STATE OF INDIANA	)	IN THE HANCOCK CIRCUIT COURT
	) SS:	
HANCOCK COUNTY	)	CAUSE NO: 30C01-2307-MI-001202

SHERRY CHILDERS and **DIANA POLSTON**, individually and on behalf of all others similarly situated,	)
Plaintiffs,	)
v.	)
BOARD OF TRUSTEES OF THE HANCOCK REGIONAL HOSPITAL,	)
Defendant.	)

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Sherry Childers and Diana Polston, individually and on behalf of all others similarly situated (hereinafter "Plaintiffs"), bring this First Amended Class Action Complaint against Defendant, Board of Trustees of Hancock Regional Hospital d/b/a Hancock Health ("Hancock" or "Defendant"), and allege, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this case to address Defendant's outrageous, illegal, and widespread practice of disclosing Plaintiffs' and Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook"), Google, LLC ("Google"), and other unauthorized third parties (the "Disclosure").

2. 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.

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

4. Defendant operates Hancock Health, a healthcare system within Hancock County, Indiana and surrounding areas that consists of "Hancock Regional Hospital, Hancock Physician Network[,] and more than 20 other healthcare facilities."[1] In spite of its unique position as a massive and trusted healthcare provider, Defendant knowingly configured and implemented a software device known as a Tracking Pixel ("Pixel") to collect and transmit information from crh.org (the "Website") to third parties, including information communicated in sensitive and presumptively confidential patient searches such as through the "Find a Doctor" webpage (collectively the "Online Platforms").

5. Plaintiffs and other Class Members who used Defendant's Website thought they were communicating only with their trusted healthcare provider. Unbeknownst to Plaintiffs and

[1] *About*, HANCOCK HEALTH, https://www.hancockregionalhospital.org/about/ (last visited July 3, 2023).

Class Members, however, Defendant has embedded the Tracking Pixel from Facebook, Google, and other third-party tracking technology vendors on their Website, surreptitiously forcing Plaintiffs and Class Members to transmit every click, keystroke, and intimate detail about their medical treatment to third parties. Operating as designed and as implemented by Defendant, the Pixel allows the Private Information that Plaintiffs and Class Members submit to Defendant to be unlawfully disclosed to unauthorized third parties alongside the individual's IP address and unique and persistent IDs used by third parties such as Facebook ("FID").[2]

6. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[3] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

7. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Tracking Pixel is thus customizable and programmable, meaning that the website owner controls which of its pages contain the Pixel and which events are tracked and transmitted to Facebook or other third parties. By installing the Tracking Pixel on its Website, Defendant effectively planted

[2] The 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." *What are cookies?*, CLOUDFLARE, https://www.cloudflare.com/learning/privacy /what-are-cookies/ (last visited Mar. 21, 2023). "Cookies help inform websites about the user, enabling the websites to personalize the user experience." *Id.*

[3] *Regargeting*, FACEBOOK, https://www.facebook.com/business/goals/retargeting (last visited Mar. 21, 2023).

a bug on Plaintiffs' and Class Members' web browsers and compelled them to disclose their communications with Defendant to Facebook and other unauthorized third parties.

8. In addition to the Tracking Pixel, Facebook also encourages and recommends that website owners install and implement Facebook's Conversions Application Programming Interface ("CAPI") on their website servers.[4]

9. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[5] Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[6]

10. 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

[4] "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir ElKamouny, *How to Implement Facebook Conversions API (In Shopify)*, FETCH&FUNNEL, https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Mar. 21, 2023).

[5] *What is the Facebook Conversion SPI and How to Use It*, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last visited Mar. 21, 2023). "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 Mar. 21, 2023).

[6] *About Conversions API*, META, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Mar. 21, 2023).

blockers or other denials of consent by the website user that would prevent the Pixel from sending website users' Private Information to Facebook directly.

11. In addition to the Facebook Pixel and CAPI, Defendant installed numerous other tracking technologies responsible for tracking patients' usage of Defendant's Online Platforms and transmitting that information to additional third parties, including Google, LinkedIn, Twitter, CrazyEgg, MonsterInsights, and likely others.

12. Defendant utilized data from these trackers for marketing purposes in an effort to bolster its profits and market its services. The Facebook Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiffs' and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

13. The information that Defendant's Tracking Pixel and CAPI sent to Facebook and other likely third parties included the Private Information that Plaintiffs and Class Members submitted to Defendant's Online Platforms, including for example, the type of medical treatment sought, the individual's particular health condition, from whom the individual sought healthcare treatment, and the fact that the individual attempted to book a medical appointment.

14. Such information allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who geotarget Plaintiffs' and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI. Facebook and any third-party purchasers of Plaintiffs' 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.

15. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patient's consent. Neither Plaintiffs nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook, Google, Microsoft, or any other third-party tracking technology vendor.

16. Despite willfully and intentionally incorporating the Tracking Pixel and other tracking technologies into its Website and servers, Defendant has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook, Google, or other unauthorized third parties. Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook and other third parties as they communicated with their healthcare provider via the Online Platforms, or stored on Defendant's servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.

