Health Information with Facebook so that this information can be exploited for advertising purposes.

115. Despite these possibilities, Defendant willfully chose to implement Meta Pixel on its websites and aid in the disclosure of personally identifiable information and sensitive medical information about its patients, as well as the contents of their communications with Defendant, to third parties, including Facebook.

I. Plaintiff and Class Members have a reasonable expectation of privacy in their Personal Health Information, especially with respect to sensitive medical information.

116. Plaintiff and Class Members have a reasonable expectation of privacy in their Personal Health Information, including personally identifying data and sensitive medical information. Defendant's surreptitious interception, collection, and disclosure of Personal Health Information to Facebook violated Plaintiff and Class Member's privacy interests.

117. Patient health information is specifically protected by law. The prohibitions against disclosing patient Personal Health Information include prohibitions against disclosing personally identifying data such as patient names, IP addresses, and other unique characteristics or codes. *See, e.g.*, CAL. CIV. CODE § 56.05 ("medical information"); 45 C.F.R. § 164.514.

118. Given the application of these laws to Defendant, coupled with Defendant's express promises that they would protect the confidentiality of patients' Personal Health

Information, Plaintiff and the Members of the Class had a reasonable expectation of privacy in their protected health information.

119. Several studies examining the collection and disclosure of consumers' sensitive medical information confirm that the disclosure of sensitive medical information violates expectations of privacy that have been established as general social norms.

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

121. For example, a recent study by *Consumer Reports* showed that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believed that internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[58]

122. Users act consistently with these preferences. For example, following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to share data when prompted.[59]

123. "Patients are highly sensitive to disclosure of their health information," particularly because it "often involves intimate and personal facts, with a heavy emotional overlay." Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 621 (2002). Unsurprisingly, empirical evidence demonstrates that "[w]hen asked, the overwhelming majority of Americans express concern about the privacy of their medical records." Sharona Hoffman & Andy Podgurski, *E-Health Hazards:*

[58] https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/

[59] https://www.wired.co.uk/article/apple-ios14-facebook

Provider Liability and Electronic Health Record Systems, 24 BERKLEY TECH L.J. 1523, 1557 (2009).

124. The concern about sharing personal medical information is compounded by the reality that advertisers view this type of information as particularly valuable. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one recent article noted, "What is particularly worrying about this process of datafication of children is that companies like [Facebook] are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[60]

125. Many privacy law experts have expressed serious concerns about patients' sensitive medical information being disclosed to third-party companies like Facebook. As those critics have pointed out, having a patient's Personal Health Information disseminated in ways the patient is unaware of could have serious repercussions, including affecting their ability to obtain life insurance, how much they might pay for such coverage, the rates they might be charged on loans, and the likelihood of their being discriminated against.

126. Plaintiff's Personal Health Information that Defendant collected, monitored, disclosed, and used is Plaintiff's property, has economic value, and its illicit disclosure has caused Plaintiff harm.

127. It is common knowledge that there is an economic market for consumers' personal data—including the kind of data that Defendant has collected and disclosed from Plaintiff and Class Members.

128. In 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, "age, gender and location information" were being sold for approximately "$0.50 per 1,000 people."[61]

[60] https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/

[61] https://ig ft.com/how-much-is-your-personal-data-worth/

129. In 2015, *TechCrunch* reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about "$0.30" per name.[62] That same article noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge" and that the value of a single user's data can vary from $15 to more than $40 per user.[63]

130. In a 2021 Washington Post article, the legal scholar Dina Srinivasan said that consumers "should think of Facebook's cost as [their] data and scrutinize the power it has to set its own price."[64] This price is only increasing. According to Facebook's own financial statements, the value of the average American's data in advertising sales rose from $19 to $164 per year between 2013 and 2020.[65]

131. Despite the protections afforded by law, there is an active market for health information. Medical information obtained from health providers garners substantial value because of the fact that it is not generally available to third party data marketing companies because of the strict restrictions on disclosure of such information by state laws and provider standards, including the Hippocratic oath. Even with these restrictions, however, a multi-billion-dollar market exists for the sale and purchase of such private medical information.[66]

132. Further, individuals can sell or monetize their own data if they so choose. For example, Facebook has offered to pay individuals for their voice recordings,[67] and has paid teenagers and adults up to $20 per month plus referral fees to install an app that allows Facebook to collect data on how individuals use their smart phones.[68]

---

[62] https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/

[63] https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/

[64] https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/

[65] https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/

[66] https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it/; *see also https://slate.com/technology/2022/06/health-data-brokers-privacy.html*

[67] https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounnciations-app

[68] https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch html

133. A myriad of other companies and apps such as DataCoup, Nielsen Computer, Killi, and UpVoice also offer consumers money in exchange for access to their personal data.[69]

134. Given the monetary value that data companies like Facebook have already paid for personal information in the past, Defendant has deprived Plaintiff and the Class Members of the economic value of their sensitive medical information by collecting, using, and disclosing that information to Facebook without consideration for Plaintiff and the Class Member's property.

J. Defendant is enriched by making unlawful, unauthorized, and unnecessary disclosures of patients' and users' protected health information.

135. In exchange for disclosing Personal Health Information about its patients and users, Defendant is compensated by Facebook with enhanced online advertising services, including (but not limited to) retargeting and enhanced analytics functions.

136. Retargeting is a form of online targeted advertising that targets users with ads based on their previous internet actions, which is facilitated through the use of cookies and tracking pixels. Once an individual's data is disclosed and shared with a third-party marketing company, the advertiser is able to show ads to the user elsewhere on the internet.

137. For example, retargeting could allow a web-developer to show advertisements on other websites to customers or potential customers based on the specific communications exchanged by a patient or their activities on a website. Using the Meta Pixel, a website could target ads on Facebook itself or on the Facebook advertising network. The same or similar advertising can be accomplished via disclosures to other third-party advertisers and marketers.

138. Once personally identifiable information relating to patient communications is disclosed to third parties like Facebook, Defendant loses the ability to control how that information is subsequently disseminated and exploited.

139. The monetization of the data being disclosed by Defendant, both by Defendant and Facebook, demonstrates the inherent value of the information being collected.

[69] https://www.creditdonkey.com/best-apps-data-collection.html; *see also https://www.monetha.io/blog/rewards/earn-money-from-your-data/*

K. Facebook's History of Egregious Privacy Violations

140. Defendant knew or should have known that Facebook could not be trusted with its patients' sensitive medical information.

141. Due to its ability to target individuals based on granular data, Facebook's ad-targeting capabilities have frequently come under scrutiny. For example, in June 2022, Facebook entered into a settlement with the Department of Justice regarding its Lookalike Ad service, which permitted targeted advertising by landlords based on race and other demographics in a discriminatory manner. That settlement, however, reflected only the latest in a long history of egregious privacy violations by Facebook.

142. In 2007, when Facebook launched "Facebook Beacon," users were unaware that their online activity was tracked, and that the privacy settings originally did not allow users to opt-out. As a result of widespread criticism, Facebook Beacon was eventually shut down.

143. Two years later, Facebook made modifications to its Terms of Service, which allowed Facebook to use anything a user uploaded to its site for any purpose, at any time, even after the user ceased using Facebook. The Terms of Service also failed to provide for any way for users to completely delete their accounts. Under immense public pressure, Facebook eventually returned to its prior Terms of Service.

