**IN THE SUPERIOR COURT OF DEKALB COUNTY**
**STATE OF GEORGIA**

| | | |
|---|---|---|
| **JANE DOE,** individually, on behalf of her minor children, **JOHN DOE I** and **JOHN DOE II,** and on behalf of all others similarly situated, | ) | 24CV3735 |
| **Plaintiff,** | ) | Case No. _____ |
| **v.** | ) | |
| **CHILDREN'S HEALTHCARE OF ATLANTA, INC.** | ) | |
| **Defendant.** | ) | |

**CLASS ACTION COMPLAINT AND JURY DEMAND**

Plaintiff, Jane Doe, individually, on behalf her two minor children, John Doe I and John Doe II., and on behalf of all others similarly situated, (hereinafter "Plaintiffs") brings this Class Action Complaint against Defendant, Children's Healthcare of Atlanta, Inc. (hereinafter "Children's," "CHOA" or "Defendant"), and alleges, upon personal knowledge as to her 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 Information ("PHI")[2] (collectively referred to as "Private Information") of Plaintiff and the

[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).

[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,

proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta")[3] 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 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,

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). CHOA 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.*

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 may disclose a person's personally identifiable protected health information to a third party without express written authorization.

5. Children's Healthcare of Atlanta is a nonprofit healthcare organization that operates the only freestanding pediatric healthcare system in Georgia and touts itself as a "top pediatric healthcare system in the Southeast."[7]

6. Despite its unique position as a trusted community healthcare provider, CHOA knowingly configured and implemented into its website, https://www.choa.org/ (the "Website"),

[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.**

[7] https://www.choa.org/about-us (last acc. Mar. 22, 2024).

code-based tracking devices known as "trackers" or "tracking technologies," which collected and transmitted Plaintiff and Class Members' Private Information to third party platforms such as Facebook and potentially other third parties, using the Meta Pixel, AdRoll, Marketo's Munchkin, and potentially other tracking technologies, without Plaintiff and Class Members' knowledge or authorization.

7. Defendant encourages patients to use its Website, along with its various web-based tools and services (collectively, the "Online Platforms"), to find doctors[8] and locations;[9] schedule appointments and follow-up visits;[10] access the patient/billing portal ("MyChart");[11] learn about particular health conditions and treatments,[12] and more.

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 tracking technologies from Facebook, AdRoll, and Marketo's Munchkin into its Website and Online Platforms, surreptitiously forcing Plaintiff and Class Members to transmit intimate details about their medical treatment to third parties without their consent.

9. Facebook's tracker is called the Meta Pixel (also referred to as the "Pixel"). The Meta Pixel is a snippet of code, embedded into a website, that tracks information about its visitors and their website interactions.[13] As a visitor uses the website, the Meta Pixel records any "events"

[8] Doctors, CHOA, https://www.choa.org/search?tab=doctors&ran=16 (last acc. Mar. 22, 2024).
[9] Locations, CHOA, https://www.choa.org/search?q=&tab=locations&zip= (last acc. Mar. 22, 2024).
[10] Schedule an Appointment, CHOA, https://www.choa.org/appointments
[11] MyChart Patient Portal, CHOA, https://mychart.choa.org/mychart/Authentication/Login? (last acc. Mar. 22, 2024).
[12] Medical Services, CHOA https://www.choa.org/medical-services (last acc. Mar. 22, 2024).
[13] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

it is configured to track, such as pages viewed, buttons clicked, and information submitted.[14] Then, the Pixel transmits the event information back to the website server and to Facebook, where it can be combined with other data and used for marketing.[15]

10. By default, the Meta Pixel tracks information about a website user's device and the URLs and domains they visit.[16] When configured to do so, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[17] 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.[18]

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 Plaintiff's 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 that website owners who use the Metal Pixel also employ a Business Tool called Conversions Application Programming Interface

[14] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[15] *Id.*
[16] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).
[17] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[18] 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).

("CAPI").[19]

13. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interactions from the website owner's private servers, which transmits the data directly to Facebook, without involvement from the website user's browser.[20, 21]

14. 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. For this reason, 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."[22]

15. Defendant utilized data from these trackers to market its services and bolster its profits. Facebook utilizes data from the Meta Pixel and CAPI to build data profiles for the purpose of creating targeted online advertisements and enhanced marketing services, which it sells for profit.

---

[19] "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).

[20] 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).

[21] "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).

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

16. The information that Defendant's Meta Pixel and possibly CAPI sent to Facebook included Private Information that Plaintiff and Class Members submitted to Defendant's Website, including, for example, the pages they visited, the content they viewed, and the buttons they clicked. Such information allows third parties (e.g., Facebook) to learn about a particular individual's health conditions and their seeking of medical care.

17. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers, who then target Plaintiff and Class Members with online advertisements, based on the information they communicated to Defendant via the Website. 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.

18. In addition to the Facebook tracker and likely CAPI, Defendant installed other tracking technologies, including AdRoll and Marketo's Munchkin. On information and belief, these trackers operate similarly to the Meta Pixel and transmitted Plaintiff and Class Members' Private Information to unauthorized third parties.

19. Healthcare patients simply do not anticipate that their trusted healthcare provider will send their private health information to a hidden third party—let alone Facebook, a company with a sordid history of violating consumer privacy in pursuit of ever-increasing advertising revenue—without their consent.

20. Neither Plaintiff nor any Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook, AdRoll, Marketo's Munchkin, or any other third parties uninvolved in their treatment.

21. Despite willfully and intentionally incorporating the Meta Pixel, potentially CAPI,

and other third-party trackers into its Website and servers, CHOA has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications and Private Information with third parties including Facebook, AdRoll, and Marketo's Munchkin.

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

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

24. Upon information and belief, CHOA 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.

25. 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 their information from unauthorized disclosure.

26. 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 its 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, AdRoll, Marketo's Munchkin; (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.

27. Plaintiff seeks 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; (VII) Breach of Confidence; and (VIII) Bailment.

## PARTIES

28. Plaintiff Jane Doe is a natural person and a resident and citizen of Georgia, where she intends to remain, with a principal residence in Conyers, in Rockdale County. Her minor children, John Doe I and John Doe II are patients of CHOA and victims of Defendant's unauthorized Disclosure of Private Information.

29. Defendant, Children's Healthcare of Atlanta, Inc. is a nonprofit corporation organized and existing under the laws of the State of Georgia with its principal place of business at 1575 Northeast Expressway, Atlanta, Georgia, 30329, in Dekalb County and may be served through its registered agent CSC of Cobb County, Inc., 192 Anderson Street SE, Suite 125, Marietta, GA 30060.

## JURISDICTION AND VENUE

30. This Court has subject matter jurisdiction over this case under O.C.G.A. § 15-6-8.

31. This Court has personal jurisdiction over Defendant because it is organized under the laws of Georgia, transacts business in Georgia, and maintains its principal places of business in Georgia.

32. Venue is proper under O.C.G.A. § 9-10-93 because Fulton County is where a substantial part of the business was transacted, and where tortious acts alleged herein and injury occurred.

## COMMON FACTUAL ALLEGATIONS

### A. Background

33. CHOA, a nonprofit healthcare organization, is the largest pediatric healthcare provider in Georgia. CHOA's resources include "2,300 physicians representing more than 60 pediatric specialties and programs," three hospitals with 673 licensed beds, the Marcus Autism Center, specializing in children with autism spectrum disorder, the Center for Advanced Pediatrics, and a team of 12,700 employees.[23]

34. CHOA manages more than 1 million patient visits annually.[24]

35. CHOA promotes the convenience and functionality of its Website and online Platforms. For example, CHOA encourages families to sign up for CHOA's free mobile app so parents can "focus on your child during an appointment or hospital stay rather than worry about directions." CHOA further entices patients and their families by demonstrating the following app capabilities:

> With the Children's app, you can:
> - Find a hospital or neighborhood **location**.
> - Locate a department, patient room or **amenity** from inside our three hospitals.
> - Look up Children's **physicians**.
> - Find the nearest **Emergency Department** and see **wait times**.
> - Find the nearest **Urgent Care Center**, see wait times and save your spot in line.
> - Access your child's patient information through **MYchart**.
> - **NEW**: Access additional **amenities** such as child life services, family libraries and movie streaming when connected to the Children's Wi-Fi network.[25]

36. To enhance its marketing efforts and increase profits, Defendant purposely installed the Meta Pixel and other trackers onto its Website to gather Private Information of Plaintiff and

[23] https://www.choa.org/about-us/why-choose-childrens (last acc. Mar. 22, 2024).
[24] https://www.choa.org/about-us (last acc. Mar. 22, 2024).
[25] https://www.choa.org/patients/mobile-app (last acc. Mar. 22, 2024).

Class Members in order to enhance its marketing efforts and increase its profits. But Defendant did not only generate information for its own use: it also shared patients' Private Information, including that belonging to Plaintiff and Class Members, with Facebook, AdRoll, Marketo's Munchkin, and potentially other unauthorized third parties.

37. 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***

38. 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]

39. In conjunction with its advertising business, Facebook encourages website owners like Defendant to use its "Business Tools" to gather customer data, identify customers and potential customers, and market products and services.

40. 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.

41. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, clicks a button, fills out a form, and more.[27] Businesses that want to target customers and advertise their services can also create their own tracking

[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).

