

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

7 Foster C. Johnson
 fjohnson@azalaw.com (SBN 289055)
 8 David Warden (*pro hac vice forthcoming*)
 dwarden@azalaw.com
 9 Joseph Ahmad (*pro hac vice forthcoming*)
 jahmad@azalaw.com
 10 Nathan Campbell (*pro hac vice forthcoming*)
 ncampbell@azalaw.com
 11 AHMAD, ZAVITSANOS, & MENSING, P.C.
 12 1221 McKinney Street, Suite 3460
 Houston TX 77010
 13 Tel: (713) 655-1101
 Fax: (713) 655-0062

14 *Attorneys for Plaintiff*

15 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
 16 **COUNTY OF LOS ANGELES**

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

19 *Plaintiff,*

20 v.

21 TORRANCE MEMORIAL
 MEDICAL CENTER,

22 *Defendant.*

CASE No. 23STCV00395

**CLASS ACTION COMPLAINT
 AND DEMAND FOR JURY TRIAL**

23
 24
 25
 26
 27
 28 CASE No.

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

6 **I. SUMMARY OF ALLEGATIONS**

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

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

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

20 4. Defendant discloses this protected health information through the deployment of
21 various digital marketing and automatic rerouting tools embedded on its websites that
22 purposefully and intentionally redirect personal health information to Facebook, who exploits that
23 information for advertising purposes. Defendant’s use of these rerouting tools causes personally
24

25 _____
¹ <https://www.torrancememorial.org/website-privacy-notice/>

26 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>

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

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

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

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

19 II. PARTIES

20 A. Plaintiff

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

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

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

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

3 **B. Defendant**

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

6 **III. JURISDICTION AND VENUE**

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

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

16 **IV. FACTUAL BACKGROUND**

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

23 16. Unbeknownst to Plaintiff Jane Doe, Torrance Memorial had embedded computer
24 code on its website that took every search term she entered and every page of the site she visited
25 and sent that information directly to Facebook, the largest and most profitable social media
26

27 ³ <https://www.torrancememorial.org/>

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

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

19 V. CLASS ACTION ALLEGATIONS

20 A. Defendant routinely discloses the protected health information of patients and users of 21 its services to Facebook.

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

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

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

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

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

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

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

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

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

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

25 26. By design, third parties receive and record the exact contents of these
26 communications before the full response from Defendant has been rendered on the screen of the
27

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

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

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

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

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

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

25
26
27 ⁴ https://www.w3schools.com/tags/ref_httpmethods.asp

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

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

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

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

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

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

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

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

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

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

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

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

24
25
26
27 ⁵ <https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/>

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

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

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

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

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

22
23 ⁶ <https://www.blog.google/products/chrome/building-a-more-private-web/>

24 ⁷ <https://pixelprivacy.com/resources/browser-fingerprinting/>

25 ⁸ <https://www.blog.google/products/chrome/building-a-more-private-web/>

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

27 ¹⁰ <https://www.facebook.com/help/211813265517027>

28 ¹¹ <https://smallseotools.com/find-facebook-id/>

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

3 **D. Facebook’s Business Model: Exploiting User Data to Sell Advertising**

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

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

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

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

20
21 _____
22 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.>

23 ¹³ <https://transparency.fb.com/policies/community-standards/account-integrity-and-authentic-identity/>

24 ¹⁴ <http://www.facebook.com/help/406644739431633>

25 ¹⁵ <https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/>

26 ¹⁶ <https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/>

27 ¹⁷ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

28 ¹⁸ <https://www.facebook.com/business/ads/ad-targeting>

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

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

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

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

20 56. Ad Targeting has been extremely successful due to Facebook's ability to target
21 individuals at a granular level. For example, among many possible target audiences, "Facebook
22 offers advertisers 1.5 million people 'whose activity on Facebook suggests that they're more
23 likely to engage with/distribute liberal political content' and nearly seven million Facebook users
24 who 'prefer high-value goods in Mexico.'"²⁰ Aided by highly granular data used to target specific
25
26

27 ²⁰ <https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>

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

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

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

10 58. One of Facebook’s most powerful tools is called the “Meta Pixel.” Once a third-
11 party like Defendant installs the Meta Pixel on its website, by default it begins sending user
12 information to Facebook automatically.²¹

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

21 60. When someone visits a third-party website page that includes the Meta Pixel code,
22 the Meta Pixel code is able to replicate and send the user data to Facebook through a separate (but
23

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

25 ²² <https://developers.facebook.com/docs/meta-pixel/>

26 ²³ <https://www.facebook.com/business/goals/retargeting>

27 ²⁴ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

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

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

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

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

23
24 _____
25 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).

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

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

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

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

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

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

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

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

17 68. Once Meta Pixel is installed on a business's website, the Meta Pixel tracks users
18 as they navigate through the website and logs which pages are visited, which buttons are clicked,
19 the specific information entered in forms (including personal information), as well as "optional
20 values" set by the business website.³⁵ Meta Pixel tracks this data regardless of whether a user is
21
22

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

24 ³¹ <https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/>

25 ³² <https://www.oviond.com/understanding-the-facebook-pixel>

26 ³³ <https://developers.facebook.com/docs/meta-pixel/get-started>

27 ³⁴ <https://developers.facebook.com/docs/meta-pixel/get-started>

28 ³⁵ <https://developers.facebook.com/docs/meta-pixel/>

1 logged into Facebook.³⁶ It is unclear how Facebook exploits the data collected from nonusers, but
2 when asked by Congress about Facebook’s business practices, Mark Zuckerberg conceded that
3 company maintains “shadow profiles” on nonusers of Facebook.³⁷