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

18. Defendant owed common law, statutory, and regulatory duties to keep Plaintiffs' and Class Members' communications and medical information safe, secure, and confidential.

19. Upon information and belief, Defendant utilized the Pixel data to improve and to save costs on its marketing campaigns, improve its data analytics, and attract new patients.

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

21. Defendant breached its statutory and common law obligations to Plaintiffs and Class Members by, *inter alia*: (i) failing to adequately review its marketing programs and web based technology to ensure the Website and Online Platforms were 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 Plaintiffs and Class Members; (iv) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook or others; (v) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Tracking Pixels and other tracking technologies; (vi) failing to warn Plaintiffs and Class Members; and (vii) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

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

THE PARTIES

23. Plaintiff Sherry Childers is a natural person, resident, and a citizen of Indiana. She has no intention of moving to a different state in the immediate future. Plaintiff is a current patient

of Defendant.

24. Plaintiff Diana Polston is a natural person, resident, and a citizen of Indiana. She has no intention of moving to a different state in the immediate future. Plaintiff is a current patient of Defendant.

25. Defendant Hancock is a corporation organized and existing under the laws of the State of Indiana with its principal place of business at 801 North State Street, Greenfield, Indiana 46140.

JURISDICTION AND VENUE

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

27. This Court has personal jurisdiction over Defendant because it was formed within and according to the laws of Indiana and maintains its principal place of business within Greenfield, Indiana, making Defendant at home in Indiana.

28. Venue is preferred in this County pursuant to Indiana Rule of Trial Procedure 75(A)(4) because Defendant maintains its principal office in this County.

COMMON FACTUAL ALLEGATIONS

A. Background

29. Hancock, headquartered in Greenfield, Indiana, offers a full range of medical services within Hancock County and the surrounding area through its network of healthcare facilities and physicians. Hancock's main campus, Hancock Regional Hospital, is "a full-service community hospital" that offers "a state-of-the-art surgery department, 24-hour emergency services, OB services, progressive and critical care, home healthcare, occupational health, a

transitional care unit, a total oncology program with a cutting-edge radiation oncology center, many private rooms, and a full complement of inpatient and outpatient services."[7]

30. Defendant also operates the Hancock Physicians Network, a network of over a hundred primary physicians and specialists practicing across numerous specialties.[8]

31. Defendant promotes the convenience and comprehensive functionality of its Online Platforms and encourages its patients to use its Online Platforms to find healthcare services and providers, access information about specific health conditions, sign up for classes and events, and more.

32. Defendant uses its Website to connect Plaintiffs and Class Members to Defendant's online healthcare platforms with the goal of increasing profitability.

33. In furtherance of that goal, and to increase the success of its advertising and marketing, Defendant purposely installed the Tracking Pixel, Facebook's Conversions API tools, and other tracking technologies on many of the webpages within its Website and on its servers and programmed those webpages and servers. In doing so, Defendant surreptitiously shared patients' private and protected communications with Facebook and other third parties, including communications that contain Plaintiffs' and Class Members' Private Information.

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

[7] *History*, Hancock Health, https://www.hancockregionalhospital.org/about/history/ (last visited July 3, 2023).

[8] *See Find a Doctor*, Hancock Health, https://www.hancockregionalhospital.org/find-a-doctor/ (last visited July 3, 2023).

i. Facebook's Business Tools and the Pixel

35. Facebook operates the world's largest social media company, which generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[9]

36. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify, target, and market products and services to individuals.

37. Facebook's Business Tools, including the 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.

38. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[10] Businesses that want to target customers and advertise their services, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[11]

---

[9] *Meta Reports Fourth Quarter and Full Year 2021 Results*, META INVESTOR RELATIONS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Dec. 2, 2022).

[10] *Specifications for Meta Pixel Standard Events*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Mar. 21, 2023); *see Facebook Pixel, Accurate Event Tracking, Advanced*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/advanced (last visited Mar. 21, 2023); *see also Best Practices for Meta Pixel Setup*, FACEBOOK, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited Mar. 21, 2023); *App Events API*, FACEBOOK, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Mar. 21, 2023).

[11] *About Standard and Custom Website Events*, FACEBOOK, https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (last visited Mar. 21, 2023); *see also App Events API*, *supra* note 10.

39. One such Business Tool is the Pixel that "tracks the people and type of actions they take."[12] When a user accesses a webpage that is hosting the Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook—traveling from the user's browser to Facebook's server.

40. Notably, this transmission only occurs on webpages that contain a Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate privacy (such as the homepage) and disable it on pages that do implicate patient privacy. Thus, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook and other third parties via the Pixel but for Defendant's decisions to install the Pixel on its Website and specifically on webpages that solicit and receive Private Information.

41. Similarly, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook via Conversions API but for Defendant's decisions to install and implement that tool on its servers.

42. By installing and implementing the Tracking Pixel and other tracking technologies, Defendant caused Plaintiffs' and Class Members' communications to be intercepted and transmitted from Plaintiffs' and Class Members' browsers directly to Facebook and other third parties.[13]

43. The Pixel's primary purpose is for marketing, ad targeting, and sales generation.[14]

---

[12] *Retargeting*, *supra* note 3.

