49D01-2308-PL-031254
Filed: 8/9/2023 9:37 AM
Clerk
Marion Superior Court 1
Marion County, Indiana

INDIANA COMMERCIAL COURT

STATE OF INDIANA	)	IN THE MARION SUPERIOR COURT 1
	) SS:	
COUNTY OF MARION	)	CAUSE NO. _____

JANE DOE, Individually, and on behalf of all others similarly situated,	)
Plaintiff	)
v.	)
MARGARET MARY COMMUNITY HOSPITAL, INC. d/b/a MARGARET MARY HEALTH,	)
Defendant.	)

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff, JANE DOE, Individually, and on behalf of all others similarly situated (hereinafter "Plaintiff") brings this Class Action Complaint against Defendant, MARGARET MARY COMMUNITY HOSPITAL, INC. d/b/a MARGARET MARY HEALTH (hereinafter "MMH" or "Defendant"), and alleges, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiff brings this class action to address Defendant's improper practice of disclosing the confidential Personally Identifying Information ("PII")[1] and/or Protected Health

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

Information ("PHI")[2] (collectively referred to as "Private Information") of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"),[3] Google, LLC ("Google"), Microsoft Corp. ("Microsoft"), LinkedIn Corp. ("LinkedIn"), Hotjar, Ltd. ("Hotjar"), and potentially others ("the Disclosure") via tracking technologies used on its website.

2. The Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC") warn about the "serious privacy and security risks related to the use of online tracking technologies" present on websites or online platforms, such as Defendant's, that "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[4] OCR and FTC agree that such tracking technologies, like those present on Defendant's website, "can track a user's online activities" and "gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users."[5] OCR and FTC warn that "[i]mpermissible

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). MMH is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021. Plaintiff's reference to both "Facebook" and "Meta" throughout this complaint refer to the same company.

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

[5] *Id.*

disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others."[6]

3. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

4. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

[6] Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **attached as Exhibit A.**

5. Defendant MMH is an Indiana-based, nonprofit hospital and health network that treats a patient population of approximately 65,000 people, who are largely residents of Ripley County, Franklin County, and the surrounding area.[7]

6. Defendant encourages its patients to use its website, https://www.mmhealth.org/about-mmh/ (the "Website"), and its various web-based tools and services (collectively, the "Online Platforms"), which allow patients to search for physicians, locate healthcare facilities, learn about specific health conditions and treatment options, and more.

7. Despite its unique position as a massive and trusted healthcare provider, MMH knowingly configured and implemented into its Website devices known as "pixels" (also known as "trackers" or "tracking technologies"), which then collected and transmitted patients' Private Information to Facebook and other third parties, without the patient's knowledge or authorization. The information transmitted to Facebook and others included information communicated by patients through Defendant's sensitive and presumptively confidential Online Platforms.

8. When Plaintiff and Class Members used Defendant's Website and Online Platforms, they thought they were communicating exclusively with their trusted healthcare provider. Unbeknownst to them, Defendant embedded pixels from Facebook, Google, Microsoft, and others into its Website, surreptitiously forcing Plaintiff and Class Members to transmit intimate details about their medical treatment to third parties without their consent.

9. A pixel (also referred to as a "tracker" or "tracking technology") is a snippet of code embedded into a website that tracks information about its visitors and their website interactions.[8] When a person visits a website with an embedded pixel, the pixel tracks "events"

[7] About Us, Margaret Mary Health, https://www.mmhealth.org/about-mmh/ (last visited Aug. 2, 2023).
[8] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

(i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted.[9] Then, the pixel transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing.[10]

10. Among the trackers that Defendant embedded onto its Website is the Facebook Pixel (also referred to as the "Meta Pixel" or "Pixel"). By default, the Meta Pixel tracks information about a visitor's device, including their IP address, and the pages viewed.[11] When configured to do so, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[12] Additionally, the Meta Pixel can link a visitor's website interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to be linked with their Facebook profile.[13]

11. Operating as designed and as implemented by Defendant, the Meta Pixel allowed Defendant to unlawfully disclose Plaintiff and Class Members' private health information alongside identifying details to Facebook. By installing the Meta Pixel on its Website, Defendant effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled them to disclose Private Information and confidential communications to Facebook without their authorization or knowledge.

12. Facebook encourages and recommends use of its Conversions Application

[9] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[10] *Id.*
[11] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).
[12] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[13] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." What are Cookies?, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

Programming Interface ("CAPI") alongside use of the Meta Pixel.[14]

13. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[15, 16]

14. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[17]

15. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners (like Defendant) to circumvent any ad blockers or other denials of consent by the website user that would prevent the Meta Pixel from sending website users' Private Information to Facebook directly.

16. Defendant utilized data from these trackers to market its services and bolster its profits. Meta Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical

---

[14] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, How to Implement Facebook Conversions API (In Shopify), FETCH & FUNNEL https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

[15] What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last updated May 20, 2022).

[16] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api (last visited May 15, 2023).

[17] About Conversions API, META FOR DEVELOPERS, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

conditions and other information disclosed to Defendant.

17. The information that Defendant's Meta Pixel and CAPI sent to Facebook can include the Private Information that Plaintiff and Class Members submitted to Defendant's Website, including, for example, the contents of their search queries, the pages they visited, and the content they viewed.