[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).

parameters by building a "custom event."[28]

42. One such Business Tool is the Meta Pixel, a tool that "tracks the people and type of actions they take."[29] When an individual 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 directly from the user's browser to Facebook's server, based off instructions from the Meta Pixel.

43. 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 a homepage, and disable it on pages that do implicate patient privacy.

44. The Meta Pixel's primary purpose is to enhance online marketing, improve online ad targeting, and generate sales.[30]

45. 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]

46. 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.

[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.
[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).

> **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]

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

48. Facebook likewise benefits from Meta Pixel data and uses it to enhance its own ad targeting abilities.

### *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*

49. 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).

50. Every website is hosted by a computer "server" that holds the website's contents

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

and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

51. 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]

52. 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.

53. When an individual visits a website, their web browser sends an HTTP Request to the entity's servers that essentially asks the website to retrieve certain information. 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.

54. 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.

55. 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.

56. In this way, the Meta Pixel acts much like a traditional wiretap, intercepting and transmitting communications intended only for the website host and diverting them to Facebook.

[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).

57. Separate from the Meta Pixel, Facebook and other third parties place cookies in the web browsers of users who visit their websites or online platforms. These cookies can uniquely identify the user, allowing the third party to track the user as they browse the internet—on the third-party site and beyond. Facebook uses its own cookie to identify users of a Meta-Pixel-enabled website and connect their activities on that site to their individual identity. As a result, when a Facebook account holder uses a website with the Meta Pixel, the account holder's unique Facebook ID is sent to Facebook, along with the intercepted communication, allowing Facebook to identify the user associated with the information it has intercepted.

58. With substantial work and technical know-how, internet users can sometimes circumvent these browser-based wiretap technologies. To counteract this, third parties bent on gathering data implement workarounds that are difficult for web users to detect or evade. Facebook's workaround is Conversions API, which "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[35] This makes Conversions API a particularly effective tool because it allows sends Facebook data directly from the website server to Facebook, without relying on the user's web browser. Notably, client devices do not have access to host servers containing Conversions API, and thus, they cannot prevent (or even detect) this transmission of information to Facebook.

59. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the website 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

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

events [with Facebook] that the pixel may lose."[36] Consequently, if a website owner utilizes the Meta Pixel on its website, it is also reasonable to infer that it implemented the Conversions API on its website server(s), in accordance with Facebook's documentation.

60. The Meta Pixel, Conversions API, and other third-party trackers do not provide any substantive content on the host website. Rather, their only purpose is to collect information to be used for marketing and sales purposes.

61. Accordingly, without any knowledge, authorization, or action by a user, a website owner can use its website source code to commandeer its users' computing devices and web browsers, causing them to invisibly re-direct the users' communications to Facebook, Google, or others.

62. 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.

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

64. CHOA also employed trackers from AdRoll and Marketo's Munchkin. On information and belief, Defendant likewise transmitted Plaintiff's and the Class Members' Private Information to these third parties without Plaintiff's and Class Members' knowledge or authorization.

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

### *iii. Defendant's Privacy Policies Prohibit Use and Disclosure of Private Information without Authorization*

65. CHOA is covered under its Privacy Notice[37] and Terms of Use,[38] which are posted and maintained on CHOA's Website (collectively referred to as the "Privacy Policies").

66. CHOA's Privacy Notice provides, "This notice describes how medical information about your child may be used and disclosed, and how you can get access to this information." (Ex. B).

67. CHOA's Privacy Notice further acknowledges that "providers of data transmission services" are bound by the terms of the Privacy Notice:

> **Who will follow this notice:**
>
> This notice describes the privacy practices of Children's related to medical information generated at Children's. This notice applies to Children's and:
>
> - All departments and units of Children's.
> - Any member of a volunteer group we allow to help you or your child while your child is at Children's.
> - All employees, professional staff and other personnel at Children's.
> - Business associates of Children's, such as patient safety organizations, health information organizations or providers of data transmission services.

*Id.*

68. CHOA further acknowledges, represents, and promises:

[37] *See Privacy Notice, CHOA*, available at https://www.choa.org/-/media/Files/Childrens/patients/patient-privacy-notice-2021.pdf (last acc. Mar. 22, 2024) (attached hereto as **Exhibit B**).
[38] *See Terms of Use, CHOA*, available at https://www.choa.org/about-us/terms-of-use (last acc. Mar. 22, 2024) (attached as **Exhibit C**).

**OUR PLEDGE REGARDING MEDICAL INFORMATION:**

We understand that medical information about your child and your child's health is personal. We are committed to protecting medical information about your child. We create a record of the care and services your child receives at Children's. We need this record to provide your child with quality care and to comply with certain legal requirements. This notice applies to all of the records of your child's care created or maintained by Children's, whether made by Children's personnel or your child's personal doctor while at Children's. Your child's personal doctor and other doctors involved in your child's care may have different policies or notices regarding the doctor's use and disclosure of your child's medical information created in the doctor's office.