[13] Facebook assigns a unique "event_id" parameter to each separate communication with a website and then duplicates the data based on the event_id so that the same event tracked by the Pixel and recorded by the CAPI are not reported as two separate events. *Set Up Conversions API for Server-Side Tagging in Google Tag Manager*, FACEBOOK, https://www.facebook.com/business/help/702509907046774 (last visited Mar. 21, 2023).

[14] *See Meta Pixel*, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last visited June 22, 2023).

44. 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."[15]

45. According to Facebook, the Pixel can collect the following data.

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and person using the website. (emphasis added).
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
>
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[16]

46. Facebook boasts to its prospective users that the 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.[17]

---

[15] *About Meta Pixel*, META, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited June 22, 2023).

[16] *Meta Pixel*, *supra* note 14.

[17] *About Meta Pixel*, *supra* note 15.

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

ii. Defendant's method of transmitting Plaintiffs' and Class Members' Private Information via the Tracking Pixel and/or Conversion API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Pixel

48. 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 a 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).

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

50. 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.

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means

they can store and communicate data when visiting one website to an entirely different website.

- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

51. When an individual visits Defendant's Website, their web browser sends an HTTP Request to Defendant's servers that essentially asks Defendant's Website to retrieve certain information (such as Defendant's "Find a Doctor" page). Defendant'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 Defendant's Website.

52. 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.

53. 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. Defendant's Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When patients visit Defendant's website via an HTTP Request to Defendant's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel. Thus, Defendant is in essence handing patients a tapped phone, and once the Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the

Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook and Google.

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

55. Furthermore, if the patient is also a Facebook user, the information Facebook receives is linked to the patient's Facebook profile (via their FID), which includes other identifying information.

56. Defendant intentionally configured the Tracking Pixels installed on its Website to capture both the "characteristics" of individual patients' communications with the Defendant's Websites (*i.e.,* their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (*i.e.*, the buttons, links, pages, and tabs they click and view).

57. As an example, anyone who visits one of Defendant's websites, such as *https://www.hancockregionalhospital.org/*, and clicks on the "Healthcare Services" tab is presented with a search bar and a list of approximately 34 links to pages with information on specific conditions, treatments, services, and locations, ranging from "Bariatrics & Weight Loss" to "Women's Health." Someone who clicks on the "Cancer Care" button is directed to a page,

https://www.hancockregionalhospital.org/healthcare-services/cancer-care/, which includes buttons and links that provide patients with information about specific conditions, treatment options, services, locations, doctors, appointment scheduling, clinical trials, each with a separate link. Selecting any of these links, like "Radiation Therapy," directs them to a section of the page, *https://www.hancockregionalhospital.org/healthcare-services/cancer-care/#radiation-therapy*, providing more information about radiation therapy.

58. The Facebook Pixel intercepts the "characteristics" and "content" of all these communications with Defendant's Website, and automatically transmits this data to Facebook. Thus, by receiving the contents of these communications, Facebook will know the exact webpages that a specific patient has viewed and buttons clicked on, which relates to the patient's past, present, or future health conditions (*i.e.*, the patient's individually-identifiable patient health information).

59. As another example, when a patient visits the *https://www.hancockregionalhospital.org/* homepage, navigates to the search bar, and types in specific search terms, that information is shared with Facebook through the Pixel in the form of full string URLs. Thus, on information and belief, if a patient types in "Diabetes" into the search bar, when the webpage loads into the patient's browser, the Pixel code is triggered which secretly sends an HTTP Request to Facebook including the patient's FID and the URL, informing Facebook that the user is searching for information on diabetes by transmitting the following URL to Facebook: "https://www.hancockregionalhospital.org/?s=Diabetes."

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

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

61. Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."[18] Thus, Defendant receives and stores communications with patients on its server before Conversions API collects and sends those communications—and the Private Information contained therein—to Facebook.

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

63. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the host server, Facebook instructs companies like Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[19] Thus, it is reasonable to infer that Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

64. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content on the host website. In other words, Facebook and others like it are not providing anything to the user related to the user's communications.

[18] *Prepare Your Business to Use the Conversions API*, FACEBOOK, https://www.facebook.com/business/help/1295064530841207?id=818859032317965 (last visited Mar. 21, 2023).

[19] *Best Practices for Conversions API*, FACEBOOK, https://www.facebook.com/business/help/308855623839366?id=%20818859032317965 (last visited Mar. 21, 2023).

Instead, these third parties are typically procured to track user data and communications only to serve the marketing purposes of the website owner (*i.e.*, to bolster profits).

65. Thus, without any knowledge, authorization, or action by the user, website owners like Defendant can use their source code to commandeer patients' computing devices, causing the devices' web browsers to contemporaneously and invisibly re-direct the patients' communications to hidden third parties like Facebook.