18. Such information allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers, who then geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via the Meta Pixel and CAPI. Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

19. In addition to the Facebook tracker and CAPI, Defendant installed other tracking technology, including Google Analytics with Google Tag Manager, Facebook Events, Hotjar,[18] Bizographics,[19] and Microsoft Universal Event Tracking. On information and belief, these trackers operate similarly to the Meta Pixel and transmit a website user's Private Information to other third parties.

20. Healthcare patients simply do not anticipate that their trusted healthcare provider will send Personal Health Information or other confidential medical information collected via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy

[18] Hotjar is a tracker provided by Hotjar, Ltd. that, when installed on a website, creates heatmaps of where visitors click, records user interactions with the website, and more. See Everything You Ever Wanted to Know About Your Website, Hotjar, https://www.hotjar.com/ (last visited Aug. 3, 2023).
[19] Bizographics is a tracker provided by LinkedIn Corp. that collects website visitor information for the purpose of targeting them with personalized advertisments. See LinkedIn Corporation, Better, https://better.fyi/trackers/bizographics.com/ (last visited Aug. 3, 2023).

violations in pursuit of ever-increasing advertising revenue—without the patients' consent.

21. Neither Plaintiff nor any Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook, Google, Microsoft, LinkedIn, and Hotjar, or any other third parties uninvolved in their treatment.

22. Despite willfully and intentionally incorporating tracking technology, including the Meta Pixel and other trackers, into its Website and servers, MMH never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications with third parties including Facebook, Google, Microsoft, LinkedIn, and Hotjar.

23. Plaintiff and Class Members were unaware that their Private Information was being secretly transmitted to Facebook and other third parties as they communicated their confidential PHI with their healthcare provider via the Website and Online Platforms.

24. Defendant further made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendant.

25. Defendant owed common law, statutory, and regulatory duties to keep Plaintiff's and Class Members' communications and Private Information safe, secure, and confidential.

26. Upon information and belief, MMH utilized the Meta Pixel and other tracker data to improve and to save costs on its marketing campaigns, improve its data analytics, attract new patients, and generate sales.

27. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and to safeguard that information from unauthorized disclosure.

28. Defendant breached its statutory and common law obligations to Plaintiff and Class

Members by, *inter alia*, (i) failing to adequately review its marketing programs and web based technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and conspiring with third parties to intercept communications sent and received by Plaintiff and Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook and others; (v) failing to protect Private Information and take steps to block the transmission of Plaintiff's and Class Members' Private Information through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiff and Class Members; and (vii) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

29. Plaintiffs seek to remedy these harms and bring causes of action for (I) Negligence; (II) Negligence *Per Se*; (III) Invasion of Privacy; (IV) Breach of Implied Contract; (V) Unjust Enrichment; (VI) Breach of Fiduciary Duty; and (VII) Violation of the Indiana Deceptive Consumer Sales Act.

PARTIES

30. Plaintiff, JANE DOE, is a natural person and a resident and citizen of Indiana, where she intends to remain, with a principal residence in Greensburg in Decatur County. She is a former patient of MMH and a victim of Defendant's unauthorized Disclosure of Private Information.

31. Defendant, MARGARET MARY COMMUNITY HOSPITAL, INC. d/b/a MARGARET MARY HEALTH ("MMH" or "Defendant"), is a nonprofit corporation organized and existing under the laws of the State of Indiana, with its principal place of business at 321 Mitchell Avenue, Batesville, Indiana 47006 in Franklin County.

JURISDICTION AND VENUE

32. This Court has jurisdiction over the subject matter of this action by virtue of Indiana Rule Trial Procedure 4.4 because MMH operates and provides services within the state of Indiana.

33. This case is eligible for the Indiana Commercial Court docket under Indiana Commercial Court Rules 2 and 4.

COMMON FACTUAL ALLEGATIONS

A. Background

34. MMH, headquartered in Batesville, Indiana, is one of the largest healthcare providers in Indiana. [20] It treats approximately 65,000 patients hailing from Ripley County, Franklin County, and the surrounding area.[21] MMH provides a wide range of both inpatient and outpatient services, including behavioral health care, cancer care, diabetes care, emergency services, family medicine, heart and vascular care, hospice, obstetrics and gynecology, occupational health, orthopaedic services, rehab services, sleep medicine, surgery, wound care, and more.[22]

35. Defendant portrays itself as a technologically proficient, trusted provider, stating "[a]t Margaret Mary, we want to earn your trust. And in order to do that, we have to prove we have well-trained staff, up-to-date technology and organized systems in place."[23]

36. MMH's main campus is located at 321 Mitchell Avenue in Batesville, Indiana. It also operates ten other clinics and facilities: MMH Center at Brookville, 11137 U.S. 52, Brookville, Indiana; MMH Center of Osgood, 112 North Buckeye Street, Osgood, Indiana; MMH Center at Milan, 930 North Main Street, Milan, Indiana; Margaret Mary Physician Center, 26 Six

[20] About Us, Margaret Mary Health, https://www.mmhealth.org/about-mmh/ (last visited Aug. 2, 2023).
[21] *Id.*
[22] Services, Margaret Mary Health, https://www.mmhealth.org/services/ (last visited Aug. 2, 2023).
[23] About Us, Margaret Mary Health, https://www.mmhealth.org/about-mmh/ (last visited Aug. 2, 2023).