This notice will tell you about the ways in which we may use and disclose medical information about your child. We will also describe your rights and certain obligations we have regarding the use and disclosure of medical information.

We are required by law to:

- Make sure medical information that identifies your child is kept private;
- Give you this notice of our legal duties and privacy practices with respect to medical information about your child; and
- Follow the terms of the notice that is currently in effect.

*Id.*

69. CHOA delineates the ways in which it is permitted to use and disclose private information, such as for treatment, payment, and healthcare operations. *Id.* Children's specifically notes that it "must also obtain [patients'] written permission (authorization) prior to using your public [sic] health information (PHI) to send you any marketing materials. We may not sell your PHI without your written authorization." *Id.*

70. CHOA further states:

> In situations where marketing communications involve financial compensation, Children's will obtain a valid authorization from you before using or disclosing PHI for such purposes. The disclosure will indicate that we are receiving financial compensation from a third party. Additionally, where we have an arrangement with a business associate, including a subcontractor who receives financial compensation from a third party in exchange for making a communication about a product or service, such communication also requires your prior authorization.

*Id.*

71. Further, CHOA's Terms of Use, which includes its Website Privacy policy, states that Children's "will not sell your private information to any other group, party, or person." **Ex. C.**

72. CHOA's Cookie policy misleadingly tells website viewers that cookies CHOA collects from web users "do not have any private information." *Id.*

73. Despite these representations in its Privacy Policies, Defendant did, in fact, disclose Private Information to third parties for marketing purposes.

### *iv. Defendant Disclosed Plaintiff and Class Members' Private Information to Unauthorized Third Parties, Including Facebook*

74. Through its use of the Meta Pixel, AdRoll, and Marketo's Munchkin, CHOA disclosed to Facebook Plaintiff and Class Members' confidential communications on the Website, including the content they viewed and the buttons they clicked. Defendant thereby revealed to Facebook Plaintiff and Class Members' health concerns, the medical appointments they sought, their status as patients, their doctors, their usage of the patient portal and billing portal, and their requests for medical records.

75. A few examples are demonstrative here.

a. **CHOA disclosed user's keyword searches**. For example, when the user searched for the keywords, fetal care, CHOA sent PageView and Microdata events informing Facebook about the search. The Microdata event divulges the user's specific keywords "Fetal+Care."

b. **CHOA disclosed User's Service Browsing and Physician Search Details.** When a user clicked to navigate to the Find a Doctor page, CHOA sent a SubscribedButtonClick event informing Facebook that the user clicked to "Find a

Doctor." As the Find a Doctor page loaded, CHOA sent a pair of PageView and Microdata events confirming that the user is viewing the page. From the Find a Doctor page, users could search for doctors by specialty, name, or location. As the user performed searches based on each of those parameters, CHOA informed Facebook about those activities. For example, when a user searched for a physician with a specialty in cardiology, CHOA sent PageView and Microdata events informing Facebook that the user performed a search. The Microdata event also specifically discloses the user's doctor search query for "q=cardiac."

c. **CHOA also disclosed users' interactions with their search results.** For instance, when the user clicked to view Michael J Wolf, MD's profile page after searching for cardiology specialists, CHOA sent a SubscribedButtonClick event revealing that the user clicked "Michael J Wolf, MD," after searching for "cardiac . . . doctors.". Next, as the profile page for Dr. Wolf loaded, CHOA sent another set of PageView and Microdata events.

d. **CHOA Disclosed Users' Appointment Activities**. CHOA also shared details about users' appointment activities. Upon a user's clicked to make an appointment, CHOA sent a SubscribedButtonClick event disclosing that the user clicked to "Schedule an appointment with a pediatric specialist." As the appointment page loaded, CHOA transmitted PageView and Microdata events confirming the user loaded the appointment page.

e. **CHOA Disclosed Users' Appointment Activities. Disclosed Users' MyChart Activities.** Finally, CHOA disclosed when users clicked to access MyChart. Upon a user's click to sign in to MyChart, CHOA transmitted a SubscribedButtonClick

event which discloses that the user clicked a button labeled "SIGN IN TO MYCHART," leading to the page, "https://mychart.choa.org/mychart."

76. In addition to this information, the Meta Pixel collects and transmits to Facebook identifying information, including the website visitor's IP address, browser and device information, and, if applicable, their Facebook ID. Combined with information about Plaintiffs' specific medical conditions and treatments, this information constitutes Private Information, or PHI.

77. After receiving Plaintiff and Class Members' data from Defendant, Facebook processed it, analyzed it, and assimilated it into its own massive datasets, before selling access to this data in the form of targeted advertisements.