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

67. Consequently, when Plaintiffs and Class Members visited Defendant's website and communicated their Private Information, including but not limited to, medical treatment sought, medical conditions, physician selected, specific button/menu selections, content (such as searches for symptoms or treatment options) typed into free text boxes, demographic information, email addresses, phone numbers, and emergency contact information, it is simultaneously intercepted and transmitted to Facebook and other third parties.

iii. Defendant Violated its own Privacy Policies

68. Defendant's Notice of Privacy Practices provides:

> **Understand your privacy rights.**
>
> Hancock Health takes your privacy seriously. We are required by law to maintain that privacy, and to provide you with this notice of our privacy practices, which explains our duties and practices in regard to your private information. We are required to abide by the terms of this notice, which is currently in effect.
>
> . . .

Hancock Health Notice of Privacy Practices

> This notice describes how medical information about you may be used and disclosed, and how you can get access to this information. Please review it carefully.
>
> **OUR RESPONSIBILITIES**
>
> Hancock Regional Hospital (HRH) takes the privacy of your protected health information ("PHI") seriously. We are required by law to maintain that privacy, to provide you with this Notice of Privacy Practices, and to notify you following a breach of your unsecured PHI. This Notice is provided to tell you about our duties and practices with respect to your PHI. We are required to abide by the terms of this Notice that is currently in effect.[20]

69. Defendant's Notice of Privacy Practices does not permit Defendant to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes without written permission.[21]

70. Specifically, Defendant's Notice of Privacy Practices states:

> **MARKETING**
>
> Most uses and disclosures of PHI for marketing purposes will be made only with your written authorization. We may use PHI to communicate to you about a product or service if the communication occurs face-to-face, involves a gift of nominal value, or is for a drug refill.
> . . .
>
> **SALE OF PHI**
>
> Except in limited circumstances permitted by law, we will not sell your PHI without your written authorization.[22]

71. Defendant's Notice of Privacy Practices makes no mention of Defendant's use of third-party tracking technologies, such as the Facebook Pixel, within its Online Platforms to

---

[20] *Privacy Notice (HIPAA)*, HANCOCK HEALTH (Nov. 7, 2019), https://www.hancockregional hospital.org/patient-information/privacy-notice-hipaa/.

[21] *Id.*

[22] *Id.*

passively and surreptitiously intercept and transmit confidential patient communications and Private Information to unauthorized entities such as Meta (Facebook), Google, and other likely third parties.

72. Defendant violated its own Notice of Privacy Practices by unlawfully disclosing Plaintiffs' and Class Members' Private Information to Meta (Facebook), Google, and likely other third parties. Defendant further misrepresented that it would preserve the privacy and security of Plaintiffs' and Class Members' Private Information.

iv. Warnings about the Pixel's Interception and Transmission of Private Information and Defendant's Implementation of the Pixel

73. In or around June 2022, The Markup, a nonprofit newsroom and media organization focusing on technology and its effects on society, conducted an investigation of the use of tracking tools, such as the Facebook Pixel, on the online platforms of Newsweek's top 100 hospitals in America.[23]

74. The investigation by The Markup revealed that the Facebook Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[24] On those hospital websites, the Facebook Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website by, for example, clicking a button to schedule a doctor's appointment.[25] The data is connected to an IP address, which is "an identifier

[23] Todd Feathers et al, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[24] *Id.*

[25] *Id.*

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."[26]

75. The Markup found that the data the Facebook Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[27]

76. Despite knowing that the Pixel code embedded in its Online Platforms was sending patients' personal health information to Facebook and other third parties, Defendant did nothing to protect its patients from egregious intrusions into its patients' privacy, choosing instead to benefit at those patients' expense.

77. Despite notification of the risks the Pixel poses to the security of patients' Private Information, Defendant has failed to remove the Pixel from its Online Platforms.

78. An example illustrates the point. If a patient visits Defendant's Website and clicks "Cardiovascular Services" under Defendant's "Healthcare Services" tab, the individual's browser sends a request to Defendant's server requesting that it load the webpage. Then, the Pixel sends secret instructions back to the individual's browser, causing it to imperceptibly record the patient's communications with Defendant, such as the page visited or treatment specialty searched, and transmit it to Facebook's servers alongside personally identifying information, such as the patient's IP address. Thus, any Website page a patient visits is then reported back to Facebook, alongside personally identifying information about that patient.

[26] *Id.*

[27] *Id.*

79. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

80. Every time Defendant sends a patient's website activity data to Facebook, that patient's PII is also disclosed, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to the corresponding Facebook profile and the person's real-world identity. A user who accesses Defendant's Online Platforms while logged into Facebook will transmit the user cookie to Facebook, which contains that user's unencrypted Facebook ID.

81. Google, Microsoft, and other companies likewise process this data in a similar manner and use it to connect the information to particular individuals to build marketing and other data profiles.

82. Through the Pixel, Defendant shares its patients' identities and online activity, including personal information and search results related to their private medical treatment. In this way, Defendant unlawfully disclosed Plaintiffs' and Class Members' confidential communications and Private Information to Facebook, Google, and Microsoft, without authorization or proper de-identification, in violation of its own Notice of Privacy Practices.