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

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

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

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

21
22 _____
23 ³⁶ <https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients>

24 ³⁷ <https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/>

25 ³⁸ <https://developers.facebook.com/docs/meta-pixel/>

26 ³⁹ <https://developers.facebook.com/docs/meta-pixel/>

27 ⁴⁰ <https://developers.facebook.com/docs/meta-pixel/>

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

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

6 74. Alternatively, Facebook can link the data to a user’s Facebook account through the
7 “Facebook Cookie.”⁴² The Facebook Cookie is a workaround to recent cookie-blocking
8 applications used to prevent websites from tracking users.⁴³

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

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

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

23 _____
24 ⁴² <https://clearcode.cc/blog/facebook-first-party-cookie-adtech/>

25 ⁴³ <https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/>

26 ⁴⁴ <https://www.facebook.com/business/help/611774685654668?id=1205376682832142>

27 ⁴⁵ <https://www.facebook.com/business/help/611774685654668?id=1205376682832142>

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

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

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

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

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

20 81. Facebook also uses browser fingerprinting to uniquely identify individuals. Web
21 browsers have several attributes that vary between users, like the browser software system,
22 plugins that have been installed, fonts that are available on the system, the size of the screen, color
23 depth, and more. Together, these attributes create a fingerprint that is highly distinctive. The
24

25 _____
26 ⁴⁷ <https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbfd8a#:~:text=browser%20session%20ends,-,%E2%80%9Cdatr%E2%80%9D,security%20and%20site%20integrity%20features.>

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

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

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

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

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

22 84. Facebook provides websites using Meta Pixel with the data it captures in the "Meta
23 Pixel page" in Events Manager, as well as tools and analytics to reach these individuals through
24 future Facebook ads.⁵⁰ For example, websites can use this data to create "custom audiences" to
25

26 _____
⁴⁹ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

27 ⁵⁰ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

1 target the specific Facebook user, as well as other Facebook users who match “custom audience’s”
2 criteria.⁵¹ Businesses that use Meta Pixel can also search through Meta Pixel data to find specific
3 types of users to target, such as men over a certain age.

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

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

21 87. Defendant is among the hospital systems who have embedded Meta Pixel on their
22 websites. When a prospective or actual patient enters their personal information through
23 Defendant’s websites that incorporate Meta Pixel, such as to locate a doctor or make an
24 appointment, this information, including what the patient is being treated for, is immediately and
25

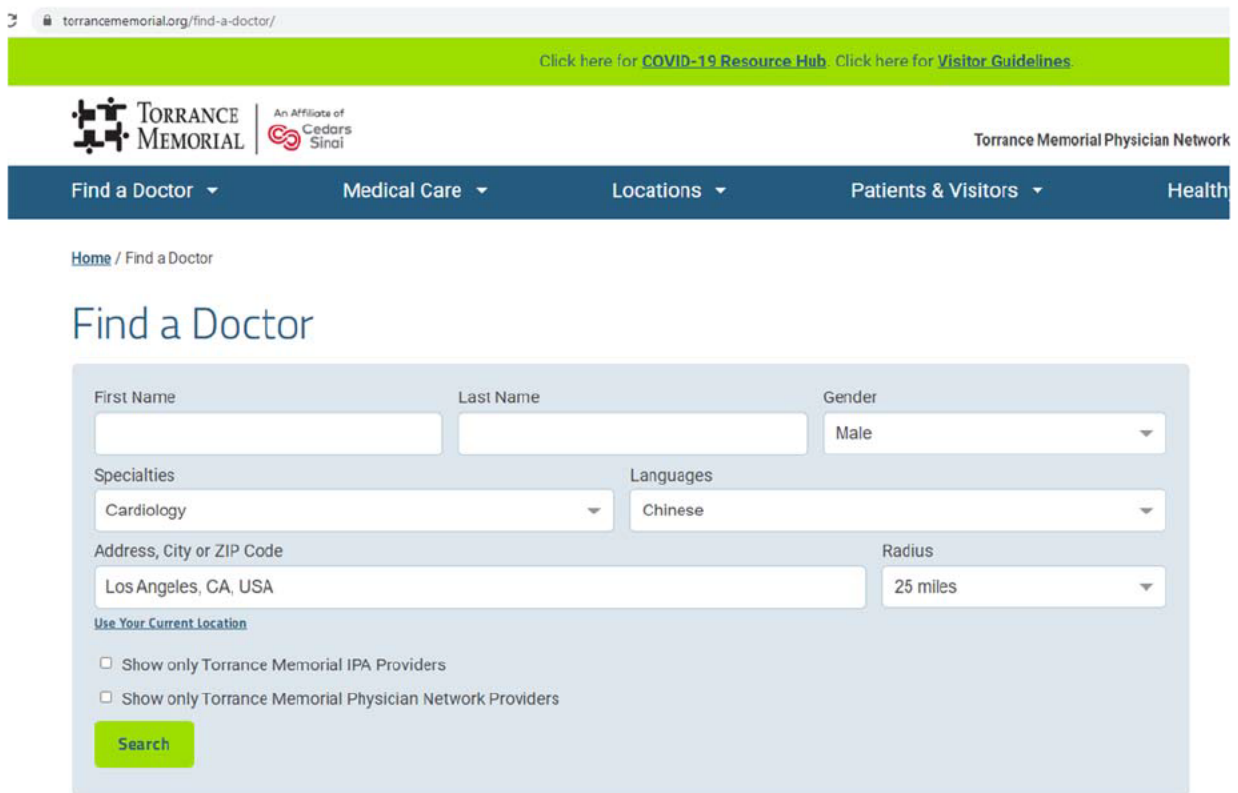
26 ⁵¹ <https://developers.facebook.com/docs/marketing-api/reference/custom-audience/>