144. In 2011, Facebook settled charges with the Federal Trade Commission relating to its sharing of Facebook user information with advertisers, as well as its false claim that third-party apps were able to access only the data they needed to operate when—in fact—the apps could access nearly all of a Facebook user's personal data. The resulting Consent Order prohibited Facebook from misrepresenting the extent to which consumers can control the privacy of their information, the steps that consumers must take to implement such controls, and the extent to which Facebook makes user information available to third parties.[70]

[70] https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter

145. Facebook found itself in another privacy scandal in 2015 when it was revealed that Facebook could not keep track of how many developers were using previously downloaded Facebook user data. That same year, it was also revealed that Facebook had violated users' privacy rights by harvesting and storing Illinois' users' facial data from photos without asking for their consent or providing notice. Facebook ultimately settled claims related to this unlawful act for $650 million.

146. In 2018, Facebook was again in the spotlight for failing to protect users' privacy. Facebook representatives testified before Congress that a company called Cambridge Analytica may have harvested the data of up to 87 million users in connection with the 2016 election. This led to another FTC investigation in 2019 into Facebook's data collection and privacy practices, resulting in a record-breaking five-billion-dollar settlement.

147. Likewise, a different 2018 report revealed that Facebook had violated users' privacy by granting access to user information to over 150 companies.[71] Some companies were even able to read users' private messages.

148. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[72] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

149. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that

[71] https://www.cnbc.com/2018/12/19/facebook-gave-amazon-microsoft-netflix-special-access-to-data-nyt.html

[72] https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/

"[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective … at preventing the receipt of sensitive data."[73]

150. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[74] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[75]

151. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose."[76]

152. These revelations were confirmed by an article published by the Markup in 2022, which found during the course of its investigation that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included

[73] https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf

[74] https://slate.com/technology/2022/06/health-data-brokers-privacy.html

[75] https://slate.com/technology/2022/06/health-data-brokers-privacy.html

[76] https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes

details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[77]

153. Despite knowing that the Meta Pixel code embedded in its websites was sending patients' Personal Health Information to Facebook, Defendant did nothing to protect patients and users from egregious intrusions into patient privacy, choosing instead to benefit at those patients' and users' expense.

154. Despite knowing that the Meta Pixel code embedded in its websites was sending patients' Personal Health Information to Facebook, Defendants did nothing to protect patients and users from egregious intrusions into patient privacy, choosing instead to benefit at those patients' and users' expense.

L. Defendant's failure to inform its patients and prospective patients that their Personal Health Information has been disclosed to Facebook or to take any steps to halt the continued disclosure of patients' Personal Health Information is malicious, oppressive, and in reckless disregard of Plaintiffs' and Class Members' rights.

155. Hospital systems, like other businesses, have a legal obligation to disclose data breaches to their customers. *See e.g.*, CAL. CIV. CODE § 1798.82.

156. After publication of the Markup's investigative article in June 2022, hospital systems around the United States began self-reporting data breaches arising from their installation of pixel technology on their websites.[78]

157. For example, in August 2022, Novant Health informed approximately 1.3 million patients that their medical data was disclosed to Facebook due to the installation of the Facebook Meta Pixel on the hospital system's websites.[79] Novant Health's data breach announcement conceded that the Meta Pixel tool installed on its websites "allowed certain private information to

[77] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

[78] https://www.scmagazine.com/analysis/breach/pixel-fallout-expands-community-health-informs-1-5m-of-unauthorized-disclosure

[79] https://www.scmagazine.com/analysis/breach/1-3m-novant-health-patients-notified-of-unintended-disclosure-via-facebook-pixel

be transmitted to Meta from the Novant Health website."[80] Novant Health further admitted that the information about its patients that was disclosed to Facebook included "an impacted patient's: demographic information such as email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes."[81]

158. Likewise, in October 2022, Advocate Aurora Health informed approximately 3 million patients that their Personal Health Information had been disclosed to Facebook via the Meta Pixel installed on Advocate Aurora Health's website.[82] Advocate Aurora Health's data breach notification conceded that patient information had been transmitted to third parties including Facebook and Google when patients used the hospital system's website.[83]

159. Advocate Aurora Health further admitted that a substantial amount of its patients' Personal Health Information has been shared with Facebook and Google including patients' "IP address; dates, times, and/or locations of scheduled appointments; your proximity to an Advocate Aurora Health location; information about your provider; [and] type of appointment or procedure."[84] Even more troubling, Advocate Aurora Health admitted that "[w]e cannot confirm how vendors used the data they collected."[85]

160. In conjunction with its data breach notice, Advocate Aurora Health claimed that the hospital system had "disabled and/or removed the pixels from our platforms and launched an internal investigation to better understand what patient information was transmitted to our

[80] https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx

[81] https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx

[82] https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3

[83] https://www.advocateaurorahealth.org/

[84] https://www.advocateaurorahealth.org/pixel-notification/faq

[85] https://www.advocateaurorahealth.org/pixel-notification/faq

vendors."[86] Advocate Aurora Health also promised its 3 million patients that the company had instituted an "enhanced, robust technology vetting process" to prevent such disclosures of patients' Personal Health Information in the future.[87]

161. Similarly, in October 2022, WakeMed notified more than 495,000 patients that their Personal Health Information had been transmitted to Facebook through the use of tracking pixels installed on its website.[88] In announcing this data breach, WakeMed admitted that the Facebook Meta Pixel tool had been installed on both of its websites resulting in the transmission of patient information.[89] WakeMed further admitted that "[d]epending on the user's activity, the data that may have been transmitted to Facebook could have included information such as: email address, phone number, and other contact information; computer IP address; emergency contact information; information provided during online check-in, such as allergy or medication information; COVID vaccine status; and information about an upcoming appointment, such as appointment type and date, physician selected, and button/menu selections."[90] WakeMed also conceded that it had no idea what Facebook had done with the Personal Health Information that WakeMed had disclosed about its patients.[91] Like the other hospital systems who have come clean about their use of the Meta Pixel tool, WakeMed promised its patients that it had "proactively disabled Facebook's pixel" and had "no plans to use it in the future without confirmation that the pixel no longer has the capacity to transmit potentially sensitive or identifiable information."[92]

[86] https://www.advocateaurorahealth.org/pixel-notification/faq

[87] https://www.advocateaurorahealth.org/pixel-notification/faq

[88] https://healthitsecurity.com/news/wakemed-faces-data-breach-lawsuit-over-meta-pixel-use

[89] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident

[90] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident

[91] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident

[92] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident

162. In November 2022, the fallout from hospital systems' use of the Meta Pixel tool expanded when Community Health Network informed 1.5 million of its patients that their personal health information had been routinely transmitted and disclosed to Facebook since at least April 2017.[93]

163. In its data breach notice, Community Health informed patients that "third-party tracking technologies were installed on Community's website."[94] Community Health further admitted that it had "discovered through our investigation that the configuration of certain technologies allowed for a broader scope of information to be collected and transmitted to each corresponding third-party tracking technology vendor (e.g., Facebook and Google) than Community had ever intended." Community Health also conceded that its use of the Meta Pixel and related third-party tracking technologies had resulted in surreptitiously recording and transmitting a wide range of patient engagements with its websites, including "seeking treatment at a Community or affiliated provider location."[95]

164. Community Health—like WakeMed, Novant, and Advocate Aurora Health—also promised its patients that it had disabled or removed the third-party tracking technologies that it had installed on its website and had instituted new "evaluation and management processes for all website technologies moving forward."[96] Community Health, however, also conceded that it had no idea how Facebook or other third parties had exploited the patient Personal Health Information that had been disclosed to them via the pixel technology.