78. Employing "Audiences"—subsections of individuals identified as sharing common traits—Facebook promises the ability to "find the people most likely to respond to your ad."[39] Advertisers can purchase the ability to target their ads based on a variety of criteria: "Core Audiences," individuals who share a location, age, gender, and/or language;[40] "Custom Audiences," individuals who have taken a certain action, such as visiting a website, using an app, or buying a product bought a product;[41] and/or "Lookalike Audiences," groups of individuals who "resemble" a Custom Audience, and who, as Facebook promises, "are likely to be interested in your business because they're similar to your best existing customers.[42]

79. By sharing its patients' data with Facebook, Defendant enabled itself to take advantage of these enhanced ad targeting capabilities.

---

[39] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).
[40] *Id.*
[41] *Id.*
[42] How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Help Center, https://www.facebook.com/business/help/465262276878947 (last visited Aug. 14, 2023).

80. On information and belief, Facebook, AdRoll, and Marketo's Munchkin processed the data they received from Defendant in a similar manner and used it to build marketing and other data profiles allowing for targeted online advertising—by Defendant or other third parties.

81. Defendant could have chosen not to use the Meta Pixel, or it could have configured it to limit the information that it communicated to Facebook, but it did not. Instead, it intentionally selected and took advantage of the features and functionality of the Pixel that resulted in the Disclosure of Plaintiffs' and Class Members' Private Information.

82. Along those same lines, Defendant could have chosen not to use Facebook, AdRoll, and Marketo's Munchkin 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 harm to Plaintiff and Class Members' privacy.

83. Defendant used and disclosed Plaintiff's and Class Members' Private Information to Facebook, AdRoll, and Marketo's Munchkin, for the purpose of marketing its services and increasing its profits.

84. On information and belief, Defendants shared, traded, or sold Plaintiff's and Class Members' Private Information with Facebook, AdRoll, and Marketo's Munchkin, in exchange for improved targeting and marketing services.

85. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information for marketing purposes. Defendant did not notify Plaintiff and Class Members of its practice of disclosing patients' Private Information to Facebook, AdRoll, and Marketo's Munchkin, nor were they provided any means of opting out of such disclosures. Defendant, nonetheless, used Plaintiff and Class Members' Private Information and knowingly disclosed that Private Information to unauthorized entities for Defendant's own gain

86. Plaintiff 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.

87. Defendant misrepresented that it would preserve the security and privacy of Plaintiff's and Class Members' Private Information, while knowingly disclosing their Private Information to unauthorized third parties.

88. By law, Plaintiff and the Class Members are entitled to privacy in their Private Information and confidential communications. CHOA 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, AdRoll, and Marketo's Munchkin; (3) profited from the Disclosure; and (4) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent.

**B. Plaintiff's Experience**

89. Plaintiff Jane Doe has been using Defendant's Website for her children's healthcare since 2020.

90. John Doe II has been a patient of CHOA since 2020.

91. John Doe I has been a patient of CHOA since 2023.

92. John Doe I and John Doe II have received healthcare services from CHOA and physicians in CHOA's network for various health concerns.

93. John Doe I has sought or received care from CHOA in neurology, orthopedics, and oncology.

94. John Doe II has sought or received care from CHOA in phlebotomy and oncology.

95. John Doe I has received care at CHOA's Stockbridge and Clifton Road locations.

96. John Doe II has received care at CHOA's Atlanta and Clifton Road locations.

97. Ms. Doe relied on CHOA's Website and Online Platforms to communicate confidential patient information for her children. Ms. Doe began using the website in 2020. She used the Website's "Find a Doctor" (sic) function to search for neurologists, orthopedic doctors, phlebotomists, and oncologists.

98. Ms. Doe has also used the website to learn about health conditions and possible treatments, as well as to schedule an appointment using the Website's "Schedule an Appointment" tool.

99. Ms. Doe used Defendant's Website and Online Platforms at Defendant's direction and encouragement. Ms. Doe reasonably expected that her online communications with CHOA were confidential, solely between herself and CHOA, and that, as such, those communications would not be transmitted to or intercepted by a third party.

100. Ms. Doe provided her children's Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's legal obligations.

101. Through its use of the Meta Pixel, Defendant disclosed to Facebook

a. Ms. Doe's children's identity;

b. Ms. Doe's children's status as a patient;

c. Ms. Doe's children's seeking of medical treatment;

d. Ms. Doe's children's health conditions and the treatment she sought;

e. Ms. Doe's children's location; and

f. the name of their doctor[s].

102. By failing to receive the requisite consent to disclose Ms. Doe's children's Private Information, CHOA violated its agreements with Ms. Doe, its own policies, and the law.

103. Plaintiff paid for Defendant's healthcare services, which included reasonable privacy and data security protections for Ms. Doe's Private Information; however, Ms. Doe did not receive the privacy and security protections for which she paid.