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

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

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

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



25 90. When a patient clicks on the “search” button, Defendant’s website generates a list
 26 of providers that a patient can review and choose from:

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

The screenshot shows a web browser displaying the Torrance Memorial website. The URL is torrancememorial.org/find-a-doctor/imp/results/?termid=c707772-c8eb-e011-a855-000d3a619008&filterTermid=5a51402c-f967-ec11-a855-000d3a619008&sort=3. The page has a green header with links for COVID-19 Resource Hub and Visitor Guidelines. Below the header is a navigation bar with options: Find a Doctor, Medical Care, Locations, Patients & Visitors, and Healthy Living. The main content area is titled 'Results' and shows a search for doctors. It displays two results:

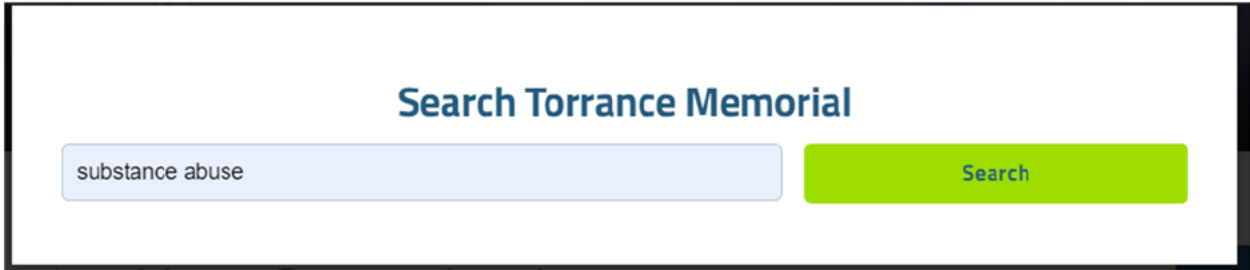
Doctor Name	Specialty	Location	Phone Number	Membership
William K. Aveill, MD	Cardiology, Interventional Cardiology	Torrance, CA	310-326-5142	Member of Torrance Memorial IPA
Salman Mohammed Azam, MD	Cardiology, Interventional Cardiology, Internal Medicine	Torrance, CA	310-257-0508	Member of Torrance Memorial IPA

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:

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



Related Pages

Found 34 pages matching the search term **substance abuse**.



[What Every Parent Needs to Know](#)

Substance use and abuse during adolescence can have permanent consequences.
2/27/2018



[Medication Assisted Treatment](#)

Medication assisted treatment (MAT) for substance use disorders at the Thelma McMillen Center for Alcohol and Drug Treatment.
2/27/2018



[Returning to School in 2021: A Parent's Survival Guide](#)

9/23/2021



[Mental Health Corner](#)

Our feelings and thoughts are connected. Our feelings are always correct and result from our thinking. Our thinking can be inaccurate, distorted or based on old information.
8/28/2022

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

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

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

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

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

25
26 ⁵³ [https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-
27 manipulation-experiment/373648/](https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/)

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

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

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

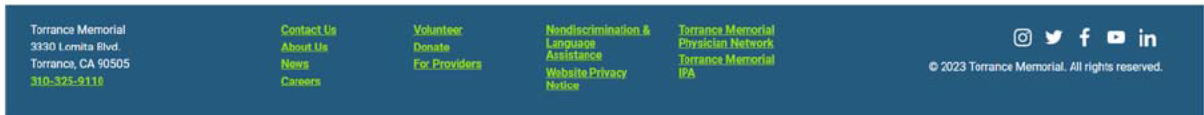
13 99. Plaintiff and Class Members had no idea when they interacted with Defendant’s
14 websites that their personal data, including sensitive medical data, was being collected and
15 simultaneously transmitted to Facebook. That is because, among other things, the Meta Pixel tool
16 is seamlessly and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

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

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

24 102. While Defendant purports to have a “Privacy Notice,” that Privacy Notice is
25 effectively hidden from patients, concealed at the bottom of Defendant’s homepage in type so
26 small as to be unreadable to many visitors⁵⁴:

27 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/>

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

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

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

21 108. Defendant’s promises are unsurprising. Defendant does not have a legal right to
22 share Plaintiff’s and Class Members’ Protected Health Information with Facebook, because this
23 information is protected from such disclosure by law. *See, e.g.*, CAL. CIV. CODE §§ 56 *et seq.*; 45
24 C.F.R. § 164.508. Defendant is not permitted to disclose patients’ Protected Health Information to
25

26
27 ⁵⁷ <https://www.torrancememorial.org/website-privacy-notice/>

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

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

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

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

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

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

25 113. There is no information anywhere on the websites operated by Defendant that
26 would alert patients that their most private information (such as their identifiers, their medical
27

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

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

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

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

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

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

25 118. Given the application of these laws to Defendant, coupled with Defendant's
26 express promises that they would protect the confidentiality of patients' Personal Health
27

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

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

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

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

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

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

24
25
26 ⁵⁸ <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/>

27 ⁵⁹ <https://www.wired.co.uk/article/apple-ios14-facebook>

1 *Provider Liability and Electronic Health Record Systems*, 24 BERKLEY TECH L.J. 1523, 1557
2 (2009).