83. Defendant could have configured its tracking software to limit the information that it communicated to third parties, but it did not and instead intentionally selected the features and functionality of the Pixel that resulted in the Disclosure.

84. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information or assist with intercepting their communications. Plaintiffs were never provided with any written notice that Defendant discloses its patients' protected health information, nor were they provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiffs' protected health information to Meta (Facebook), Google, and other unauthorized entities.

85. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and 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.

86. By law, Plaintiffs are entitled to privacy in their protected health information and confidential communications. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiffs' and Class Members' confidential communications, personally identifiable information, and protected health information; (2) disclosed patients' protected information to Facebook and others—unauthorized third-party eavesdroppers; and (3) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent.

B. Plaintiffs' Experiences

i. Plaintiff Sherry Childers' Experience

87. Plaintiff received healthcare services from one of the hospitals within Defendant's network and relied on Defendant's digital healthcare platforms to communicate confidential patient information. In the course of seeking medical treatment, Plaintiff has used Defendant's Online Platforms to, for example, search for a physician, specific conditions, and treatments.

88. Plaintiff accessed Defendant's digital tools to receive healthcare services from Defendant at Defendant's direction and encouragement. Plaintiff reasonably expected that her online communications with Defendant were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

89. Plaintiff is also a Facebook user and visited Defendant's website and digital platforms while logged in to Facebook.

90. Plaintiff used Defendant's Online Platforms to search for physicians, specific conditions, and treatments and communicate her Private Information to Defendant. Plaintiff trusted that her Private Information would be safeguarded according to Defendant's privacy policies and state and federal law.

91. As described herein, by use of the Pixel and other tracking technologies, Defendant sent Plaintiff's Private Information to Meta (Facebook), Google, and others when she used Defendant's digital platforms to communicate healthcare and identifying information to Defendant.

92. Pursuant to the process described herein, Defendant assisted Meta (Facebook), Google, and others with intercepting Plaintiff's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Defendant facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

93. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff's personally identifiable information and protected health information.

94. Since Plaintiff began using Defendant's digital healthcare platforms, Plaintiff has received targeted medical advertising related to her medical treatment on social media and via spam calls.

ii. Plaintiff Diana Polston's Experience

95. Plaintiff received healthcare services from one of the hospitals within Defendant's network and relied on Defendant's digital healthcare platforms to communicate confidential patient information. In the course of seeking medical treatment, Plaintiff has used Defendant's Online Platforms to, for example, search for a physician.

96. Plaintiff accessed Defendant's digital tools to receive healthcare services from Defendant at Defendant's direction and encouragement. Plaintiff reasonably expected that her online communications with Defendant were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

97. Plaintiff is also a Facebook user and visited Defendant's website and digital platforms while logged in to Facebook.

98. Plaintiff used Defendant's Online Platforms to search for physicians and communicate her Private Information to Defendant. Plaintiff trusted that her Private Information would be safeguarded according to Defendant's privacy policies and state and federal law.

99. As described herein, by use of the Pixel and other tracking technologies, Defendant sent Plaintiff's Private Information to Meta (Facebook), Google, and others when she used Defendant's digital platforms to communicate healthcare and identifying information to Defendant.

100. Pursuant to the process described herein, Defendant assisted Meta (Facebook), Google, and others with intercepting Plaintiff's communications, including those that contained

personally identifiable information, protected health information, and related confidential information. Defendant facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

101. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff's personally identifiable information and protected health information.

102. Since Plaintiff began using Defendant's digital healthcare platforms, Plaintiff has received targeted medical advertising related to her medical treatment on social media.

C. Defendant Violated HIPAA Standards

103. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[28]

104. Guidance from the United States Department of Health and Human Services ("HHS") instructs healthcare providers that patient status alone is protected by HIPAA.

105. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[29]

[28] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 165.508(a), 164.514(b)(2)(i).

[29] *The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

106. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."[30]

107. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."[31]

108. Under the HIPPA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination;" or (2)(i) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed: (A) Names; . . . (H) Medical record numbers; . . . (J) Account numbers; . . . (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; . . . and (R) [a]ny other unique identifying number, characteristic, or code . . . ; and (ii) [t]he covered entity must not have actual knowledge that the information could be used

[30] 45 C.F.R. § 160.103.

[31] *Id.*

alone or in combination with other information to identify an individual who is a subject of the information."[32]

109. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization.[33]

110. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."[34] The statute states that a "person . . . shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization."[35]

111. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

112. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties.[36] There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use

[32] 45 C.F.R. § 160.514.

[33] *Id.* §§ 160.103, 164.502.

[34] 42 U.S.C. § 1320d-6.