165. Unlike Community Health, WakeMed, Novant, Advocate Aurora Health, and other responsible hospital systems who have informed their patients of the serious privacy violations resulting from the installation of Facebook's Meta Pixel tool on their websites,

[93] https://healthitsecurity.com/news/community-health-network-notifies-1.5m-of-data-breach-stemming-from-tracking-tech; *see also* https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach

[94] https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach

[95] https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach

[96] https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach

Defendant has done nothing. Indeed, not only has Defendant hidden these privacy violations from its patients, but Defendant continues to collect, transmit, and disclose its patients' Personal Health Information to Facebook despite widespread knowledge in the health care community that such collection and disclosure of patient Personal Health Information is patently illegal and in violation of patients' fundamental privacy rights.

166. As these data breach announcements demonstrate, there is widespread knowledge within the health care community that installation of the Meta Pixel tool on hospital websites results in the disclosure of patients' Personal Health Information to Facebook. There is also widespread recognition that such disclosures are not only illegal but fundamentally unethical, given the privacy rights involved.

167. Defendant's decision to hide its use of the Meta Pixel tool from its own patients and its refusal to remove such technologies from its websites even after learning that its patients' Personal Health Information was being routinely collected, transmitted, and exploited by Facebook is malicious, oppressive, and in reckless disregard of Plaintiff's and Class Members' rights.

M. Tolling, Concealment, and Estoppel

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

169. Defendant seamlessly and secretively incorporated Meta Pixel and other trackers into its websites, providing no indication to users that they were interacting with a website enabled by Meta Pixel. Defendant had knowledge that its websites incorporated Meta Pixel and other trackers yet failed to disclose that by interacting with Meta-Pixel enabled websites, Plaintiff and Class Members' sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook.

170. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendant's conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel.

171. The earliest that Plaintiff and Class Members, acting with due diligence, could have reasonably discovered this conduct would have been on June 15, 2022, following the release of the Markup's investigation.

172. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Defendant's illegal interception and disclosure of patients' and users' Personal Health Information has continued unabated through the date of the filing of Plaintiff's Original Complaint. What's more, Defendant was under a duty to disclose the nature and significance of its data collection practices but did not do so. Defendant is therefore estopped from relying on any statute of limitations defenses.

VI. CLASS DEFINITION

173. Defendant's conduct violates the law and breaches express and implied privacy promises.

174. Defendant's unlawful conduct has injured Plaintiff and Class Members.

175. Defendant's conduct is ongoing.

176. Plaintiff brings this action individually and as a class action against Defendant.

177. Plaintiff brings this action in accordance with the Code of Civil Procedure Rule 382 individually and on behalf of the following proposed Class and subclass:

> **The Torrance Memorial Class:** For the period January 9, 2018, to the present, all California citizens who are, or were, patients or prospective patients of Torrance Memorial or any of its affiliates and who exchanged communications at Defendant's websites, including https://www.torrancememorial.org and any other Torrance Memorial affiliated website.
>
> **The Patient Subclass:** For the period January 9, 2018, to the present, all California citizens who are, or were, patients of Torrance Memorial or any of its affiliates and who exchanged communications at Defendant's websites, including https://www.torrencememorial.org/ and any other Torrance Memorial affiliated website.

178. Excluded from the Class and Subclass are: (1) any Judge or Magistrate presiding over this action and any members of their immediate families or staff; (2) any jurors assigned to hear this case and any members of their immediate families; (3) the Defendant, Defendant's subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendant or their parents have a controlling interest and their current or former employees, officers, and directors; and (4) Plaintiff's counsel and Defendant's counsel.

179. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, adequacy, and predominance requirements for suing as representative parties.

180. **Numerosity:** The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of thousands of individuals throughout California. The exact number of Class Members can be determined by review of information maintained by Defendant. The proposed class is defined objectively in terms of ascertainable criteria, such that the Court may determine the constituency of the class for the purposes of the conclusiveness of any judgment that may be rendered.

181. **Predominant Common Questions:** The Class's claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

(a) Whether Defendant violated Plaintiff's and Class Members' privacy rights;

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

(c) Whether Defendant's acts and practices violated California's Confidentiality of Medical Information Act, CIVIL CODE §§ 56, *et seq.*;

(d) Whether Defendant's acts and practices violated the California Invasion of Privacy Act, CAL. PENAL CODE §§ 630, *et seq.*;

(e) Whether Defendant's acts and practices violated the California Comprehensive Computer Data Access and Fraud Act, CAL. PENAL CODE § 502;

(f) Whether Defendant's acts and practices violated California's Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575, *et seq*;

(g) Whether Defendant's acts and practices violated California's Unfair Competition Law, CAL. BUS. & PROF. CODE §§ 17200, *et seq*;

(h) Whether Defendant's acts and practices violated CAL. CIVIL CODE §§ 1798.81.5, § 1798.81.5;

(i) Whether Defendant's acts and practices violated CAL. CIVIL CODE § 1798.83;

(j) Whether Defendant was unjustly enriched;

(k) Whether Plaintiff and the Class Members are entitled to equitable relief, including but not limited to injunctive relief, restitution, and disgorgement; and,

(l) Whether Plaintiff and the Class Members are entitled to actual, statutory, punitive or other forms of damages and other monetary relief.

182. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Class. The claims of Plaintiff and the members of the Class arise from the same conduct by Defendant and are based on the same legal theories.

183. **Adequate Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigation to remedy privacy violations. Plaintiff has no interest that is in conflict with the interests of the Class, and Defendant has no defenses unique to any Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do

so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Class.

184. **Substantial Benefits:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy, and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

185. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned, and legal developments following, additional investigation, discovery, or otherwise.

VII. CLAIMS FOR RELIEF

COUNT I—VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA") CAL. PENAL CODE §§ 630, *ET SEQ.*

186. Plaintiff re-alleges and incorporates all preceding paragraphs.

187. Plaintiff brings this claim on behalf of herself and all members of the Torrance Memorial Class.

188. The California Legislature enacted the California Invasion of Privacy Act, CAL. PENAL CODE §§ 630, *et seq*. ("CIPA") finding that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.* § 630. Thus, the intent behind CIPA is "to protect the right of privacy of the people of this state." *Id.*

189. CAL. PENAL CODE § 631(a) generally prohibits individuals, businesses, and other legal entities from "aid[ing], agree[ing] with, employ[ing], or conspir[ing] with" a third party to read, attempt 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 to use, or attempt to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained.

190. CAL. PENAL CODE § 632(a) generally prohibits individuals, businesses, and other legal entities from recording confidential communications without consent of all parties to the communication.

191. All alleged communications between Plaintiff or Class Members and Defendant qualify as protected communications under CIPA because each communication is made using personal computing devices (e.g., computers, smartphones, tablets) that send and receive communications in whole or in part through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

192. Defendant used a recording device to record the confidential communications without the consent of Plaintiff or Class members and then transmitted such information to others, such as Facebook.

193. At all relevant times, Defendant's aiding Facebook to learn the contents of communications and Defendant's recording of confidential communications was without authorization and consent.

194. The Plaintiff and Class Members had a reasonable expectation of privacy regarding the confidentiality of their communications with Defendant. Defendant told them they would not sell, rent, license, or trade their personally identifiable information to third parties without express consent. Defendant never received that express consent. Nor could Defendant have received consent from Plaintiff and Class Members because Defendant never sought to, nor

did, obtain Plaintiff's and Class Members' consent to transmit their Personal Health Information to Facebook.