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

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

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

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

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

25
26 _____
27 ⁶⁰ <https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/>

28 ⁶¹ <https://ig.ft.com/how-much-is-your-personal-data-worth/>

1 129. In 2015, *TechCrunch* reported that “to obtain a list containing the names of
2 individuals suffering from a particular disease,” a market participant would have to spend about
3 “\$0.30” per name.⁶² That same article noted that “Data has become a strategic asset that allows
4 companies to acquire or maintain a competitive edge” and that the value of a single user’s data
5 can vary from \$15 to more than \$40 per user.⁶³

6 130. In a 2021 Washington Post article, the legal scholar Dina Srinivasan said that
7 consumers “should think of Facebook’s cost as [their] data and scrutinize the power it has to set
8 its own price.”⁶⁴ This price is only increasing. According to Facebook’s own financial statements,
9 the value of the average American’s data in advertising sales rose from \$19 to \$164 per year
10 between 2013 and 2020.⁶⁵

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

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

21 _____
22 ⁶² <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>

23 ⁶³ <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>

24 ⁶⁴ <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/>

25 ⁶⁵ <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/>

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

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

⁶⁸ <https://www.cNBC.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html>

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

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

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

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

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

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

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

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

26 _____
27 ⁶⁹ <https://www.creditdonkey.com/best-apps-data-collection.html>; *see also*
<https://www.monetha.io/blog/rewards/earn-money-from-your-data/>

1 **K. Facebook’s History of Egregious Privacy Violations**

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

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

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

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

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

25
26
27 ⁷⁰ <https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter>

1 145. Facebook found itself in another privacy scandal in 2015 when it was revealed that
2 Facebook could not keep track of how many developers were using previously downloaded
3 Facebook user data. That same year, it was also revealed that Facebook had violated users' privacy
4 rights by harvesting and storing Illinois' users' facial data from photos without asking for their
5 consent or providing notice. Facebook ultimately settled claims related to this unlawful act for
6 \$650 million.

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

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

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

20 149. On February 18, 2021, the New York State Department of Financial Services
21 released a report detailing the significant privacy concerns associated with Facebook's data
22 collection practices, including the collection of health data. The report noted that while Facebook
23 maintained a policy that instructed developers not to transmit sensitive medical information,
24 Facebook received, stored, and analyzed this information anyway. The report concluded that
25

26 _____
⁷¹ <https://www.cnbc.com/2018/12/19/facebook-gave-amazon-microsoft-netflix-special-access-to-data-nyt.html>

27 ⁷² <https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/>

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

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

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

20 152. These revelations were confirmed by an article published by the Markup in 2022,
21 which found during the course of its investigation that Facebook’s purported “filtering” failed to
22 discard even the most obvious forms of sexual health information. Worse, the article found that
23 the data that the Meta Pixel was sending Facebook from hospital websites not only included
24

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

26 ⁷⁴ <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>

27 ⁷⁵ <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>

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

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

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

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

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

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

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

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

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

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

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

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

7 158. Likewise, in October 2022, Advocate Aurora Health informed approximately
 8 3 million patients that their Personal Health Information had been disclosed to Facebook via the
 9 Meta Pixel installed on Advocate Aurora Health’s website.⁸² Advocate Aurora Health’s data
 10 breach notification conceded that patient information had been transmitted to third parties
 11 including Facebook and Google when patients used the hospital system’s website.⁸³

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

18 160. In conjunction with its data breach notice, Advocate Aurora Health claimed that
 19 the hospital system had “disabled and/or removed the pixels from our platforms and launched an
 20 internal investigation to better understand what patient information was transmitted to our
 21

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

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

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

25 ⁸³ <https://www.advocateaurorahealth.org/>

26 ⁸⁴ <https://www.advocateaurorahealth.org/pixel-notification/faq>

27 ⁸⁵ <https://www.advocateaurorahealth.org/pixel-notification/faq>

1 vendors.”⁸⁶ Advocate Aurora Health also promised its 3 million patients that the company had
 2 instituted an “enhanced, robust technology vetting process” to prevent such disclosures of
 3 patients’ Personal Health Information in the future.⁸⁷

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

19
 20
 21 ⁸⁶ <https://www.advocateaurorahealth.org/pixel-notification/faq>

22 ⁸⁷ <https://www.advocateaurorahealth.org/pixel-notification/faq>

23 ⁸⁸ <https://healthitsecurity.com/news/wakemed-faces-data-breach-lawsuit-over-meta-pixel-use>

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

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

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

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

1 162. In November 2022, the fallout from hospital systems’ use of the Meta Pixel tool
2 expanded when Community Health Network informed 1.5 million of its patients that their
3 personal health information had been routinely transmitted and disclosed to Facebook since at
4 least April 2017.⁹³

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

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

20 165. Unlike Community Health, WakeMed, Novant, Advocate Aurora Health, and
21 other responsible hospital systems who have informed their patients of the serious privacy
22 violations resulting from the installation of Facebook’s Meta Pixel tool on their websites,
23

24 _____
25 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>

26 ⁹⁴ <https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach>

27 ⁹⁵ <https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach>

28 ⁹⁶ <https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach>

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

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

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

16 **M. Tolling, Concealment, and Estoppel**

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

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

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

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

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

13 **VI. CLASS DEFINITION**

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

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

17 175. Defendant's conduct is ongoing.

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

19 177. Plaintiff brings this action in accordance with the Code of Civil Procedure Rule
20 382 individually and on behalf of the following proposed Class and subclass:

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

25 **The Patient Subclass:** For the period January 9, 2018, to the present,
26 all California citizens who are, or were, patients of Torrance Memorial
27 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.