Pine Ranch Road, Batesville, Indiana; Margaret Mary Medical Arts Center, 188 State Route 129, Batesville, Indiana; Margaret Mary Outpatient & Cancer Center, 24 Six Pine Ranch Road, Batesville, Indiana; Margaret Mary Rehabilitation Center, 206 State Route 129, Batesville, Indiana; Margaret Mary Orthopaedic & Specialty Center, 256 State Route 129, Batesville, Indiana; Margaret Mary Professional Center, 1033 State Route 229, Batesville, Indiana; and Margaret Mary Occupational Health & Wellness Center, 1051 State Route 229, Batesville, Indiana.[24]

37. MMH serves many of its patients via its Website and Online Platforms, which it encourages patients to use to find healthcare services and providers, access information about specific health conditions, find contact information, and more.[25]

38. In furtherance of that goal, and to increase the success of its advertising and marketing and sales, Defendant purposely installed the Meta Pixel and other trackers onto its Website. Defendant's use of the Meta Pixel did not only generate information for its own use, however; it also shared patients' Private Information, including that of the Plaintiff and Class Members, with Facebook and other third parties.

39. To better understand Defendant's unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows.

i. Facebook's Business Tools and the Meta Pixel

40. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[26]

41. In conjunction with its advertising business, Facebook encourages and promotes

[24] Locations, Margaret Mary Health, https://www.mmhealth.org/locations/ (last visited Aug. 2, 2023).
[25] *See generally*, Margaret Mary Health, https://www.mmhealth.org/ (last visited Aug. 2, 2023).
[26] Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

42. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

43. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[27] Businesses that want to target customers and advertise their services, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[28]

44. One such Business Tool is the Meta Pixel, a tool that "tracks the people and type of actions they take."[29] When a user accesses a webpage that is hosting the Meta Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook—traveling from the user's browser to Facebook's server.

45. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate patient privacy (such as the homepage) and disable it on pages that do implicate patient privacy (such as Defendant's "Find a Doctor" page).

---

[27] Specifications for Facebook Pixel Standard Events, META, https://www.facebook.com/business/help/402791146561655 (last visited Jan. 31, 2023); *see also* Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS; https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Best Practices for Facebook Pixel Setup, META https://www.facebook.com/business/help/218844828315224; App Events API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).

[28] About Standard and Custom Website Events, META, https://www.facebook.com/business/help/964258670337005; *see also* Facebook, App Events API, *supra*.

[29] Retargeting, META, https://www.facebook.com/business/goals/retargeting.

46. The Meta Pixel's primary purpose is for marketing and ad targeting and sales generation.[30]

47. Facebook's own website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[31]

48. According to Facebook, the Meta Pixel can collect the following data.

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** (emphasis added).
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
>
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[32]

49. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.
- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.
- **Measure the results of your ads.** Better understand the impact of your ads

[30] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[31] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).
[32] Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

by measuring what happens when people see them.[33]

50. Facebook likewise benefits from the data received from the Meta Pixel and uses the data to serve targeted ads and identify users to be included in such targeted ads.

ii. Defendant's Method of Transmitting Plaintiff's and Class Members' Private Information via the Meta Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Meta Pixel

51. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

52. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

53. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.[34]

54. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

55. When an individual visits a website, their web browser sends an HTTP Request to

[33] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

[34] "Cookies are small files of information that a web server generates and sends to a web browser . . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

the entity's servers that essentially asks the website to retrieve certain information (such as Defendant's "Find a Doctor" page). The entity's servers send the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate a website.

56. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

57. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user.

58. Defendant's implementation of the Meta Pixel is source code that acted much like a traditional wiretap, intercepting and transmitting communications intended only for Defendant.

59. Separate from the Meta Pixel, Facebook and other website owners can place third-party cookies in the web browsers of users logged into their websites or services. These cookies can uniquely identify the user so the cookie owner can track the user as she moves around the internet—whether on the cookie owner's website or not. Facebook uses this type of third-party cookie when Facebook account holders use the Facebook app or website. As a result, when a Facebook account holder uses Defendant's Website, the account holder's unique Facebook ID is sent to Facebook, along with the intercepted communication, allowing Facebook to identify the patient associated with the Private Information it has intercepted.

60. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. To counteract this, third parties bent on gathering data and Private Information implement workarounds that are difficult to detect or evade.

Facebook's workaround is its Conversions API tool, which is particularly effective because the data transmitted via this tool does not rely on the website visitor's web browsers. Rather, the information travels directly from the entity's server to Facebook's server.

61. Conversions API "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[35] Thus, the entity receives and stores its communications with patients on its server before Conversions API collects and sends those communications—and the Private Information contained therein—to Facebook.

62. Notably, client devices do not have access to host servers and thus cannot prevent (or even detect) this additional transmission of information to Facebook.

63. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the host server, Facebook instructs companies like Defendant to "[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website events [with Facebook] that the pixel may lose."[36] Thus, if an entity implemented the Meta Pixel in accordance with Facebook's documentation, it is also reasonable to infer that it implemented the Conversions API tool on its Website.

64. The third parties to whom a website transmits data through pixels and other tracking technology do not provide any substantive content on the host website. In other words, Facebook and others like it are not providing anything to the user relating to the user's communications. Instead, these third parties are typically procured to track user data and communications only to serve the marketing purposes of the website owner (i.e., to bolster profits).

---

[35] About Conversions API, META, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).
[36] *See* Best Practices for Conversions API, META, https://www.facebook.com/business/help/308855623839366 (last visited May 15, 2023).