195. Defendant engaged in and continues to engage in interception by aiding others (including Facebook) to secretly record the contents of Plaintiff's and Class Members' wire communications.

196. The intercepting devices used in this case include, but are not limited to:

(a) Plaintiff and Class Members' personal computing devices;

(b) Plaintiff and Class Members' web browsers;

(c) Plaintiff and Class Members' browser-managed files;

(d) Facebook's Meta Pixel;

(e) Internet cookies;

(f) Defendant's computer servers;

(g) Third-party source code utilized by Defendant; and

(h) Computer servers of third parties (including Facebook) to which Plaintiff and Class Members' communications were disclosed.

197. Defendant aided in, and continues to aid in, the interception of contents in that the data from the communications between Plaintiff and/or Class Members and Defendant that were redirected to and recorded by the third parties include information which identifies the parties to each communication, their existence, and their contents.

198. Defendant aided in the interception of "contents" in at least the following forms:

(a) The parties to the communications;

(b) The precise text of patient search queries;

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

(d) The precise text of patient communications about specific doctors;

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

(f) The precise text of patient communications about specific treatments;

(g) The precise text of patient communications about scheduling appointments with medical providers;

(h) The precise text of patient communications about billing and payment;

(i) The precise text of specific buttons on Defendant's website(s) that patients click to exchange communications, including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;

(j) The precise dates and times when patients click to Log-In on Defendant's website(s);

(k) The precise dates and times when patients visit Defendant's websites;

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

(m) Any other content that Defendant has aided third parties in scraping from webpages or communication forms at web properties.

199. Plaintiff and Class Members reasonably expected that their Personal Health Information was not being intercepted, recorded, and disclosed to Facebook.

200. No legitimate purpose was served by Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Personal Health Information to Facebook. Neither Plaintiff nor Class Members consented to the disclosure of their Personal Health Information by Defendant to Facebook. Nor could they have consented, given that Defendant never sought

Plaintiff's or Class Members' consent, or even told visitors to their websites that their every interaction was being recorded and transmitted to Facebook via the Meta Pixel tool.

201. Plaintiff's and Class Members' electronic communications were intercepted during transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their Personal Health Information, including using their sensitive medical information to develop marketing and advertising strategies.

202. Plaintiff and the Class Members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

203. In addition to statutory damages, Defendant's breach caused Plaintiff and Class Members, at minimum, the following damages:

(a) Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

(b) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(c) Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(e) Defendant's actions diminished the value of Plaintiff and Class Members' personal information.

204. Plaintiff and Class Members have also suffered irreparable injury from Defendant's unauthorized acts of disclosure. Their personal, private, and sensitive data has been collected, viewed, accessed, stored, and used by Defendant and Facebook without their consent and has not been destroyed. Plaintiff and Class Members have suffered harm and injury, including but not limited to the invasion of their privacy rights. Plaintiff continues to desire to search for health information on Torrance Memorial's website. Plaintiff will continue to suffer harm if the website is not redesigned. If the website were redesigned to comply with applicable laws, Plaintiff would use the Torrance Memorial website to search for health information in the future. Due to the continuing threat of injury, Plaintiff and Class Members have no adequate remedy at law, and Plaintiff and Class Members are therefore entitled to injunctive relief.

205. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT II—VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA") CIVIL CODE § 56.06

206. Plaintiff re-alleges and incorporates all preceding paragraphs.

207. Plaintiff brings this claim on behalf of herself and all members of the Torrance Memorial Class.

208. Defendant is a provider of health care under CAL. CIV. CODE. § 56.06, subdivision (a) and (b), because it maintains medical information and offers software to consumers that is designed to maintain medical information for the purposes of allowing their users to manage their information or for the diagnosis, treatment, or management of a medical condition.

209. Defendant is therefore subject to the requirements of the CMIA and obligated under subdivision (d) to maintain the same standards of confidentiality required of a provider of health care with respect to medical information disclosed to it.

210. Defendant violated Civil Code section 56.06 because it did not maintain the confidentiality of users' medical information. Instead, Defendant disclosed Plaintiff's and Class

members' medical information to Facebook without consent. This information was intentionally shared with Facebook, whose business is to sell advertisements based on the data that it collects about individuals, including the data Plaintiff and the Class Members shared with Defendant.

211. Defendant knowingly and willfully, or negligently, disclosed medical information without consent to Facebook for financial gain. Defendant's conduct was knowing and willful as it was aware that Facebook would collect all data inputted while using their website, yet intentionally embedded Meta Pixel anyway.

212. Accordingly, Plaintiff and Class members are entitled to: (1) nominal damages of $1,000; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to 56.36(c); and (4) reasonable attorney's fees and other litigation costs reasonably incurred.

213. In addition to statutory damages, Defendant's breach caused Plaintiff and Class Members, at minimum, the following damages:

(a) Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

(b) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(c) Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(e) Defendant's actions diminished the value of Plaintiff and Class Members' personal information.

214. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT III—VIOLATION OF CMIA CIVIL CODE § 56.101

215. Plaintiff re-alleges and incorporates all preceding paragraphs.

216. Plaintiff brings this claim on behalf of herself and all members of the Torrance Memorial Class.

217. CIVIL CODE § 56.101, subdivision (a) requires that every provider of health care "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein."

218. Any health care provider who "negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36."

219. Defendant failed to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information contained therein because it disclosed to Facebook Plaintiff's and Class Members' sensitive medical information without consent, including information concerning their health status, medical diagnoses, treatment, and appointment information, as well as personally identifiable information.

220. Defendant's failure to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information was, at the least, negligent and violates CIVIL CODE § 56.36 subdivisions (b) and (c).

221. Accordingly, Plaintiff and Class Members may recover: (1) nominal damages of $1,000; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to 56.36(c); and (4) reasonable attorney's fees and other litigation costs reasonably incurred.

222. In addition to statutory damages, Defendant's breach caused Plaintiff and Class Members, at minimum, the following damages:

(a) Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

(b) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(c) Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(e) Defendant's actions diminished the value of Plaintiff and Class Members' personal information.

223. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT IV—VIOLATION OF CMIA CIVIL CODE § 56.10

224. Plaintiff re-alleges and incorporates all preceding paragraphs.

225. Plaintiff brings this claim on behalf of herself and all members of the Torrance Memorial Class.

226. CIVIL CODE § 56.10, subdivision (a), prohibits a health care provider from disclosing medical information without first obtaining an authorization, unless a statutory exception applies.

227. Defendant disclosed medical information without first obtaining authorization when it disclosed Plaintiff's and Class Members' sensitive medical information to Facebook without consent, including information concerning their health status, medical diagnoses,

treatment, and appointment information, as well as personally identifiable information. No statutory exception applies. As a result, Defendant violated CIVIL CODE § 56.10, subdivision (a).

228. Defendant knowingly and willfully, or negligently, disclosed medical information without consent to Facebook for financial gain.

229. Accordingly, Plaintiff and Class Members may recover: (1) nominal damages of $1,000; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to 56.36(c); (4) punitive damages pursuant to 56.35; and (5) reasonable attorney's fees and other litigation costs reasonably incurred.

230. In addition to statutory damages, Defendant's breach caused Plaintiff and Class Members, at minimum, the following damages:

(a) Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

(b) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(c) Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(e) Defendant's actions diminished the value of Plaintiff and Class Members' personal information.

231. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT V—INVASION OF PRIVACY AND VIOLATION OF THE CALIFORNIA CONSTITUTION, ART. 1, § 1

232. Plaintiff re-alleges and incorporates all preceding paragraphs.

233. Plaintiff brings this claim on behalf of herself and all members of the Torrance Memorial Class.

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

235. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of social norms.

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

237. Plaintiff and Class Members had and continue to have a reasonable expectation of privacy in their personal information, identities, and user data pursuant to Article I, Section I of the California Constitution.

238. Plaintiff and Class Members had a reasonable expectation of privacy under the circumstances, including that: (i) the data collected, used, and disclosed by Defendant included personal, sensitive medical information, decisions, and medical diagnoses; and (ii) Plaintiff and Class Members did not consent or otherwise authorize Defendant to disclose this information to others or to collect and use this private information for their own monetary gain.

239. Given the nature of the Personal Health Information that Defendant disclosed to Facebook, such as patients' names, email addresses, phone numbers, information entered into forms, doctor's names, potential doctor's names, the search terms used to locate doctors (i.e., "Weight loss"), medications, and details about upcoming doctor's appointments, this kind of intrusion would be (and in fact is) highly offensive to a reasonable person.

240. The disclosure of personally identifiable medical information constitutes an unreasonable, substantial, and serious interference with Plaintiff's and Class Members' rights to privacy.

241. Plaintiff and Class Members did not consent to, authorize, or know about Defendant's disclosure of their Personal Health Information to Facebook at the time it occurred. Plaintiff and Class Members never agreed that their sensitive medical information could be collected, used, and monetized by Facebook.

242. Plaintiff and Class Members have suffered harm and injury, including but not limited to the invasion of their privacy rights. Plaintiff continues to desire to search for health information on Torrance Memorial's website. They will continue to suffer harm if the website is not redesigned. If the website were redesigned to comply with applicable laws, Plaintiff would use the Torrance Memorial website to search for health information in the future.

243. Plaintiff and Class Members therefore seek injunctive relief to prevent Defendant from continuing to collect, use, and sell Personal Health Information without consent.

244. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to seek just compensation, including monetary damages.

245. Plaintiff and Class Members seek appropriate relief for their injuries, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as well as a disgorgement of profits made by Defendant as a result of their intrusions on Plaintiff and Class Members' privacy.

246. Defendant's breach caused Plaintiff and Class Members, at minimum, the following damages:

(a) Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

(b) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(c) Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(e) Defendant's actions diminished the value of Plaintiff and Class Members' personal information.

247. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, which caused injury to Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

248. Plaintiff and Class Members seek attorney's fees in accordance with CAL. CODE CIV. PROCEDURE § 1021.5.

249. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT VI—VIOLATION OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA") CAL. PENAL CODE § 502

250. Plaintiff re-alleges and incorporates all preceding paragraphs.

251. Plaintiff brings this claim on behalf of herself and all members of the Torrance Memorial Class.

252. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act, CAL. PENAL CODE § 502 ("CDAFA") to "expand the degree of protection . . . from

tampering, interference, damage, and unauthorized access to [including the extraction of data from] lawfully created computer data and computer systems," finding and declaring that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and computer data," and that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals . . ." CAL. PENAL CODE § 502(a).

253. Plaintiff's and the Class Members' devices on which they accessed the hospital website, including their computers, smart phones, and tablets, constitute computers or "computer systems" within the meaning of CDAFA. *Id.* § 502(b)(5).

254. Defendant violated § 502(c)(1)(B) of CDAFA by knowingly accessing without permission Plaintiff's and Class Members' devices in order to wrongfully obtain and use their personal data, including their sensitive medical information, in violation of Plaintiff and Class Members' reasonable expectations of privacy in their devices and data.

255. Defendant violated CAL. PENAL CODE § 502(c)(2) by knowingly and without permission accessing, taking, copying, and using Plaintiff's and the Class Members' personally identifiable information, including their sensitive medical information.

256. The computers and mobile devices that Plaintiff and Class Members used when accessing the hospital website all have and operate "computer services" within the meaning of CDAFA. Defendant violated §§ 502(c)(3) and (7) of CDAFA by knowingly and without permission accessing and using those devices and computer services, and/or causing them to be accessed and used, *inter alia*, in connection with Facebook's wrongful collection of such data.

257. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any set of computer instructions that are designed to . . . record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information." Defendant violated § 502(c)(8) by knowingly and without permission

introducing a computer contaminant via Meta Pixel embedded into the hospital website, which intercepted Plaintiff's and the Class Members' private and sensitive medical information.

258. Defendant's breach caused Plaintiff and Class Members, at minimum, the following damages:

(a) Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

(b) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(c) Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(e) Defendant's actions diminished the value of Plaintiff and Class Members' personal information.

259. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

260. Plaintiff and the Class Members seek compensatory damages in accordance with CAL. PENAL CODE § 502(e)(1), in an amount to be proved at trial, and injunctive or other equitable relief. Plaintiff continues to desire to search for health information on Torrance Memorial's website. They will continue to suffer harm if the website is not redesigned. If the website were redesigned to comply with applicable laws, Plaintiff would use the Torrance Memorial website to search for health information in the future.

261. Plaintiff and Class members are entitled to punitive or exemplary damages pursuant to CAL. PENAL CODE § 502(e)(4) because Defendant's violations were willful and, upon information and belief, Defendant is guilty of oppression, fraud, or malice as defined in CAL. CIVIL CODE § 3294.

262. Plaintiff and the Class members are also entitled to recover their reasonable attorney's fees under § 502(e)(2).

COUNT VII—BREACH OF IMPLIED-IN-FACT CONTRACT

263. Plaintiff re-alleges and incorporates all preceding paragraphs.

264. Plaintiff Jane Doe brings this claim on behalf of herself and all members of the Patient Subclass.

265. Defendant promised in its "Website Privacy Notice" that it would "follow generally accepted industry standards to protect the information submitted to us, both during transmission and once we receive it."[97] Defendant also promised that "[o]nly employees who need the information to perform a specific job … are granted access to personally identifiable information."[98] Defendant further promised that "We will not sell or otherwise provide the information we collect to outside third parties."[99]

266. Defendant solicited and invited Plaintiff and Patient Subclass Members to provide their Private Health Information on its website as part of Defendant's regular business practices. Plaintiff and Patient Subclass Members accepted Defendant's offers and provided their Private Health Information to Defendant as part of acquiring Defendant's medical services. Per its contractual, legal, ethical, and fiduciary duties, Defendant was obligated to take adequate measures to protect Plaintiff's and Patient Subclass Members' Personal Health Information from unauthorized disclosure to third parties such as Facebook. These facts give rise to the inference

[97] https://www.torrancememorial.org/website-privacy-notice/

[98] https://www.torrancememorial.org/website-privacy-notice/

[99] https://www.torrancememorial.org/website-privacy-notice/

that Defendant took on obligations outside the plain terms of any express contracts that it may have had with Plaintiff and Patient Subclass Members.

267. Plaintiff and the Patient Subclass Members entered into valid and enforceable implied contracts with Defendant when they sought medical treatment from Defendant. Specifically, through their course of conduct, Defendant, Plaintiff and Patient Subclass Members entered into implied contracts for the provision of medical care and treatment, which included an implied agreement for Defendant to retain and protect the privacy of Plaintiff's and Patient Subclass Members' Personal Health Information.