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

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.*;

- 1 (e) Whether Defendant's acts and practices violated the California
2 Comprehensive Computer Data Access and Fraud Act, CAL. PENAL
3 CODE § 502;
- 4 (f) Whether Defendant's acts and practices violated California's Online
5 Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575, *et seq*;
- 6 (g) Whether Defendant's acts and practices violated California's Unfair
7 Competition Law, CAL. BUS. & PROF. CODE §§ 17200, *et seq*;
- 8 (h) Whether Defendant's acts and practices violated CAL. CIVIL CODE
9 §§ 1798.81.5, § 1798.81.5;
- 10 (i) Whether Defendant's acts and practices violated CAL. CIVIL CODE §
11 1798.83;
- 12 (j) Whether Defendant was unjustly enriched;
- 13 (k) Whether Plaintiff and the Class Members are entitled to equitable relief,
14 including but not limited to injunctive relief, restitution, and
15 disgorgement; and,
- 16 (l) Whether Plaintiff and the Class Members are entitled to actual, statutory,
17 punitive or other forms of damages and other monetary relief.

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

21 183. **Adequate Representation:** Plaintiff has and will continue to fairly and adequately
22 represent and protect the interests of the Class. Plaintiff has retained counsel competent and
23 experienced in complex litigation and class actions, including litigation to remedy privacy
24 violations. Plaintiff has no interest that is in conflict with the interests of the Class, and Defendant
25 has no defenses unique to any Plaintiff. Plaintiff and her counsel are committed to vigorously
26 prosecuting this action on behalf of the members of the Class, and they have the resources to do
27

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

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

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

13 VII. CLAIMS FOR RELIEF

14 COUNT I—VIOLATION OF THE CALIFORNIA INVASION 15 OF PRIVACY ACT (“CIPA”) CAL. PENAL CODE §§ 630, 16 *ET SEQ.*

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

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

19 188. The California Legislature enacted the California Invasion of Privacy Act, CAL.
20 PENAL CODE §§ 630, *et seq.* (“CIPA”) finding that “advances in science and technology have led
21 to the development of new devices and techniques for the purpose of eavesdropping upon private
22 communications and that the invasion of privacy resulting from the continual and increasing use
23 of such devices and techniques has created a serious threat to the free exercise of personal liberties
24 and cannot be tolerated in a free and civilized society.” *Id.* § 630. Thus, the intent behind CIPA is
25 “to protect the right of privacy of the people of this state.” *Id.*
26
27

1 189. CAL. PENAL CODE § 631(a) generally prohibits individuals, businesses, and other
2 legal entities from “aid[ing], agree[ing] with, employ[ing], or conspir[ing] with” a third party to
3 read, attempt to read, or to learn the contents or meaning of any message, report, or
4 communication while the same is in transit or passing over any wire, line, or cable, or is being
5 sent from, or received at any place within this state; or to use, or attempt to use, in any manner,
6 or for any purpose, or to communicate in any way, any information so obtained.

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

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

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

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

21 194. The Plaintiff and Class Members had a reasonable expectation of privacy
22 regarding the confidentiality of their communications with Defendant. Defendant told them they
23 would not sell, rent, license, or trade their personally identifiable information to third parties
24 without express consent. Defendant never received that express consent. Nor could Defendant
25 have received consent from Plaintiff and Class Members because Defendant never sought to, nor
26
27

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

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

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

- 7 (a) Plaintiff and Class Members' personal computing devices;
- 8 (b) Plaintiff and Class Members' web browsers;
- 9 (c) Plaintiff and Class Members' browser-managed files;
- 10 (d) Facebook's Meta Pixel;
- 11 (e) Internet cookies;
- 12 (f) Defendant's computer servers;
- 13 (g) Third-party source code utilized by Defendant; and
- 14 (h) Computer servers of third parties (including Facebook) to which
15 Plaintiff and Class Members' communications were disclosed.

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

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

- 21 (a) The parties to the communications;
 - 22 (b) The precise text of patient search queries;
 - 23 (c) Personally identifying information such as patients' IP addresses,
24 Facebook IDs, browser fingerprints, and other unique identifiers;
 - 25 (d) The precise text of patient communications about specific doctors;
- 26
27
28

- 1 (e) The precise text of patient communications about specific medical
- 2 conditions;
- 3 (f) The precise text of patient communications about specific treatments;
- 4 (g) The precise text of patient communications about scheduling
- 5 appointments with medical providers;
- 6 (h) The precise text of patient communications about billing and payment;
- 7 (i) The precise text of specific buttons on Defendant’s website(s) that
- 8 patients click to exchange communications, including Log-Ins,
- 9 Registrations, Requests for Appointments, Search, and other buttons;
- 10 (j) The precise dates and times when patients click to Log-In on
- 11 Defendant’s website(s);
- 12 (k) The precise dates and times when patients visit Defendant’s websites;
- 13 (l) Information that is a general summary or informs third parties of the
- 14 general subject of communications that Defendant send back to
- 15 patients in response to search queries and requests for information
- 16 about specific doctors, conditions, treatments, billing, payment, and
- 17 other information; and
- 18 (m) Any other content that Defendant has aided third parties in scraping
- 19 from webpages or communication forms at web properties.

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

22 200. No legitimate purpose was served by Defendant’s willful and intentional
23 disclosure of Plaintiff’s and Class Members’ Personal Health Information to Facebook. Neither
24 Plaintiff nor Class Members consented to the disclosure of their Personal Health Information by
25 Defendant to Facebook. Nor could they have consented, given that Defendant never sought
26

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

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

7 202. Plaintiff and the Class Members seek statutory damages in accordance with
8 § 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the
9 amount of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well
10 as injunctive or other equitable relief.