65. Accordingly, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer its patients' computing devices, causing the device's web browser to contemporaneously and invisibly re-direct the patients' communications to hidden third parties like Facebook.

66. In this case, Defendant employed the Meta Pixel and potentially Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

67. Consequently, when Plaintiff and Class Members visited Defendant's website and communicated their Private Information, it was simultaneously intercepted and transmitted to Facebook.

68. MMH also employed other trackers, including Google Analytics with Google Tag Manager, Facebook Events, Hotjar, Bizographics, and Microsoft Universal Event Tracking, which, on information and belief, likewise transmitted Plaintiff's and the Class Members' Private Information to third parties, without Plaintiff's and Class Members' knowledge or authorization.

iii. Defendant Violated its own Privacy Policy

69. MMH, its doctors and employees, and its clinics are all covered under its Joint Notice of Privacy Policies, which is posted and maintained on Defendant's Website ("Privacy Policy").[37]

70. On information and belief, Defendants do not maintain a separate Website privacy policy.

71. Defendants' Privacy Policy provides, "THIS NOTICE DESCRIBES HOW

[37] *See* Margaret Mary Health, Joint Notice of Privacy Practices (revised Oct. 1, 2013), https://web.archive.org/web/20210410120351/https://www.mmhealth.org/privacy-policy/ (visited Aug. 3, 2023), **attached as Exhibit B.**

HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO THIS INFORMATION."

72. Therein, MMH further acknowledges, represents, and promises:

> We are dedicated to maintaining the privacy of your health information. In conducting our business, we will create records regarding you and the treatment and services we provided to you. We are required by law to maintain the confidentiality of health information that identifies you which we call "protected health information", or "PHI" for short. We are required by law to notify you following a breach of your unsecured health information. We also are required by law to provide you with this Notice of our legal duties and the privacy practices that we maintain concerning your PHI. The terms of this Notice apply to all records containing your personal health information that are created or retained by us. By federal and state law, we must follow the terms of the Notice of Privacy Practices that we have in effect at the time.[38]

73. Under the section "PERMITTED USES AND DISCLOSURES," Defendant lists "the different ways in which [it] may use and disclose your PHI."[39] Those "permitted uses and disclosures" include for the purposes of medical treatment, collecting payment, healthcare operations, and more.[40] For the purpose of marketing and/or advertising is not a "permitted use and disclosure" of PHI, according to Defendant's Privacy Policy.[41]

74. In the section "USE AND DISCLOSURE OF YOUR PHI IN CERTAIN SPECIAL CIRCUMSTANCES" Defendant's policy addresses "Marketing/Sale of PHI" specifically.[42] Therein, the Privacy Policy states "[m]ost uses and disclosures of your PHI for marketing purposes will be made only with your written authorization. We cannot give or sell lists of patients to a third party for the purpose of the third party marketing its own products. Such a use would require an

[38] Margaret Mary Health, Joint Notice of Privacy Practices (revised Oct. 1, 2013), https://web.archive.org/web/20210410120351/https://www.mmhealth.org/privacy-policy/ (visited Aug. 3, 2023).
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*

express written authorization from you."[43]

75. Concerning "YOUR RIGHTS REGARDING YOUR PHI," Defendant's Privacy Policy states that patients have the right to "Confidential Communications" and the "Right to Provide an Authorization for Other Uses and Disclosures. We will obtain your written authorization for uses and disclosures that are not identified by this Notice or permitted by applicable law."[44]

76. Despite these representations, MMH does indeed transfer Private Information to third parties without its patients' written authorization. Via the Meta Pixel, Defendants used and disclosed Plaintiff's and Class Member's Private Information and confidential communications to Facebook, Google, and other third parties without authorization and in violation of its own Privacy Policy.

77. Defendants disclosed Plaintiff's and Class Members' Private Information and confidential communications to Facebook and potentially many others by collecting and transmitting user interactions with Defendant's Website and sending records of those interactions to Facebook.

78. Defendant installed the Meta Pixel on its Website on or prior to December 30, 2019. The Pixel remained on Defendant's Website until as recently as June 16, 2023. MMH removed the Meta Pixel from its Website sometime after June 16, 2023.

79. During the years that Defendant utilized the Meta Pixel, MMH tracked and recorded patients' interactions with and movement through its Website while simultaneously transmitting those records to Facebook. For example, when a visitor navigated to the Website's "Services" page and selected "Cancer Care," the Meta Pixel sent to Facebook the URLs of each

[43] *Id.* (underline added).
[44] *Id.*

page viewed. These URLs revealed information about the type of medical treatment that the patient is seeking. For instance, if a patient viewed the Website page "Cancer Treatments," Defendant shared with Facebook via Meta Pixel that the visitor viewed a page about "cancer-care/treatments/."

80. Similarly, if a patient navigated to the "Events" page of the Website and viewed the "Hope Cancer Support Group," Facebook would have received a report that the patient viewed a page about "events/hope-cancer-support-group."

81. In the same way, if a Website visitor used the "Find a Doctor" search, Facebook would receive that information ("find-a-doctor"). And if the visitor clicked to learn more about that specific doctor, that doctor's name was also shared with Facebook (e.g., "doctor/gina-chung-md/").