268. Defendant required and obtained Plaintiff's and Patient Subclass Members' Personal Health Information as part of the physician-patient relationship, evincing an implicit promise by Defendant to act reasonably to protect the confidentiality of Plaintiff's and Patient Subclass Members' Personal Health Information. Defendant, through its privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised that it would safeguard Plaintiff's and Patient Subclass Members' Personal Health Information in exchange for access to that information and the opportunity to treat Plaintiff and Patient Subclass Members.

269. Implied in the exchange was a promise by Defendant to ensure that the Personal Health Information of Plaintiff and Patient Subclass Members in its possession would only be used for medical treatment purposes and would not be shared with third parties such as Facebook without the knowledge or consent of Plaintiff and Patient Subclass Members. By asking for and obtaining Plaintiff's and Patient Subclass Members' Personal Health Information, Defendant assented to protecting the confidentiality of that information. Defendant's implicit agreement to safeguard the confidentiality of Plaintiff's and Patient Subclass Members' Personal Health Information was necessary to effectuate the contract between the parties.

270. Plaintiff and Patient Subclass Members provided their Personal Health Information in reliance on Defendant's implied promise that this information would not be shared with third parties without their consent.

271. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Patient Subclass Members would provide their Personal Health Information in exchange for the medical treatment and other benefits provided by Defendant (including the protection of their confidential personal and medical information). A portion of the price of each payment that Plaintiff and the Patient Subclass Members made to Defendant for medical services was intended to ensure the confidentiality of their Personal Health Information.

272. In entering into such implied contracts, Plaintiff and Patient Subclass Members reasonably believed and expected that Defendant would comply with its promises to protect the confidentiality of their Personal Health Information as well as applicable laws and regulations governing the disclosure of such information and that Defendant would not allow third parties to collect or exploit their communications with Defendant without their consent.

273. It is clear by these exchanges that the parties intended to enter into an agreement and mutual assent occurred. Plaintiff and Patient Subclass Members would not have disclosed their Personal Health Information to Defendant but for the prospect of Defendant's promise of medical treatment and other benefits. Conversely, Defendant presumably would not have taken Plaintiff and Patient Subclass Members' Personal Health Information if they did not intend to provide them with medical treatment and other benefits.

274. Defendant was therefore required to reasonably safeguard and protect the Personal Health Information of Plaintiff and Patient Subclass Members from unauthorized disclosure and/or use by third parties.

275. Plaintiff and Patient Subclass Members accepted Defendant's medical services offer and fully performed their obligations under the implied contract with Defendant by providing their Personal Health Information to Defendant among other obligations. Plaintiff and Patient Subclass Members would not have provided and entrusted their Personal Health Information to Defendant in the absence of their implied contracts with Defendant and would

have instead retained the opportunity to control their Personal Health Information for uses other than the benefits offered by Defendant.

276. Plaintiff and Patient Subclass Members relied on Defendant's implied promises to safeguard their Personal Health Information to their detriment. Defendant breached the implied contracts with Plaintiff and Patient Subclass Members by failing to reasonably safeguard and protect Plaintiff's and Patient Subclass Members' Personal Health Information from disclosure to Facebook.

277. Defendant's failure to implement adequate measures to protect the Personal Health Information of Plaintiff and Patient Subclass Members and Defendant's intentional disclosure of the same to Facebook violated the purpose of the agreement between the parties: Plaintiff's and Patient Subclass Members' provision of money and Personal Health Information in exchange for medical services and other benefits.

278. Instead of safeguarding Plaintiff's and Patient Subclass Members' Personal Health Information, Defendant intentionally shared that information with Facebook, thereby breaching the implied contracts it had with Plaintiff and Patient Subclass Members.

279. Plaintiff and Patient Subclass Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to operate its website free of surreptitious collection and exploitation of communications between the parties. Defendant failed to do so. Plaintiff and Patient Subclass Members would not have sought medical services from Defendant if they had known that Defendant would share their Personal Health Information with Facebook without their knowledge or written consent.

280. Under the implied contracts, Defendant and/or its affiliated healthcare providers promised and were obligated to: (a) provide healthcare to Plaintiff and Patient Subclass Members; and (b) protect Plaintiff's and the Patient Subclass Members' Personal Health Information provided to obtain such healthcare. In exchange, Plaintiff and Patient Subclass Members agreed

to pay money for these services, and to turn over their Personal Health Information through the use of Defendant's websites.

281. Both the provision of medical services and the protection of Plaintiff and Patient Subclass Members' Private Health Information were material aspects of these implied contracts.

282. The implied contracts for the provision of medical services—contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Patient Subclass Members' Private Health Information unless they consented to third-party disclosures—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's published Notice of Privacy Practices.

283. Defendant's express representations, including, but not limited to, the express representations found in its Website Privacy Notice, memorialize and embody an implied contractual obligation requiring Defendant to refrain from aiding or allowing third parties to collect Plaintiff's and Patient Subclass Members' Private Health Information without consent. By soliciting and acquiring Plaintiff's and Patient Subclass Members' Personal Health Information, Defendant assumed an independent duty to handle Plaintiff's and Patient Subclass Members' Personal Health Information with due care and consistent with industry standards to prevent the foreseeable harm that arises from a breach of that duty.

284. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Health Information associated with obtaining healthcare private. To customers such as Plaintiff and the Patient Subclass Members, healthcare that allows third parties to secretly collect their Private Health Information without consent is fundamentally less useful and less valuable than healthcare that refrains from such practices. Plaintiff and Patient Subclass Members would not have entrusted their Private Health Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Health Information would be safeguarded and protected or entrusted their Private Health Information to Defendant in the absence of its implied promise to do so.

285. A meeting of the minds occurred when Plaintiff and the Patient Subclass Members agreed to, and did, provide their Private Health Information to Defendant and/or its affiliated healthcare providers and paid for the provided healthcare in exchange for, amongst other things, (a) the provision of healthcare and medical services and (b) the protection of their Private Health Information.

286. Plaintiff and the Patient Subclass Members performed their obligations under the contract when they paid for their healthcare services and provided their Private Health Information.

287. Defendant materially breached its contractual obligation to protect the nonpublic Private Health Information Defendant gathered when it allowed Facebook to collect and exploit that information without Plaintiff's and Patient Subclass Members' consent.

288. Defendant also materially breached its contractual obligation to protect Plaintiff's and Patient Subclass Members' non-public Personal Health Information when it failed to implement adequate security measures and policies to protect the confidentiality of that information. For example, on information and belief, Defendant (1) failed to implement internal policies and procedures prohibiting the disclosure of patients' Personal Health Information without consent to third-party advertising companies like Facebook, (2) failed to implement adequate reviews of the software code and java script installed on its websites to ensure that patients' Personal Health Information was not being automatically routed without consent to third-party advertising companies like Facebook, (3) failed to provide adequate notice to the public that visitors to its websites risked having their Personal Health Information shared with third-party advertising companies like Facebook, (4) failed to take other industry-standard privacy protection measures such as providing a "cookie" acceptance button on its website homepages, (5) failed to implement internal policies and educational programs to ensure that Defendant's website managers and coders were familiar with the legal regulations governing the disclosure patient Personal Health Information to third parties, and (6) failed to install adequate firewalls or

take similar measures to prevent the automatic routing of patients' Personal Health Information to third-party advertising companies like Facebook.