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

- 13 (a) Sensitive and confidential information that Plaintiff and Class Members
14 intended to remain private is no longer private;
- 15 (b) Defendant eroded the essential confidential nature of the doctor-patient
16 relationship;
- 17 (c) Defendant took something of value from Plaintiff and Class Members and
18 derived benefit therefrom without Plaintiff's and Class Members'
19 knowledge or informed consent and without sharing the benefit of such
20 value;
- 21 (d) Plaintiff and Class Members did not get the full value of the medical
22 services for which they paid, which included Defendant's duty to maintain
23 confidentiality; and
- 24 (e) Defendant's actions diminished the value of Plaintiff and Class Members'
25 personal information.
- 26
27
28

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

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

13 **COUNT II—VIOLATION OF CALIFORNIA**
14 **CONFIDENTIALITY OF MEDICAL INFORMATION ACT**
 (“CMIA”) CIVIL CODE § 56.06

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

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

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

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

25 210. Defendant violated Civil Code section 56.06 because it did not maintain the
26 confidentiality of users’ medical information. Instead, Defendant disclosed Plaintiff’s and Class
27

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

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

8 212. Accordingly, Plaintiff and Class members are entitled to: (1) nominal damages of
9 \$1,000; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant
10 to 56.36(c); and (4) reasonable attorney's fees and other litigation costs reasonably incurred.

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

- 13 (a) Sensitive and confidential information that Plaintiff and Class Members
14 intended to remain private is no longer private;
- 15 (b) Defendant eroded the essential confidential nature of the doctor-patient
16 relationship;
- 17 (c) Defendant took something of value from Plaintiff and Class Members and
18 derived benefit therefrom without Plaintiff's and Class Members'
19 knowledge or informed consent and without sharing the benefit of such
20 value;
- 21 (d) Plaintiff and Class Members did not get the full value of the medical
22 services for which they paid, which included Defendant's duty to maintain
23 confidentiality; and
- 24 (e) Defendant's actions diminished the value of Plaintiff and Class Members'
25 personal information.
- 26
27
28

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

3 **COUNT III—VIOLATION OF CMIA CIVIL CODE**
4 **§ 56.101**

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

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

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

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

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

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

22 221. Accordingly, Plaintiff and Class Members may recover: (1) nominal damages of
23 \$1,000; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant
24 to 56.36(c); and (4) reasonable attorney’s fees and other litigation costs reasonably incurred.

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

- 1 (a) Sensitive and confidential information that Plaintiff and Class Members
2 intended to remain private is no longer private;
- 3 (b) Defendant eroded the essential confidential nature of the doctor-patient
4 relationship;
- 5 (c) Defendant took something of value from Plaintiff and Class Members and
6 derived benefit therefrom without Plaintiff's and Class Members'
7 knowledge or informed consent and without sharing the benefit of such
8 value;
- 9 (d) Plaintiff and Class Members did not get the full value of the medical
10 services for which they paid, which included Defendant's duty to maintain
11 confidentiality; and
- 12 (e) Defendant's actions diminished the value of Plaintiff and Class Members'
13 personal information.

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

16 **COUNT IV—VIOLATION OF CMIA CIVIL CODE § 56.10**

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

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

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

23 227. Defendant disclosed medical information without first obtaining authorization
24 when it disclosed Plaintiff's and Class Members' sensitive medical information to Facebook
25 without consent, including information concerning their health status, medical diagnoses,
26
27

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

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

5 229. Accordingly, Plaintiff and Class Members may recover: (1) nominal damages of
6 \$1,000; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant
7 to 56.36(c); (4) punitive damages pursuant to 56.35; and (5) reasonable attorney's fees and other
8 litigation costs reasonably incurred.

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

- 11 (a) Sensitive and confidential information that Plaintiff and Class Members
12 intended to remain private is no longer private;
- 13 (b) Defendant eroded the essential confidential nature of the doctor-patient
14 relationship;
- 15 (c) Defendant took something of value from Plaintiff and Class Members and
16 derived benefit therefrom without Plaintiff's and Class Members'
17 knowledge or informed consent and without sharing the benefit of such
18 value;
- 19 (d) Plaintiff and Class Members did not get the full value of the medical
20 services for which they paid, which included Defendant's duty to maintain
21 confidentiality; and
- 22 (e) Defendant's actions diminished the value of Plaintiff and Class Members'
23 personal information.

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

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

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

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

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

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

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

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

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

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

27

28

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

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

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

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

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

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

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

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

- 1 (b) Defendant eroded the essential confidential nature of the doctor-patient
2 relationship;
- 3 (c) Defendant took something of value from Plaintiff and Class Members and
4 derived benefit therefrom without Plaintiff's and Class Members'
5 knowledge or informed consent and without sharing the benefit of such
6 value;
- 7 (d) Plaintiff and Class Members did not get the full value of the medical
8 services for which they paid, which included Defendant's duty to maintain
9 confidentiality; and
- 10 (e) Defendant's actions diminished the value of Plaintiff and Class Members'
11 personal information.

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

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

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

20 **COUNT VI—VIOLATION OF THE COMPREHENSIVE**
21 **COMPUTER DATA ACCESS AND FRAUD ACT**
22 **(“CDAFA”) CAL. PENAL CODE § 502**

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

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

26 252. The California Legislature enacted the Comprehensive Computer Data Access and
27 Fraud Act, CAL. PENAL CODE § 502 (“CDAFA”) to “expand the degree of protection . . . from
28

1 tampering, interference, damage, and unauthorized access to [including the extraction of data
2 from] lawfully created computer data and computer systems,” finding and declaring that “the
3 proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of
4 unauthorized access to computers, computer systems, and computer data,” and that “protection of
5 the integrity of all types and forms of lawfully created computers, computer systems, and
6 computer data is vital to the protection of the privacy of individuals . . .” CAL. PENAL CODE
7 § 502(a).