82. Defendant configured the Meta Pixel to share with Facebook each visitor's search terms. For example, if a patient searched Defendant's Website for the term "cancer," the Meta Pixel then that information is transmitted to Facebook (e.g., "s=Cancer"). If the patient then clicked on one of the results, the Meta Pixel would alert Facebook that the patient has viewed a page about "know-the-facts-on-cervical-cancer" and that the patient navigated to that page after searching the Website for the term "cancer."

83. As Defendant transmitted this information to Facebook via the Meta Pixel, it did so alongside identifying details, such as the individual's IP address, web browser and operating system, Facebook cookie, and/or other unique identifiers. In this way, Defendant records and shares PII and PHI—Private Information—with Facebook.

84. Defendant could have chosen not to use the Meta Pixel, or it could have configured the Pixel to limit the information that it communicated to third parties. It did not. Instead, it

intentionally took advantage of the Meta Pixel's features and functions, resulting in the Disclosure of Plaintiffs' and Class Members' Private Information.

85. Along those same lines, Defendant could have chosen not to use Google Analytics with Google Tag Manager, Facebook Events, Hotjar, Bizographics, and Microsoft Universal Event Tracking to track Plaintiff and Class Members private communications and transmit that information to unauthorized third parties. It did so anyway, intentionally taking advantage of these trackers, despite the harms posed to Plaintiff and Class Members' privacy.

86. Defendant used and disclosed Plaintiff's and Class Members' Private Information to Facebook, Google, and possibly other third parties for the exclusive purpose of marketing its services and increasing its profits.

87. On information and belief, Defendants shared, traded, or sold Plaintiff's and Class Members' Private Information with Facebook, and potentially other third parties, in exchange for improved targeting and marketing services.

88. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant MMH to intercept their communications or to use or disclose their Private Information for marketing purposes. Plaintiff was never provided with any written notice that Defendant disclosed its patients' Protected Health Information to Facebook and others, nor were they provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiff's Protected Health Information to unauthorized entities.

89. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

90. Furthermore, Defendants actively misrepresented their commitment and intention to

preserve the confidentiality and privacy of Plaintiff's and Class Members' Private Information. In actuality, Defendant was sharing information about Plaintiffs' and Class Members with Facebook anytime they used its Website.

91. By law, Plaintiffs and the Class Members are entitled to privacy in their Protected Health Information and confidential communications. MMH deprived Plaintiff and Class Members of their privacy rights when it (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential communications, Personally Identifiable Information, and Protected Health Information; (2) disclosed patients' Private Information to unauthorized, third-party eavesdroppers, including Facebook and possibly others; and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent.

B. Plaintiff's Experiences

92. Plaintiff Jane Doe is a former patient of Defendant who received healthcare services from MMH and physicians in MMH's network. Ms. Doe became a patient of Defendant around 2016. She has received care at Defendant's main campus in Batesville, as well as Defendant's Six Pine Ranch Road location, also in Batesville. Ms. Doe has been treated by MMH physicians for knee replacement, thyroid care, high blood pressure, colonoscopy, sciatic pain, generative disc disease, and chest pain.

93. Ms. Doe accessed Defendant's Website and Online Platforms at Defendant's direction and encouragement. Ms. Doe used the Website between the years of 2018 and 2021. She last used the Website around 2021, to search for a new orthopedic doctor.

94. Ms. Doe reasonably expected that her online communications with MMH were confidential, solely between herself and MMH, and that, as such, those communications would not

be transmitted to or intercepted by a third party.

95. Plaintiff Ms. Doe provided her Private Information to Defendant and trusted that the information would be safeguarded according to MMH's privacy policy and legal obligations.

96. As described herein, by use of the Meta Pixel and tracking technology, MMH sent Ms. Doe's Private Information to Facebook, Google, and others when she used Defendant's Online Platforms to communicate healthcare and identifying information to MMH.

97. Pursuant to the process described herein, MMH assisted Facebook and possibly others with intercepting Ms. Doe's confidential communications, including those that contained PII and PHI. MMH facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

98. By failing to receive the requisite consent, MMH breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

99. Since using Defendant's Website, Ms. Doe's Facebook feed has included ads related to arthritis, knee replacement, sciatica pain, and knee and back braces.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

100. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[45] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

101. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data

[45] Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.

collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective . . . at preventing the receipt of sensitive data."[46]

102. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[47] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[48]

103. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "[w]e do not have an adequate level of control and explainability over how our systems use data,

[46] New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.
[47] Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.
[48] *Id.*

and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[49]

104. Furthermore, in June 2022, an investigation by The Markup[50] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[51] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[52] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[53]

105. During its investigation, The Markup found that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[54]

106. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the Meta

[49] Lorenzo Franceschi-Bicchierai, Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document, VICE (April 26, 2022) https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.
[50] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed Mar. 19, 2023).
[51] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
[52] *Id.*
[53] *Id.*
[54] *Id.*

Pixel inside their password-protected patient portals.[55]

107. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals capturing and sharing patient data in this way.[56]

D. Defendant Violated HIPAA Standards

108. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[57]

109. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

110. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[58]

111. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written

[55] *Id.*
[56] *Id.*
[57] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[58] U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

> authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[59]

112. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology.[60]

113. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[61]

114. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules**. For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks

[59] U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.
[60] *See* U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html.
[61] *Id.*

> medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [62]

115. In other words, HHS has expressly stated that Defendant's conduct of implementing the Meta Pixel is a violation of HIPAA Rules.