289. As a result of Defendant's failure to fulfill the data-privacy protections promised in these contracts, Plaintiff and Patient Subclass Members did not receive the full benefit of their bargains, and instead received healthcare and other services that were of a diminished value compared to those described in the contracts. Plaintiff and Patient Subclass Members were therefore damaged in an amount at least equal to the difference between the value of the healthcare services with data privacy they paid for and the healthcare services they received.

290. As a result of Defendant's material breaches, Plaintiff and Patient Subclass Members were deprived of the benefit of their bargain with Defendant because they spent more on medical services with Defendant than they would have if they had known that Defendant was not providing the reasonable data security and confidentiality of patient communications that Defendant represented it was providing in its privacy policies. Defendant's failure to honor its promises that it would protect the confidentiality of patient communications thus resulted in Plaintiff and Patient Subclass Members overpaying Defendant for the services they received.

291. The services that Plaintiff and Patient Subclass Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide, which included Defendant's promise that any patient communications with Defendant would be treated as confidential and would never be disclosed to third parties for marketing purposes without the express consent of patients.

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

293. Defendant's conduct in sharing Plaintiff's and Patient Subclass Members' Personal Health Information with Facebook also diminished the sales value of that information. There is a robust market for the type of information that Plaintiff and Patient Subclass Members shared with Defendant (which Defendant then shared with Facebook). Indeed, Facebook itself has offered to pay the public to acquire similar information in the past so that Facebook could use such information for marketing purposes. Plaintiff and Patient Subclass Members were harmed both by the dissemination of their Personal Health Information and by losing the sales value of that information.

294. As a direct and proximate result of these failures, Plaintiff and the Patient Subclass Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including, without limitation, the release and disclosure of their Private Health Information, the loss of control of their Private Health Information, the diminution in value of their Personal Health Information, and the loss of the benefit of the bargain they had struck with Defendant.

295. Plaintiff and the Patient Subclass Members are entitled to compensatory and consequential damages suffered as a result.

296. Plaintiff and Patient Subclass Members also face a real and immediate threat of future injury to the confidentiality of their Personal Health information both because such information remains within Defendant's control and because anytime that Plaintiff and/or Patient Subclass Members interact with Defendant's websites to make appointments, search for information about their medical conditions, search for a doctor, or otherwise seek assistance with their medical conditions, they risk further disclosure of their Personal Health Information. Plaintiff and the Patient Subclass Members are therefore also entitled to injunctive relief requiring Defendant to cease all website operations that allow for the third-party capture of Private Health Information.

COUNT VIII—QUASI-CONTRACT/RESTITUTION/UNJUST ENRICHMENT

297. Plaintiff re-alleges and incorporates all preceding paragraphs.

298. Plaintiff Jane Doe brings this claim on behalf of herself and all members of the Patient Subclass.

299. Plaintiff Jane Doe pleads this cause of action in the alternative to Count VII.

300. "Common law principles of restitution require a party to return a benefit when the retention of such benefit would unjustly enrich the recipient; a typical cause of action involving such remedy is 'quasi-contract.'" *Munoz v. MacMillan* (2011) 195 Cal. App. 4th 648, 661,124 Cal. Rptr. 3d 664; *see also City of Oakland v. Oakland Raiders* (2022) 83 Cal. App. 5th 458, 299 Cal. Rptr. 3d 463, 478.

301. Plaintiff and Patient Subclass Members personally and directly conferred a benefit on Defendant by paying Defendant for health care services, which included Defendant's obligation to protect Plaintiff's and Class Members' Personal Health Information. Defendant was aware of receiving these payments from Plaintiff and Patient Subclass Members and demanded such payments as a condition of providing treatment.

302. Plaintiff and Patient Subclass Members also conferred a benefit on Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiff and Patient Subclass Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from Facebook and other third parties. Defendant had knowledge that Plaintiff and Patient Subclass Members had conferred this benefit on Defendant by interacting with their website, and Defendant intentionally installed the Meta Pixel tool on its website to capture and monetize this benefit conferred by Plaintiff and Patient Subclass Members.

303. Plaintiff and the Patient Subclass Members would not have used the Defendant's services, or would have paid less for those services, if they had known that Defendant would

collect, use, and disclose this information to Facebook. The services that Plaintiff and Patient Subclass Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide, which included Defendant's promise that any patient communications with Defendant would be treated as confidential and would never be disclosed to third parties for marketing purposes without the express consent of patients.

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

305. Defendant unjustly retained those benefits at the expense of Plaintiff and Patient Subclass Members because Defendant's conduct damaged Plaintiff and Patient Subclass Members, all without providing any commensurate compensation to Plaintiff and Patient Subclass Members.

306. The benefits that Defendant derived from Plaintiff and Patient Subclass Members rightly belong to Plaintiff and Patient Subclass Members. It would be inequitable under unjust enrichment principles for Defendant to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

307. Defendant should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT IX—VIOLATION OF CAL. BUS. & PROF. CODE §§ 17200 *ET. SEQ.*

308. Plaintiff re-alleges and incorporates all preceding paragraphs.

309. Plaintiff Jane Doe brings this claim on behalf of herself and all members of the Patient Subclass.

310. Defendant's business acts and practices are "unlawful" under the Unfair Competition LAW, CAL. BUS. & PROF. CODE §§ 17200 *et. seq.* (the "UCL") because, as alleged above, Defendant violated California common law, the California Constitution, and other statutes and causes of action alleged herein.

311. Defendant's business acts and practices are also "unfair" under the UCL. California has a strong public policy of protecting consumers' privacy interests, including consumers' and patients' personal data. Defendant violated this public policy by, among other things, surreptitiously collecting, disclosing and otherwise exploiting Plaintiff and Patient Subclass Members' Personal Health Information by sharing that information with Facebook without Plaintiff's and/or Patient Subclass Members' consent.

312. Defendant's business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to patients. The gravity of the harm of Defendant's secretly collecting, disclosing, and otherwise misusing Plaintiff's and Patient Subclass Members' Personal Health Information by bartering it to Facebook in return for access to the Meta Pixel tool is significant, and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiff and Patient Subclass Members were unaware of Defendant's conduct, they could not have avoided the harm.

313. Defendant's business acts and practices are also "fraudulent" within the meaning of the UCL. Defendant expressly promised Plaintiff and Patient Subclass Members that they were committed to protecting the confidentiality of their Personal Health Information. Defendant also promised that they would never "sell, rent, license, or trade" patients' personally identifying information "to third parties for their own direct marketing use unless we receive your express consent to do so." These promises were false. Defendant regularly shared Plaintiff and Patient Subclass Members' Personal Health Information with Facebook so that Facebook could target

Plaintiff and Patient Subclass Members with advertising benefiting Facebook and its business partners.

314. Defendant's business acts and practices were likely to, and did, deceive members of the public including Plaintiff and Patient Subclass Members into believing their Personal Health Information would be protected from disclosure to Facebook and other third parties.

315. Defendant's violations were and are willful, deceptive, unfair, and unconscionable.

316. Had Plaintiff and Patient Subclass Members known that their sensitive medical information would be intercepted, collected, and transmitted to Facebook by Defendant, they would not have used Defendant's services.

317. Plaintiff and Patient Subclass Members have a property interest in their Personal Health Information. By surreptitiously collecting and otherwise misusing Plaintiff's and Patient Subclass Members' Personal Health Information, Defendant has taken property from Plaintiff and Patient Subclass Members without providing just (or indeed *any*) compensation.