104. Plaintiff first discovered that Defendant used the Meta Pixel and other tracking technologies to gather and disclose her children's Private Information in July 2023.

105. Because of Defendant's Disclosure, Plaintiff has suffered injuries, including monetary damages; loss of privacy; unauthorized disclosure of her children's Private Information; unauthorized access to her children's Private Information by third parties; use of her Private Information for advertising purposes; embarrassment, humiliation, frustration, and emotional distress; decreased value of hers and her children's Private Information; lost benefit of their bargain; and increased risk of future harm resulting from further unauthorized use and disclosure of this information.

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

106. 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.[43] 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.

107. 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

[43] 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."[44]

108. 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.[45] When a user was having their period or informed the app of their intention to get pregnant, Flo would inform Facebook, which could then use the data for 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."[46]

109. More recently, Facebook employees admitted to lax protections for sensitive user data. In 2021, Facebook engineers on the ad business product team conceded "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't

[44] 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.
[45] 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.
[46] *Id.*

confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[47]

110. In June 2022, an investigation by The Markup[48] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[49] 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.[50] 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."[51]

111. 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 patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also patients' names, addresses, email addresses, and phone numbers.[52]

112. 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

[47] 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.
[48] 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).
[49] 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.
[50] *Id.*
[51] *Id.*
[52] *Id.*

Pixel inside their password-protected patient portals.[53]

113. 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.[54]

**D. Defendant Violated HIPAA Standards**

114. 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.[55]

115. Guidance from the U.S. Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

116. 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.[56]

117. 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

[53] *Id.*
[54] *Id.*
[55] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[56] 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).[57]

118. In addition, HHS's Office for Civil Rights (OCR) 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.[58]

119. 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."[59]

120. The HHS Bulletin notes that such information—even when sent to an "unauthenticated webpage" (*i.e.*, a webpage that does not require users to log in before accessing the webpage) —constitutes a disclosure of PHI to the tracking technology vendor.[60]

121. 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.

---

[57] 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.
[58] *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.
[59] *Id.*
[60] 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.

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [61]

122. In other words, HHS has expressly stated that Defendant's conduct of implementing the Meta Pixel violates HIPAA Rules.

### E. Defendant Violated FTC Standards, and the FTC and HHS Take Action

123. The Federal Trade Commission ("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."[62]

124. On July 20, 2023, the FTC and 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."[63]

125. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible

[61] *Id.* (emphasis in original) (internal citations omitted).
[62] 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), **Exhibit A.**
[63] 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.

disclosures of PHI to third parties or any other violations of the HIPAA Rules"[64] and 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."[65]

126. Entities that are not covered by HIPAA also face accountability for disclosing consumers' sensitive health information under the Health Breach Notification Rule. 16 C.F.R. § 318. This Rule requires that companies dealing with health records 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."[66]

127. Additionally, 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). 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."[67]

128. As such, the FTC and HHS have expressly stated that conduct like Defendant's

[64] *Id.*
[65] *Id.*
[66] 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) (emphasis added).
[67] *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 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.

runs afoul of the FTC Act and/or the FTC's Health Breach Notification Rule.

### F. Defendant Violated Industry Standards

129. A medical provider's duty of confidentiality is a cardinal rule, embedded in doctor-patient and hospital-patient relationships.

130. The American Medical Association's ("AMA") Code of Medical Ethics requires the protection of patient privacy and communications, and these rules are applicable to CHOA and its physicians.

131. 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).

132. 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.

133. 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

134. At all times when Plaintiff and Class Members provided their Private Information to Defendant, they 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**

135. Defendant also disclosed Plaintiff's and Class Members' IP addresses to Facebook, AdRoll, and Marketo's Munchkin, through its use of the Meta Pixel and other tracking technologies.

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

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

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

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

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

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

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code," specifically listing IP addresses as an example of PII. *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).

142. 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 Trackers and Unauthorized Disclosures

143. The sole purpose for Defendant's use of the Meta Pixel and other tracking technology was to enhance its marketing efforts and increase its profits.

144. In exchange for disclosing the Private Information of its patients, Defendant was compensated by Facebook, AdRoll, Marketo's Munchkin, and likely others in the form of enhanced advertising services and more cost-efficient marketing.

145. 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.