E. Defendant Violated FTC Standards, and the FTC and HSS Take Action

116. The FTC has also recognized that implementation of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[63]

117. On July 20, 2023, the Federal Trade Commission (FTC) along with the U.S. Department of Health and Human Services (HHS) sent a "joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online activities."[64]

118. Therein, the FTC reminded healthcare providers of their HIPAA obligations: "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules."[65]

---

[62] *Id.* (emphasis in original) (internal citations omitted).
[63] Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf).
[64] FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.
[65] *Id.*

119. Additionally, the FTC reminded health providers of their "obligation to protect against impermissible disclosures of personal health information," adding that "[t]his is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes."[66]

120. Entities that are not covered by HIPAA also face accountability when consumers' sensitive health information is compromised under the FTC's Health Breach Notification Rule. 16 C.F.R. § 318. This requires that companies dealing with health records must notify the FTC and consumers if there has been a breach of unsecured identifiable health information, or else face civil penalties for violations. *Id*. According to the FTC, "a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, including sharing of covered information without an individual's authorization, triggers notification obligations under the Rule."[67]

121. The FTC Act makes it unlawful to employ "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" 15 U.S.C. § 45(a).

122. According to the FTC, "the disclosure of [sensitive health] information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule."[68]

---

[66] *Id.*

[67] Statement of the Commission: On Breaches by Health Apps and Other Connected Devices, U.S. Fed. Trade Commission, (Sept. 15, 2021) (available at https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf).

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

F. Defendant Violated Industry Standards

123. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

124. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to MMH and its physicians.

125. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care . . . . Patient privacy encompasses a number of aspects, including . . . personal data (informational privacy).

126. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

127. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically . . . must . . . release patient information only in keeping ethics guidelines for confidentiality.

G. Plaintiff's and Class Members' Expectation of Privacy

128. At all times when Plaintiff and Class Members provided their Private Information

---

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

to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial marketing and sales purposes, unrelated to patient care.

H. IP Addresses are Personally Identifiable Information

129. Defendant also disclosed and otherwise assisted Facebook and potentially others with intercepting Plaintiff's and Class Members' IP addresses using the Meta Pixel and other tracking technologies.

130. An IP address is a number that identifies the address of a device connected to the Internet.

131. IP addresses are used to identify and route communications on the Internet.

132. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

133. Facebook tracks every IP address ever associated with a Facebook user.

134. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

135. Under HIPAA, an IP address is Personally Identifiable Information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

136. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

I. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

137. The sole purpose for Defendant's use of the Meta Pixel and other tracking technology was marketing and profits.

138. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook and likely others in the form of enhanced advertising services and more cost-efficient marketing on its platform.

139. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients.

140. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

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

141. Plaintiff's data and Private Information has economic value. Facebook regularly uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

142. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is due to increase; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

143. In particular, the value of health data is well-known due to the media's extensive reporting on the subject. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry." Therein, Time Magazine

described the extensive market for health data and observed that the health data market is both lucrative and a significant risk to privacy.[69]

144. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[70]

TOLLING, CONCEALMENT, AND ESTOPPEL

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

146. MMH seamlessly incorporated Meta Pixel and other trackers into its Website and Online Platforms while providing users with no indication that their usage was being tracked and transmitted to third parties. MMH knew that its Website incorporated Meta Pixel and other trackers, yet it failed to disclose to Plaintiff and Class Members that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook, and likely other third parties, including Google, Microsoft, LinkedIn, and Hotjar.

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

148. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. MMH's illegal interception and disclosure of Class Members' Private Information has continued unabated through at least June 16, 2023.

---

[69] *See* Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry, TIME, (Jan. 9, 2017 at 9:00 a.m.) https://time.com/4588104/medical-data-industry/.

[70] *See* Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

What's more, MMH was under a duty to disclose the nature and significance of their data collection practices but did not do so. MMH is therefore estopped from relying on any statute of limitations defenses.

CLASS ALLEGATIONS

149. Plaintiff brings this statewide class action on behalf of herself and on behalf of other similarly situated persons.

150. The statewide Class that Plaintiff seeks to represent is defined as follows:

> **All Indiana citizens whose Private Information was disclosed by Defendant to third parties through the Meta Pixel and related technology without authorization.**

151. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

152. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

153. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly used or disclosed by Defendant, and the Class is identifiable within Defendant's records.

154. Commonality: Questions of law and fact common to the Class exist and

predominate over any questions affecting only individual Class Members. These include

a. whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' Private Information;

b. whether Defendant had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for non-healthcare purposes;

d. whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for unauthorized purposes;

e. whether Defendant failed to adequately safeguard Plaintiff's and Class Members' Private Information;

f. whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. whether Defendant failed to properly implement and configure the tracking software on its Online Platforms to prevent the disclosure of confidential communications and Private Information;

i. whether Defendant engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiff's and Class Members' Private Information.

155. Typicality: Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use and incorporation of

Meta Pixel and other tracking technology.

156. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

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

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

impractical and impose a burden on the courts.

159. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged. If the class action device were not used, Defendant would necessarily gain an unconscionable advantage because they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

162. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful use and disclosure and failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to and obtain proper consent from Class Member, and Defendant may continue to act unlawfully as set forth in this Complaint.