318. Plaintiff and Patient Subclass Members have lost money and property as a result of Defendant's conduct in violation of the UCL. Personal Health Information such as the Personal Health Information collected and transmitted to Facebook by Defendant has objective monetary value. Companies are willing to pay for Personal Health Information, like the information unlawfully collected and transmitted by Defendant to Facebook. For example, Pfizer annually pays approximately $12 million to purchase health data from various sources.[100]

319. Consumers also value their personal health data. According to the annual Financial Trust Index Survey conducted by the University of Chicago's Booth School of Business and Northwestern University's Kellogg School of Management, which interviewed more than 1,000 Americans, 93 percent would not share their health data with a digital platform for free. Half of the survey participants would only share their data for $100,000 or more, and 22 percent would only share their data if they received between $1,000 and $100,000.[101]

[100] https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/

[101] https://www.beckershospitalreview.com/healthcare-information-technology/how-much-should-health-data-cost-

320. By deceptively collecting, using, and sharing Plaintiff's and Patient Subclass Members Personal Health Information with Facebook, Defendant has taken money or property from Plaintiff and Patient Subclass Members. Accordingly, Plaintiff seeks restitution on behalf of herself and the Patient Subclass.

321. Plaintiff and Patient Subclass Members also face a real and immediate threat of future injury to the confidentiality of their Personal Health information both because such information remains within Defendant's control and because anytime that Plaintiff and/or Patient Subclass Members interact with Defendant's websites to make appointments, search for information about their medical conditions, search for a doctor, or otherwise seek assistance with their medical conditions, they risk further disclosure of their Personal Health Information. Plaintiff also continues to desire to search for health information on Torrance Memorial's website. They will continue to suffer harm if the website is not redesigned. If the website were redesigned to comply with applicable laws, Plaintiff would use the Torrance Memorial website to search for health information in the future. Plaintiff and the Patient Subclass Members are therefore also entitled to injunctive relief requiring Defendant to cease all website operations that allow for the third-party capture of Private Health Information.

COUNT IX—VIOLATION OF CAL. CIVIL CODE § 1798.83

322. Plaintiff re-alleges and incorporates all preceding paragraphs.

323. Plaintiff Jane Doe brings this claim on behalf of herself and all members of the Patient Subclass.

324. California CIVIL CODE § 1798.83 requires that "if a business has an established business relationship with a customer and has within the immediately preceding calendar year disclosed personal information" to a third party and "knows or reasonably should know that the third parties used the personal information for the third parties' direct marketing purposes, that business shall" provide in writing to its customers free of charge (1) a list of the categories of

100k-or-more-according-to-patients html

personal information provided to third parties and (2) the names and addresses of all third parties who received the customers' personal information during the preceding calendar year. The kinds of "personal information" that the statute expressly protects includes "medical information, "health insurance information," and any other kind of information that "identifies, relates to, describes, or is capable of being associated with … a particular individual." CAL. CIVIL CODE § 1798.80.

325. Any customer who is injured by a violation of the statute may institute a civil action to recover damages. CAL. CIVIL CODE § 1798.84(b). Additionally, "for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83." CAL. CIVIL CODE § 1798.84(c). Further, any business that violates, proposes to violate, or has violated this statute may be enjoined. CAL. CIVIL CODE § 1798.84(e).

326. Facebook is a third party engaged in direct marketing.

327. Defendant failed to disclose to Plaintiff and Patient Subclass Members that it was regularly collecting, transmitting, and sharing their Personal Health Information with Facebook so that Facebook could target them with advertising. Defendant willfully, intentionally, and/or recklessly failed to provide the information and disclosures required by CAL. CIVIL CODE § 1798.83 as part of a scheme to barter Plaintiff's and Patient Subclass Members' Personal Health Information to Facebook in return for access to the Meta Pixel tool.

328. Plaintiff and Patient Subclass Members conferred a benefit on Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiff and Patient Subclass Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from Facebook and other third parties. Defendant had knowledge that Plaintiff and Patient Subclass Members had conferred this benefit on Defendant by interacting

with their website, and Defendant intentionally installed the Meta Pixel tool on their website to capture and monetize this benefit conferred by Plaintiff and Patient Subclass Members.

329. Plaintiff and Patient Subclass Members also conferred a benefit on Defendant by paying Defendant for health care services, which included Defendant's obligation to protect Plaintiff's and Patient Subclass Members' Personal Health Information. Defendant was aware of receiving these payments from Plaintiff and Patient Subclass Members and demanded such payments as a condition of providing treatment.

330. Plaintiff and the Patient Subclass Members would not have used the Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to Facebook. The services that Plaintiff and Patient Subclass Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide, which included Defendant's promise that any patient communications with Defendant would be treated as confidential and would never be disclosed to third parties for marketing purposes without the express consent of patients.

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

332. Defendant unjustly retained those benefits at the expense of Plaintiff and Patient Subclass Members because Defendant's conduct damaged Plaintiff and Patient Subclass Members, all without providing any commensurate compensation to Plaintiff and Patient Subclass Members.

333. Plaintiff and Patient Subclass Members were damaged by Defendant's failure to inform them that their every communication and Personal Health Information was being shared with Facebook, resulting in, at minimum, the following damages:

(a) Sensitive and confidential information that Plaintiff and Patient Subclass Members intended to remain private is no longer private;

(b) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(c) Defendant took something of value from Plaintiff and Patient Subclass Members and derived benefit therefrom without Plaintiff's and Patient Subclass Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Patient Subclass Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(e) Defendant's actions diminished the value of Plaintiff and Patient Subclass Members' personal information.

334. Plaintiff also continues to desire to search for health information on Torrance Memorial's website. She will continue to suffer harm if Defendant does not make adequate disclosures regarding which third party marketing companies are receiving Plaintiff's and Patient Subclass Members' protected health information. Plaintiff and the Patient Subclass Members are therefore also entitled to injunctive relief requiring Defendant to comply with CAL. CIV. CODE § 1798.83.

VIII. DEMAND FOR JURY TRIAL

335. Plaintiff hereby demands a trial by jury on all issues so triable.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and the proposed Class respectfully requests that the Court enter an order:

A. Certifying the Classes and appointing Plaintiff as the Classes' representative;

B. Appointing the law firms of Caddell & Chapman, Ahmad, Zavitsanos, & Mensing P.C., and Turke & Strauss, LLP as Class Counsel;

C. Finding that Defendant's conduct was unlawful, as alleged herein;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper;

E. A declaration that Defendant is financially responsible for all Class notice and the administration of Class relief;

F. Awarding Plaintiff and the Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

Dated: January 9, 2023

Respectfully submitted,

By: */s/ Michael A. Caddell*

Michael A. Caddell (SBN 249469)
mac@caddellchapman.com
Cynthia B. Chapman (SBN 164471)
cbc@caddellchapman.com
Amy E. Tabor (SBN 297660)
aet@caddellchapman.com
CADDELL & CHAPMAN
P.O. Box 1311
MONTEREY CA 93942
Tel.: (713) 751-0400
Fax: (713) 751-0906

Foster C. Johnson (SBN 289055)
David Warden*
Joseph Amhad*
Nathan Campbell*
Ahmad, Zavitsanos, & Mensing, P.C.
1221 McKinney Street, Suite 3460
Houston TX 77010
Tel.: (713) 655-1101
fjohnson@azalaw.com
dwarden@azalaw.com
ahmad@azalaw.com
ncampbell@azalaw.com

Samuel J. Strauss*
Raina C. Borrelli*
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
Tel.: (608) 237-1775
Fax: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

* Motions for Admission to be filed

COUNSEL FOR PLAINTIFFS, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED

ClassAction.org