[35] *Id.*

[36] *Id.*

individually identifiable health information for commercial advantage, personal gain, or malicious harm."[37] In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both."[38]

113. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, HHS 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.[39]

114. In its guidance for Marketing, HHS 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 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.[40]

---

[37] *Id.*

[38] *Id.*

[39] OFFICE OF CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION (2012), available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[40] OFFICE OF CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., MARKETING (2003), available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

115. HHS has repeatedly instructed for years that patient status is protected by the HIPAA Privacy Rule:

a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA.[41]

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list.[42]

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers."[43]

116. In addition, the Office for Civil Rights (OCR) at HHS has issued a Bulletin (the "HHS 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 technologies.[44]

117. The HHS Bulletin expressly provides,

> Tracking technologies are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications ("apps"). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity's health care operations. The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). 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[45] of PHI to tracking technology vendors or any other violations of**

[41] 65 Fed. Reg. 82717 (Dec. 28, 2000).

[42] 67 Fed. Reg. 53186 (Aug. 14, 2002).

[43] 78 Fed. Reg. 5642 (Jan. 25, 2013).

[44] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Mar. 21, 2023).

[45] *See id.* at n.8 ("Regulated entities can use or disclose PHI, without an individual's written authorization, only as expressly permitted or required by the HIPAA Privacy Rule. *See* 45 CFR 164.502(a).").

> **the HIPAA Rules. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.[46]**

118. Tracking technology vendors like Facebook and Google are considered business associates under HIPAA where, as here, they provide services to Defendant and receive and maintain PHI.

> Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (*e.g.* health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.[47]

119. The HHS Bulletin explained that, through tracking technologies such as the Facebook Pixel, covered entities disclose individual's information, including PHI, provided when individuals use the entity's website or mobile applications, such as medical records numbers, addresses, appointment dates, person's IP addresses or location, medical device IDs or unique identifying codes.[48]

120. The Bulletin further explained that "[a]ll such IIHI [individually identifiable health information] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI,

---

[46] *Id.* (citations omitted) (emphasis added) (citing 45 C.F.R. § 164.508(a)(3); 45 C.F.R. § 164.501 (defining "Marketing")).

[47] *Id.*

[48] *Id.*

such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services."[49] This is because that information "connects the individual to the regulated entity . . . and thus relates to the individual's past, present, or future health or health care or payment for care."[50]

121. HIPAA applies to Defendant's webpages with tracking technologies even outside the patient portal:

> Tracking on unauthenticated webpages
>
> [T]racking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal **… [and pages] that address[] specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances**. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.[51]

122. Ultimately, in the Bulletin, HHS made clear that covered entities, such as Defendant, must comply with HIPAA rules in connection with tracking technologies such as the Facebook Pixel, including but not limited to:[52]

---

[49] *Id.*

[50] *Id.*

[51] *Id.* (emphasis added).

[52] *Id.*

- Ensuring that all disclosures of PHI to tracking technology vendors are specifically permitted by the Privacy Rule and that, unless an exception applies, only the minimum necessary PHI to achieve the intended purpose is disclosed.[33]

  - Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use.[34] However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.[35]

- If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individuals' HIPAA-compliant authorizations are required **before** the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do **not** constitute a valid HIPAA authorization.

- Further, it is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.

123. As articulated in the HHS Bulletin, covered entities utilizing tracking technologies must also implement "administrative, physical, and technical safeguards" to protect transmitted PHI, such as appropriate encryption, authentication, and audit controls; and must notify affected individuals and others of any impressible disclosure of PHI to tracking technology vendors who compromise that PHI. "In such instances, there is a presumption that there has been a breach of unsecured PHI unless the regulated entity can demonstrate that there is a low probability that the PHI has been compromised."[53]

[53] *Id.*

124. The HHS Bulletin further noted that the impermissible disclosure of PHI can cause myriad harm to individuals, including "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" and discloses highly-sensitive information regarding patients' diagnoses, and the nature, frequency and location of treatment.[54]

125. The Bulletin is not a pronouncement of new law, but instead reminded covered entities and business associates of their longstanding obligations under existing guidance. The HHS Bulletin cautioned that, "[w]hile 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."[55]

126. In other words, HHS has expressly stated that Defendant has violated HIPAA Rules by implementing the Tracking Pixel.

D. Defendant Violated Industry Standards

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

128. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

129. 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).

[54] *Id.*

[55] *Id.*

130. 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) [f]ully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity) about the purpose(s) for which access would be granted.

131. AMA Code of Medical Ethics Opinion 3.2.2 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: . . . (c) release patient information only in keeping ethics guidelines for confidentiality.

E. Plaintiffs' and Class Members' Expectation of Privacy

132. Plaintiffs and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

133. Indeed, at all times when Plaintiffs and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

F. IP Addresses Are Personally Identifiable Information

134. On information and belief, through the use of the Pixel on Defendant's Website, Defendant also disclosed and otherwise assisted Facebook and other third parties with intercepting Plaintiffs' and Class Members' Computer IP addresses.

135. An IP address is a number that identifies the address of a devise connected to the Internet.

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

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

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

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

140. Under HIPAA, an IP address is considered personally identifiable information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses.[56]
- 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."[57]

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

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

142. The sole purpose of the use of the Facebook Pixel on Defendant's Website was marketing and profits.

[56] *See* 45 C.F.R. § 164.514(2).