163. Further, Defendant has acted or refused to act on grounds generally applicable to

the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

164. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. whether Defendant breached the implied contract;

f. whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been used and disclosed to third parties;

g. whether Defendant failed to implement and maintain reasonable security procedures and practices;

h. whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information; and

i. whether Plaintiff and the Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's

wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

165. Plaintiff realleges and incorporates the above allegations as if fully set forth herein.

166. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using Plaintiff's and Class Members' Private Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that occurred.

167. Defendant acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiff's and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and Defendant.

168. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's disclosure of their Private Information to benefit third parties and Defendant. Defendant actively sought and obtained Plaintiff's and Class Members' Private Information.

169. Private Information is highly valuable, and Defendant knew, or should have known, the harm that would be inflicted on Plaintiff and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendant by way of data harvesting, advertising, and increased sales.

170. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal

information and Private Information of Plaintiff and Class Members. This failure actually and proximately caused Plaintiff's and Class Members' injuries.

171. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, inappropriate advertisements and use of their Private Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

172. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendant's negligence. These injuries are ongoing, imminent, immediate, and continuing.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

173. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

174. Plaintiff alleges this negligence *per se* theory as alternative to her other negligence claims.

175. Pursuant to the laws set forth herein, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security

Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, Defendant was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Private Information.

176. Plaintiff and Class Members are within the class of persons that these statutes and rules were designed to protect.

177. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII and PHI.

178. Defendant owed a duty to timely and adequately inform Plaintiff and Class Members, in the event of their PII and PHI being improperly disclosed to unauthorized third parties.

179. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiff's and Class Members' PII and PHI in compliance with applicable laws would result in an unauthorized third-party such as Facebook gaining access to Plaintiff's and Class Members' PII and PHI, resulting in Defendant's liability under principles of negligence *per se*.

180. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI and not complying with applicable industry standards as described in detail herein.

181. Plaintiff's and Class Member's PII and PHI constitute personal property that was taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

182. As a proximate result of Defendant's negligence and breach of duties as set forth

above, Defendant's breaches of duty caused Plaintiff and Class Members to, *inter alia*, have their data shared with third parties without their authorization or consent, receive unwanted advertisements that reveal seeking treatment for specific medical conditions, fear, anxiety and worry about the status of their PII and PHI, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their PII and PHI, all of which can constitute actionable actual damages.

183. In failing to secure Plaintiff's and Class Members' PII and PHI, Defendant is guilty of oppression, fraud, or malice. Defendant acted or failed to act with a reckless, willful, or conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, in addition to seeking actual damages, also seeks punitive damages on behalf of herself and the Class.

184. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' PII and PHI, and as a result, Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek actual, compensatory, and punitive damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence *per se*.

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

185. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

186. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and Online Platforms and the communications platforms and services therein.

187. Plaintiff and Class Members communicated sensitive PHI and PII—Private

Information—that they intended for only Defendant to receive and that they understood Defendant would keep private.

188. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion and their private affairs and concerns.

189. Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's representations and its Privacy Policy. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendant's disclosure of PHI coupled with PII is highly offensive to the reasonable person.

190. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

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

192. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

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

194. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

195. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

196. As a condition of receiving medical care from Defendant, Plaintiff and the Class provided their Private Information and paid compensation for the treatment received. In so doing, Plaintiff and Class Members entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Policy and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

197. Implicit in the agreement between MMH and its patients, Plaintiff and the proposed Class Members, was the obligation that both parties would maintain the Private Information confidentially and securely.

198. MMH had an implied duty of good faith to ensure that the Private Information of Plaintiff and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from MMH.

199. MMH had an implied duty to protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses.

200. Additionally, MMH implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

201. Plaintiff and Class Members fully performed their obligations under the implied contract with MMH. MMH did not. Plaintiff and Class Members would not have provided their confidential Private Information to MMH in the absence of their implied contracts with MMH and

would have instead retained the opportunity to control their Private Information for uses other than receiving medical treatment from MMH.

202. MMH breached the implied contracts with Plaintiff and Class members by disclosing Plaintiff's and Class Members' Private Information to an unauthorized third party.

203. MMH's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiff and Class Members to provide their Private Information in exchange for medical treatment and benefits.

204. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities.

205. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

206. Plaintiff re-alleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

207. This claim is pleaded solely in the alternative to Plaintiff's Breach of Implied Contract claim.

208. Plaintiff and Class Members conferred a monetary benefit upon MMH in the form of valuable sensitive medical information that Defendant collected from Plaintiff and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiff and the Class Members conferred a

benefit on Defendant in the form of monetary compensation.

209. Plaintiff and Class Members would not have used MMH's services or would have paid less for those services, if they had known that Defendant would collect, use, and disclose their Private Information to third parties.

210. MMH appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

211. As a result of MMH's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

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

213. MMH should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the unauthorized Disclosure alleged herein.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

214. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

215. A relationship existed between Plaintiff and the Class, on the one hand, and

Defendant, on the other, in which Plaintiff and the Class put their trust in Defendant to protect the Private Information of Plaintiff and the Class, and Defendant accepted that trust.

216. Defendant breached the fiduciary duty that it owed to Plaintiff and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, their Private Information.

217. Defendant's breach of fiduciary duty was a legal cause of injury-in-fact and damage to Plaintiff and the Class.

218. But for Defendant's breach of fiduciary duty, the injury-in-fact and damage to Plaintiff and the Class would not have occurred.