146. 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

147. The data concerning Plaintiff and Class Members, collected and shared by Defendant, has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook, are the "people most likely to respond to your ad."[68] Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain

[68] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).

online content.[69] Facebook's "Lookalike Audiences" go further, targeting individuals who resemble current customer profiles and whom, according to Facebook, "are likely to be interested in your business."[70]

148. Data harvesting is big business, and it drives Facebook's profit center, its advertising sales. In 2019, Facebook generated nearly $70 billion dollars in advertising revenue alone, constituting more than 98% of its total revenue for that year.[71]

149. This business model is not limited to Facebook. Data harvesting 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 only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

150. 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, it described the extensive market for health data and observed that the health data market is both lucrative and a significant risk to privacy.[72]

151. 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

[69] *Id.*
[70] *See* How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Center, https://www.facebook.com/business/help/465262276878947 (last visited Aug. 14, 2023).
[71] *See* Here's How Big Facebook's Ad Business Really Is, CNN, https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html (last visited Aug. 14, 2023).
[72] *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/.

compile the data from providers and other health-care organizations and sell it to buyers."[73]

## TOLLING, CONCEALMENT, AND ESTOPPEL

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

153. CHOA seamlessly incorporated Meta Pixel and other trackers into its Website and Online Platforms while providing patients with no indication that their Website usage was being tracked and transmitted to third parties. CHOA 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, AdRoll, and Marketo's Munchkin.

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

155. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. CHOA's illegal interception and disclosure of Plaintiff's Private Information has continued unabated through the present. What is more, CHOA was under a duty to disclose the nature and significance of their data collection practices but did not do so. CHOA is therefore, is estopped from relying on any statute of limitations defenses.

## CLASS ALLEGATIONS

156. Plaintiff brings this statewide class action on behalf of her minor children and on

[73] *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.

behalf of other similarly situated persons.

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

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

158. 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.

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

160. 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.

161. Ascertainability. Class Members are readily identifiable from information in Defendant's possession, custody, and control.

162. 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's conduct amounts to negligence *per se*;

j. whether Defendant committed invasion of privacy;

k. whether Defendant breached its contract with Plaintiffs and the Class Members; or in the alternate, whether Defendant was unjustly enriched; and,

l. whether Defendant breached fiduciary duties to Plaintiff and the Class Members.

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

163. 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.

164. 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.

165. 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.

166. 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.

167. 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.

168. 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.

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

170. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful use and disclosure of Class Members' Private Information; failure to properly secure the Private Information of Class Members; and refusal to provide proper notification to and obtain proper

consent from Class Members.

171. 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.

172. 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

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. in the alternate, whether Defendant was unjustly enriched;
g. whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been used and disclosed to third parties;
h. whether Defendant failed to implement and maintain reasonable security procedures and practices;
i. whether Defendant committed an invasion of privacy;
j. whether Defendant had fiduciary duties to Plaintiffs and the Class Members;

k. whether Defendant breached its fiduciary duties; and,

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

m. 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)**

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

174. 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.

175. 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.

176. 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.

177. 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.

178. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers in the handling and securing of Private Information of Plaintiff and Class Members. This failure actually and proximately caused Plaintiff's and Class Members' injuries.

179. 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.

180. Defendant's breach of its common-law duties to exercise reasonable care 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.

181. In failing to secure Plaintiffs' and Class Members' Private Information, 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 Plaintiffs' and Class Members' rights. Plaintiffs, in addition to seeking actual damages, also seek punitive damages on behalf of her minor children

and the Class.

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

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

183. Plaintiff alleges this negligence *per se* theory as alternative to her other negligence claim.

184. 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.

185. In the alternative, and as a further basis for this claim, Defendant's conduct violated the Georgia's criminal prohibition against unauthorized wiretapping, eavesdropping, and surveillance. See Ga. Code § 16-11-60 et seq.

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

187. 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.

188. 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.

189. 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-parties like Facebook, AdRoll, and Marketo's Munchkin, gaining access to Plaintiff's and Class Members' PII and PHI, and resulting in Defendant's liability under principles of negligence *per se*.

190. 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.

191. 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.

192. 200. Additionally, Defendant violated it duty under Georgia Code § 16-11-62, including, but not limited to, the following ways.

a. Through the use of a device (i.e., the Meta Pixel and other tracking technologies) and without the consent of all persons involved, Defendant recorded the activities of Plaintiff and Class Members that occurred in a private place and out of public view.

b. Defendant intentionally and secreted intercepted by use of a device the contents of Plaintiff's and Class Members' private communications with their healthcare providers.

c. Defendant sold, gave, or distributed, without legal authority, and without consent, the records of Plaintiff's and Class Member's activities, which occurred in private

places and out of public view.

193. 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.

194. 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 her minor children and the Class.

195. 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)

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

197. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and Online Platforms.

198. 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.

199. 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 in their private affairs and concerns.

200. Plaintiff and Class Members had a reasonable 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.

201. 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.

202. 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.

203. 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.

204. 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.

205. 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)

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

207. 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, 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.

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

209. CHOA 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 CHOA.

210. CHOA had an implied duty to protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, and to notify them of any breach of that information.