[57] 45 C.F.R. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

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

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

145. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

H. Plaintiffs' and Class Members' Private Information Had Financial Value

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

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

148. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it describes the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[58]

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

149. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[59]

CLASS ACTION ALLEGATIONS

150. Pursuant to Indiana Rule of Trial Procedure 23, Plaintiffs bring this statewide class action on behalf of themselves and on behalf of other similarly situated persons.

151. The statewide Class that Plaintiffs seek to represent is defined as follows:

> All Indiana citizens whose Private Information was disclosed to a third party without authorization or consent through the Pixel and related technologies on Defendant's Online Platforms ("the Class").

152. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, 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, was well as their immediate family members.

153. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

154. **Numerosity, Ind. R. Trial P. 23(a)(1):** The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, there are hundreds or thousands of

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

individuals whose Private Information may have been improperly accessed in the Disclosure, and each Class Member is apparently identifiable within Defendant's records.

155. **Commonality, Ind. R. Trial P. 23(a)(2):** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include, without limitation:

a. Whether and to what extent Defendant had a duty to protect Plaintiffs' and Class Members' Private Information;

b. Whether Defendant had duties not to disclose the Plaintiffs' and Class Members' Private Information to unauthorized third parties;

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

d. Whether Defendant had duties not to use Plaintiffs' and Class Members' Private Information for unauthorized purposes;

e. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' Private Information;

f. Whether and when Defendant actually learned of the Disclosure;

g. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

i. Whether Defendant failed to properly implement and configure the tracking software on its digital platforms to prevent the disclosure of information compromised in the Disclosure;

j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Disclosure to occur; and

k. Whether Defendant engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiffs' and Class Members' Private Information.

156. **Typicality, Ind. R. Trial P. 23(a)(3):** Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Disclosure, due to Defendant's use and incorporation of the tracking software.

157. **Adequacy of Representation, Ind. R. Trial P. 23(a)(4):** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class, and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

158. **Policies Generally Applicable to the Class, Ind. R. Trial P. 23(b)(2):** 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 Plaintiffs' 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 Plaintiffs.

159. **Predominance, Ind. R. Trial P. 23(b)(3):** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored within the same computer system and unlawfully disclosed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

160. **Superiority and Manageability, Ind. R. Trial. P. 23(b)(1) and (b)(3):** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to 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 or 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.

161. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm

the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonable consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs 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; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

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

165. Furthermore, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

166. 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 Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, 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 Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Disclosure;

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

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

CAUSES OF ACTION

COUNT I
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

167. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

168. Plaintiffs' and Class Members' communications with Defendant constitute private conversations, communications, and information.

169. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Online Platforms.

170. Plaintiffs and Class Members communicated sensitive PHI and PII that they intended for only Defendant to receive and that they understood Defendant would keep private.

171. Plaintiffs and Class Members have a reasonable expectation that Defendant would not disclose PII, PHI, and confidential communications to third parties without Plaintiffs' or Class Members' authorization, consent, or knowledge.

172. Plaintiffs and Class Members had a reasonable expectation of privacy given Defendant's representations, Notice of Privacy Practices, and HIPAA. Moreover, Plaintiffs and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

173. Defendant allowed the public disclosure of Plaintiffs' and Class Members' Private Information to Meta (Facebook), Google, and likely other third parties by allowing the Tracking Pixel and other tracking technologies to be used on its Online Platforms.

174. Defendant's actions gave publicity to the Private Information of Plaintiffs and Class Members.

175. Defendant's disclosure of PHI coupled with PII and the loss of privacy and confidentiality of Plaintiffs' and Class Members' Private Information is highly offensive to the reasonable person.

176. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion.

177. Plaintiffs and Class Members did not authorize, consent, know about, or take any action to indicate consent to Defendant's conduct alleged herein.

178. There is no legitimate public concern with respect to the Private Information of Plaintiffs and Class Members.

179. As a result of Defendant's public disclosure of Plaintiffs' and Class Members' Private Information, Plaintiffs and Class Members have been needlessly harmed by having their private and confidential medical information disseminated for profit by Defendant, Meta (Facebook), Google, and likely other third parties.

180. Plaintiffs 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.

181. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

182. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs

and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

COUNT II
Negligence
(On Behalf of Plaintiffs and the Class)

183. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

184. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Personal and Medical Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, misused, and disclosed to unauthorized parties.

185. As a provider of health care under the law, Defendant had a special relationship with Plaintiffs and Class Members who entrusted Defendant to adequately protect their Personal and Medical Information.

186. Defendant knew that the Personal and Medical Information at issue was private and confidential and should be protected as private and confidential, and thus, Defendant owed a duty of care not to subject Plaintiffs and Class Members to an unreasonable risk of unauthorized disclosure.

187. Defendant knew, or should have known, of the risks inherent in collecting and storing Personal and Medical Information and allowing it to be accessed by unauthorized third parties.