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

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

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

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

23 257. Under § 502(b)(12) of the CDAFA a “Computer contaminant” is defined as “any
24 set of computer instructions that are designed to . . . record, or transmit information within a
25 computer, computer system, or computer network without the intent or permission of the owner
26 of the information.” Defendant violated § 502(c)(8) by knowingly and without permission
27

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

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

- 5 (a) Sensitive and confidential information that Plaintiff and Class Members
6 intended to remain private is no longer private;
- 7 (b) Defendant eroded the essential confidential nature of the doctor-patient
8 relationship;
- 9 (c) Defendant took something of value from Plaintiff and Class Members and
10 derived benefit therefrom without Plaintiff's and Class Members'
11 knowledge or informed consent and without sharing the benefit of such
12 value;
- 13 (d) Plaintiff and Class Members did not get the full value of the medical
14 services for which they paid, which included Defendant's duty to maintain
15 confidentiality; and
- 16 (e) Defendant's actions diminished the value of Plaintiff and Class Members'
17 personal information.

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

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

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

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

7 **COUNT VII—BREACH OF IMPLIED-IN-FACT CONTRACT**

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

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

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

17 266. Defendant solicited and invited Plaintiff and Patient Subclass Members to provide
18 their Private Health Information on its website as part of Defendant’s regular business practices.
19 Plaintiff and Patient Subclass Members accepted Defendant’s offers and provided their Private
20 Health Information to Defendant as part of acquiring Defendant’s medical services. Per its
21 contractual, legal, ethical, and fiduciary duties, Defendant was obligated to take adequate
22 measures to protect Plaintiff’s and Patient Subclass Members’ Personal Health Information from
23 unauthorized disclosure to third parties such as Facebook. These facts give rise to the inference
24

25 _____
26 ⁹⁷ <https://www.torrancememorial.org/website-privacy-notice/>

27 ⁹⁸ <https://www.torrancememorial.org/website-privacy-notice/>

28 ⁹⁹ <https://www.torrancememorial.org/website-privacy-notice/>

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

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

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

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

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

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

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

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

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

21 275. Plaintiff and Patient Subclass Members accepted Defendant's medical services
22 offer and fully performed their obligations under the implied contract with Defendant by
23 providing their Personal Health Information to Defendant among other obligations. Plaintiff and
24 Patient Subclass Members would not have provided and entrusted their Personal Health
25 Information to Defendant in the absence of their implied contracts with Defendant and would
26
27

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

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

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

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

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

22 280. Under the implied contracts, Defendant and/or its affiliated healthcare providers
23 promised and were obligated to: (a) provide healthcare to Plaintiff and Patient Subclass Members;
24 and (b) protect Plaintiff's and the Patient Subclass Members' Personal Health Information
25 provided to obtain such healthcare. In exchange, Plaintiff and Patient Subclass Members agreed
26
27

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

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

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

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

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

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

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

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

12 288. Defendant also materially breached its contractual obligation to protect Plaintiff's
13 and Patient Subclass Members' non-public Personal Health Information when it failed to
14 implement adequate security measures and policies to protect the confidentiality of that
15 information. For example, on information and belief, Defendant (1) failed to implement internal
16 policies and procedures prohibiting the disclosure of patients' Personal Health Information
17 without consent to third-party advertising companies like Facebook, (2) failed to implement
18 adequate reviews of the software code and java script installed on its websites to ensure that
19 patients' Personal Health Information was not being automatically routed without consent to
20 third-party advertising companies like Facebook, (3) failed to provide adequate notice to the
21 public that visitors to its websites risked having their Personal Health Information shared with
22 third-party advertising companies like Facebook, (4) failed to take other industry-standard privacy
23 protection measures such as providing a "cookie" acceptance button on its website homepages,
24 (5) failed to implement internal policies and educational programs to ensure that Defendant's
25 website managers and coders were familiar with the legal regulations governing the disclosure
26 patient Personal Health Information to third parties, and (6) failed to install adequate firewalls or
27

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

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

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

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

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

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

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

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

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

COUNT VIII—QUASI-CONTRACT/RESTITUTION/UNJUST ENRICHMENT

1
2 297. Plaintiff re-alleges and incorporates all preceding paragraphs.

3
4 298. Plaintiff Jane Doe brings this claim on behalf of herself and all members of the Patient Subclass.

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

6
7 300. “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.

8
9
10
11 301. 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.

12
13
14
15
16 302. 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.

17
18
19
20
21
22 303. 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

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

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

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

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

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

25 **COUNT IX—VIOLATION OF CAL. BUS. & PROF. CODE §§**
26 **17200 ET. SEQ.**

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

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

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

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

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

20 313. Defendant’s business acts and practices are also “fraudulent” within the meaning
21 of the UCL. Defendant expressly promised Plaintiff and Patient Subclass Members that they were
22 committed to protecting the confidentiality of their Personal Health Information. Defendant also
23 promised that they would never “sell, rent, license, or trade” patients’ personally identifying
24 information “to third parties for their own direct marketing use unless we receive your express
25 consent to do so.” These promises were false. Defendant regularly shared Plaintiff and Patient
26 Subclass Members’ Personal Health Information with Facebook so that Facebook could target
27

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

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

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

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

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

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

20 319. Consumers also value their personal health data. According to the annual Financial
21 Trust Index Survey conducted by the University of Chicago's Booth School of Business and
22 Northwestern University's Kellogg School of Management, which interviewed more than 1,000
23 Americans, 93 percent would not share their health data with a digital platform for free. Half of
24 the survey participants would only share their data for \$100,000 or more, and 22 percent would
25 only share their data if they received between \$1,000 and \$100,000.¹⁰¹