219. Defendant's breach of fiduciary duty contributed substantially to producing the damage to the Plaintiff and the Class.

220. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and Class Members are entitled to and do demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT VII
VIOLATION OF THE INDIANA DECEPTIVE CONSUMER SALES ACT
(On Behalf of Plaintiff and the Class)

221. Plaintiff re-alleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

222. The purposes and policies of the Indiana Deceptive Consumer Sales Act (the "DCSA"), Indiana Code § 24-5-0.5-1 to -12, are to:

> (1) simplify, clarify, and modernize the law governing deceptive and unconscionable consumer sales practices;
> (2) protect consumers from suppliers who commit deceptive and unconscionable consumer sales practices; and

(3) encourage the development of fair consumer sales practice.

Ind. Code § 24-5-0.5-1(b).

223. The General Assembly has instructed courts to construe the DCSA liberally to promote these purposes and policies. Ind. Code § 24-5-0.5-1(a)

224. MMH is a "supplier" as defined in the DCSA because it is a seller or other person who regularly engages in or solicits consumer transactions, which are defined to include sales of personal property, *services*, and intangibles that are primarily for a personal, familial, or household purpose, such as those at issue in this action. Ind. Code § 24-5-0.5-2(1), (3) (emphasis added).

225. The DCSA provides that "[a] supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Such an act, omission, or practice by a supplier is a violation of [the DCSA] whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations." Ind. Code § 24-5-0.5-3(a).

226. An "incurable deceptive act" is a "deceptive act done by a supplier as part of a scheme, artifice, or device with the intent to defraud or mislead. Ind. Code § 24-5-0.5-2(a)(8).

227. The DCSA further provides:

> Without limiting the scope of subsection (a) the following acts, and the following representations as to the subject matter of a consumer transaction, made orally, in writing, or by electronic communication, by a supplier, are deceptive acts:
>
> a. That such subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have
> b. That such subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not . . . .

Ind. Code § 24-5-0.5-3

228. MMH committed deceptive acts, including but not limited to:.

a. Encouraging patients to use MMH's Website and Online Platform while representing its commitment to protecting the privacy of the Personal Information. Defendant also promised patients that it will never sell their medical information without patients' written authorization. Despite these representations, MMH disclosed to third parties information relating to Plaintiff's and Class Members' medical treatment, without their knowledge, consent, or authorization, as part of a scheme, artifice or device with the intent to mislead patients.

b. Plaintiff and Class Members relied on MMH's representations in using MMH's Website and Online Platform and thought they were communicating only with their trusted healthcare provider. Instead, their confidential MMH tracked, recorded, and leaked those communications to Facebook and others.

c. By installing and implementing the Meta Pixel, Defendant knew or reasonably should have known it intercepted and transmitted Plaintiff's and Class Member's communications from Plaintiff's and Class Members' browsers directly to Facebook. Likewise, by installing or implementing CAPI, Defendant knew or reasonably should have known that it recorded on its servers and transmitted to Facebook Plaintiff's and Class Member's confidential communications. Despite this knowledge, it did not inform Plaintiff or Class Members that their online communications were not secure.

229. MMH's violations were willful and were done as part of a scheme, artifice, or device with intent to defraud or mislead, and therefore are incurable deceptive acts under the DCSA.

230. The DCSA provides that "[a] person relying upon an uncured or incurable

deceptive act may bring an action for the damages actually suffered as a consumer as a result of the deceptive act or five hundred dollars ($500), whichever is greater. The court may increase damages for a willful deceptive act in an amount that does not exceed the greater of: (i) three (3) times the actual damages of the consumer suffering the loss; or (ii) one thousand dollars ($1,000). Ind. Code § 24-5-0.5-4(a).

231. The DCSA provides that "[a]ny person who is entitled to bring an action under subsection (a) on the person's own behalf against a supplier for damages for a deceptive act may bring a class action against such supplier on behalf of any class of persons of which that person is a member . . . ." Ind. Code § 24-5-0.5-4(b).

232. Had Plaintiff and members of the Classes been aware that their Private Information would be transmitted to unauthorized third parties, they would not have entered into such transactions and would not have provided payment or confidential medical information to MMH.

233. As a direct and proximate result of Defendant's unfair and deceptive acts and practices in violation of the DCSA, Plaintiff and Class Members have suffered damages for which Defendant is liable.

234. Plaintiff and Class Members seek actual damages plus interest on damages at the legal rate, as well as all other just and proper relief afforded by the DCSA. As redress for Defendant's repeated and ongoing violations, Plaintiff and Class Members are entitled to, *inter alia*, actual damages, treble damages, attorneys' fees, and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, JANE DOE, individually, and on behalf of all others similarly situated, prays for judgment as follows:

A. for an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and Plaintiff's counsel as Class Counsel;

B. for equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. for equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;

D. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. an order Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

F. an Order requiring Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

G. for an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. for an award of punitive damages, as allowable by law;

I. for an award of attorneys' fees under the DCSA, the common fund doctrine, and any other applicable law;

J. costs and any other expenses, including expert witness fees incurred by Plaintiff in connection with this action;

K. pre- and post-judgment interest on any amounts awarded; and

L. such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Dated: August 9, 2023

Respectfully submitted,

/s/ Lynn A. Toops

Lynn A. Toops (No. 26386-49)
Mary Kate Dugan (No. 37623-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
mdugan@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class

ClassAction.org