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

212. Plaintiff and Class Members fully performed their obligations under the implied contract with CHOA, but Defendant did not. Plaintiff and Class Members would not have provided their confidential Private Information to CHOA in the absence of their implied contracts with

CHOA that their Private Information would be kept in confidence and would instead have retained the opportunity to control their Private Information for uses other than receiving medical treatment from CHOA.

213. CHOA breached the implied contracts with Plaintiff and Class members by disclosing Plaintiff's and Class Members' Private Information to unauthorized third parties and failing to notify them of the breach of that Private Information.

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

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

216. 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)

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

218. This claim is pleaded solely in the alternative to Plaintiff's breach of implied contract claim.

219. Plaintiff and Class Members conferred a monetary benefit upon CHOA 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, Plaintiffs and the Class Members conferred a benefit on Defendant in the form of monetary compensation.

220. Plaintiff and Class Members would not have used CHOA'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.

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

222. As a result of CHOA'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.

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

224. CHOA 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)

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

226. 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.

227. 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, indeed, intentionally disclosing, their Private Information.

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

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

230. Defendant's breach of fiduciary duty substantially contributed to the injury and damages to the Plaintiff and the Class.

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

## COUNT VII
## BREACH OF CONFIDENCE
## (On Behalf of Plaintiff and the Class)

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

233. Under Georgia law, medical providers have a duty to their patients to keep private medical information confidential.

234. Plaintiff and the Class Members had reasonable expectations of privacy in their

Private Information transmitted to and communications exchanged with Defendant, including those on the Website and Online Platforms.

235. Contrary to its duties as a medical provider and its promises of confidentiality, Defendant utilized the Meta Pixel and related tracking technologies to unauthorizedly disclose and transmit Plaintiff's and the Class Members' Private Information (i.e., PHI) and the contents of their communications with Defendant to third parties, including Facebook, AdRoll, and Marketo's Munchkin.

236. CHOA's Disclosure of Plaintiff's and Class Members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

237. As a direct and proximate result of Defendant's breach of provider-patient confidentiality, Plaintiff and the Class Members suffered erosion of the essential confidential relationship between the healthcare provider and the patient.

238. As a direct and proximate cause of Defendant's unauthorized Disclosure, Plaintiff and Class Members suffered injury and damages including but not limited to: loss of privacy; the unauthorized access of their Private Information by third parties, and improper disclosure of their Private Information; unwanted advertisements that reveal seeking treatment for specific medical conditions; fear, anxiety and worry about the status of their PII and PHI, and emotional distress; diminution in the value of their personal data for which there is a tangible value, and lost value of their Private Information; and/or a loss of control over their PII and PHI; lost benefit of their bargain; 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.

239. As a result, Plaintiff and Class Members are entitled to general damages for

invasion of their rights in an amount to be determined by a jury and nominal damages.

## COUNT VI
## BAILMENT
## (On Behalf of Plaintiff and the Class)

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

241. Defendant acquired and was obligated to safeguard the Private Information of Plaintiff and Class Members.

242. Defendant accepted possession and took control of Plaintiff's and Class Members' Private Information under such circumstances that the law imposes an obligation to safeguard the property of another.

243. Specifically, Defendant took lawful possession of the property of Plaintiff and the Class Members—their Private Information—giving rise to a duty to account for that property, without Defendant intending to appropriate it, and a constructive bailment.

244. During the bailment, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care, diligence, and prudence in protecting their Private Information.

245. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class Members' Private Information, resulting in the unlawful and unauthorized Disclosure of such Private Information to third parties, including Facebook and likely others.

246. Defendant further breached its duty to safeguard Plaintiff's and Class Members' Private Information by failing to notify them that their Private Information had been disclosed without patient authorization and compromised.

247. As a direct and proximate result of Defendant's breach of its duties of care

attendant to the bailment, Plaintiff and the Class Members have suffered injury and damages as set forth herein.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff Jane Doe, individually, on behalf of John Doe I and John Doe II, 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 an award of actual damages, compensatory damages, and statutory damages and penalties, in an amount to be determined, as allowable by law;

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

D. 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;

E. 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;

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

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

H. for an award of attorneys' fees under the common fund doctrine and any other

applicable law;

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

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

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

**JURY DEMAND**

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

Dated: April 1, 2024 Respectfully submitted,

*/s/ Joseph B. Alonso*
Joseph B. Alonso
Ga. Bar No. 013627
Daniel H. Wirth
Ga. Bar No. 873443
ALONSO WIRTH
1708 Peachtree Street, Suite 207
Atlanta, Georgia 30309
(678) 928-4472
jalonso@alonsowirth.com
dwirth@alonsowirth.com

Lynn A. Toops (*Pro Hac Vice* forthcoming)
Amina A. Thomas (*Pro Hac Vice* forthcoming)
Mary Kate (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@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