26 _____
27 ¹⁰⁰ <https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/>

28 ¹⁰¹ <https://www.beckershospitalreview.com/healthcare-information-technology/how-much-should-health-data-cost->

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

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

17 **COUNT IX—VIOLATION OF CAL. CIVIL CODE § 1798.83**

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

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

21 324. California CIVIL CODE § 1798.83 requires that “if a business has an established
22 business relationship with a customer and has within the immediately preceding calendar year
23 disclosed personal information” to a third party and “knows or reasonably should know that the
24 third parties used the personal information for the third parties’ direct marketing purposes, that
25 business shall” provide in writing to its customers free of charge (1) a list of the categories of
26

27 _____
100k-or-more-according-to-patients.html

1 personal information provided to third parties and (2) the names and addresses of all third parties
2 who received the customers' personal information during the preceding calendar year. The kinds
3 of "personal information" that the statute expressly protects includes "medical information,
4 "health insurance information," and any other kind of information that "identifies, relates to,
5 describes, or is capable of being associated with ... a particular individual." CAL. CIVIL CODE
6 § 1798.80.

7 325. Any customer who is injured by a violation of the statute may institute a civil action
8 to recover damages. CAL. CIVIL CODE § 1798.84(b). Additionally, "for a willful, intentional, or
9 reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three
10 thousand dollars (\$3,000) per violation; otherwise, the customer may recover a civil penalty of up
11 to five hundred dollars (\$500) per violation for a violation of Section 1798.83." CAL. CIVIL CODE
12 § 1798.84(c). Further, any business that violates, proposes to violate, or has violated this statute
13 may be enjoined. CAL. CIVIL CODE § 1798.84(e).

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

15 327. Defendant failed to disclose to Plaintiff and Patient Subclass Members that it was
16 regularly collecting, transmitting, and sharing their Personal Health Information with Facebook
17 so that Facebook could target them with advertising. Defendant willfully, intentionally, and/or
18 recklessly failed to provide the information and disclosures required by CAL. CIVIL CODE §
19 1798.83 as part of a scheme to barter Plaintiff's and Patient Subclass Members' Personal Health
20 Information to Facebook in return for access to the Meta Pixel tool.

21 328. Plaintiff and Patient Subclass Members conferred a benefit on Defendant in the
22 form of valuable sensitive medical information that Defendant collected from Plaintiff and Patient
23 Subclass Members under the guise of keeping this information private. Defendant collected, used,
24 and disclosed this information for its own gain, including for advertisement purposes, sale, or
25 trade for valuable services from Facebook and other third parties. Defendant had knowledge that
26 Plaintiff and Patient Subclass Members had conferred this benefit on Defendant by interacting
27

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

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

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

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

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

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

- 4 (a) Sensitive and confidential information that Plaintiff and Patient Subclass
5 Members intended to remain private is no longer private;
- 6 (b) Defendant eroded the essential confidential nature of the doctor-patient
7 relationship;
- 8 (c) Defendant took something of value from Plaintiff and Patient Subclass
9 Members and derived benefit therefrom without Plaintiff's and Patient
10 Subclass Members' knowledge or informed consent and without sharing the
11 benefit of such value;
- 12 (d) Plaintiff and Patient Subclass Members did not get the full value of the
13 medical services for which they paid, which included Defendant's duty to
14 maintain confidentiality; and
- 15 (e) Defendant's actions diminished the value of Plaintiff and Patient Subclass
16 Members' personal information.

17 334. Plaintiff also continues to desire to search for health information on Torrance
18 Memorial's website. She will continue to suffer harm if Defendant does not make adequate
19 disclosures regarding which third party marketing companies are receiving Plaintiff's and Patient
20 Subclass Members' protected health information. Plaintiff and the Patient Subclass Members are
21 therefore also entitled to injunctive relief requiring Defendant to comply with CAL. CIV. CODE §
22 1798.83.

23 VIII. DEMAND FOR JURY TRIAL

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

25 IX. PRAYER FOR RELIEF

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

- 1 A. Certifying the Classes and appointing Plaintiff as the Classes' representative;
- 2 B. Appointing the law firms of Caddell & Chapman, Ahmad, Zavitsanos, &
- 3 Mensing P.C., and Turke & Strauss, LLP as Class Counsel;
- 4 C. Finding that Defendant's conduct was unlawful, as alleged herein;
- 5 D. Awarding such injunctive and other equitable relief as the Court deems just and
- 6 proper;
- 7 E. A declaration that Defendant is financially responsible for all Class notice and
- 8 the administration of Class relief;
- 9 F. Awarding Plaintiff and the Class Members statutory, actual, compensatory,
- 10 consequential, punitive, and nominal damages, as well as restitution and/or
- 11 disgorgement of profits unlawfully obtained;
- 12 G. Awarding Plaintiff and the Class members pre-judgment and post-judgment
- 13 interest;
- 14 H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and
- 15 expenses; and
- 16 I. Granting such other relief as the Court deems just and proper.

15 Dated: January 9, 2023

Respectfully submitted,

16 By: /s/ Michael A. Caddell

17 Michael A. Caddell (SBN 249469)

18 mac@caddellchapman.com

Cynthia B. Chapman (SBN 164471)

19 cbc@caddellchapman.com

Amy E. Tabor (SBN 297660)

20 aet@caddellchapman.com

CADDELL & CHAPMAN

21 P.O. BOX 1311

MONTEREY CA 93942

22 Tel.: (713) 751-0400

23 Fax: (713) 751-0906

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

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

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Claims Tenet Healthcare Discloses Website Visitors' Data to Facebook, Others Without Consent](#)