188. Defendant's failure to take proper security measures to protect Plaintiffs' and Class Members' Personal and Medical Information created conditions conducive to a foreseeable risk of unauthorized access and disclosure of Personal and Medical Information to unauthorized third

parties. As described above, Plaintiffs and Class Members are part of a foreseeable, discernable group that was at high risk of having their Personal and Medical Information compromised, and otherwise wrongly disclosed if not adequately protected by Defendant.

189. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Personal and Medical Information.

190. Defendant owed a duty to timely and adequately inform Plaintiffs and Class Members, in the event of their Personal and Medical Information being improperly disclosed to unauthorized third parties.

191. Defendant systematically failed to provide adequate security for data in its possession or over which it had supervision and control.

192. Defendant, through its actions and omissions, unlawfully breached duties to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Personal and Medical Information within Defendant's possession, supervision, and control.

193. Defendant, through its actions and omissions, unlawfully breached duties owed to Plaintiffs and Class Members by failing to have appropriate procedures in place to prevent dissemination of Plaintiffs' and Class Members' Personal and Medical Information.

194. Defendant, through its actions and omissions, unlawfully breached duties to timely and fully disclose to Plaintiffs and Class Members that the Personal and Medical Information within Defendant's possession, supervision, and control was improperly accessed by unauthorized third parties, the nature of this access, and precisely the type of information improperly accessed.

195. Defendant's breach of duties owed to Plaintiffs and Class Members proximately caused Plaintiffs' and Class Members' Personal and Medical Information to be compromised by being accessed by unauthorized third parties.

196. As a result, of Defendant's ongoing failure to adequately notify Plaintiffs and Class Members regarding what type of Personal and Medical Information has been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages.

197. As a proximate result of Defendant's negligence and breach of duties as set forth above, Defendant's breaches of duty caused Plaintiffs 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 Personal and Medical Information, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their Personal and Medical Information, all of which can constitute actionable actual damages.

198. In failing to secure Plaintiffs' and Class Members' Personal and Medical Information, 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 themselves and the Class.

199. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' Personal and Medical Information, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiffs 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.

COUNT III
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

200. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

201. Plaintiffs allege this negligence *per se* theory as alternative to their other negligence claims.

202. 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 Plaintiffs' and Class Members' Personal and Medical Information.

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

204. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Personal and Medical Information.

205. Defendant owed a duty to timely and adequately inform Plaintiffs and Class Members, in the event of their Personal and Medical Information being improperly disclosed to unauthorized third parties.

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

207. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' Personal and Medical Information and not complying with applicable industry standards as described in detail herein.

208. Plaintiffs' and Class Member's Personal and Medical Information constitute personal property that was taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury and damages to Plaintiffs and Class Members.

209. As a proximate result of Defendant's negligence and breach of duties as set forth above, Defendant's breaches of duty caused Plaintiffs 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 Personal and Medical Information, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their Personal and Medical Information, all of which can constitute actionable actual damages.

210. In failing to secure Plaintiffs' and Class Members' Personal and Medical Information, 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 themselves and the Class.

211. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' Personal and Medical Information, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiffs 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 IV
Breach of Implied Contract
(On Behalf of the Plaintiffs and the Class)

212. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

213. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Information through Defendant's Online Platforms as part of its regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

214. Defendant required Plaintiffs and Class Members to provide their Private Information, including full names, email addresses, phone numbers, computer IP addresses, appointment information, medical insurance information, medical provider information, medical histories, and other content submitted on Defendant's Website as a condition of their receiving healthcare services.

215. As a condition of utilizing Defendant's Online Platforms and receiving services from Defendant, Plaintiffs and Class Members provided their Private Information and compensation for their medical care. In so doing, Plaintiffs and Class Members entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information,

in its Privacy Practices and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

216. Implicit in the agreement between Defendant and its patients was the obligation that both parties would maintain the Private Information confidentially and securely.

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

218. Defendant had an implied duty to protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses.

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

220. Plaintiffs and Class members reasonable believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

221. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant. Defendant did not. Plaintiffs and Class Members would not have provided their confidential Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information for uses other than medical treatment, billing, and benefits from Defendant.

222. Consumers of medical services value their privacy and the ability to keep confidential their Private Information associated with obtaining such services. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant and entered into these

implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, nor would Plaintiffs and Class Members have entrusted their Private Information to Defendant in the absence of Defendant's implied promise to monitor the Online Platforms, computer systems, and networks to ensure that reasonable data security measures were adopted and maintained.

223. Defendant breached the implied contracts with Plaintiffs and Class Members by disclosing Plaintiffs' and Class Members' Private Information to unauthorized third parties, failing to properly safeguard and protect Plaintiffs' and Class Members' Private Information; and violating industry standards as well as legal obligations that are necessarily incorporated into implied contract between Plaintiffs, Class Members, and Defendant.

224. The Disclosure was a reasonably foreseeable consequence of Defendant's actions in breach of the implied contracts.

225. Defendant's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiffs and Class Members to provide their Personal Information in exchange for medical treatment and benefits.

226. As a result of Defendant's failure to fulfill the data security protections promised in these implied contracts, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value.

227. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and Class Members have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities, the loss of control of their Private Information, disruption of their medical care and treatment, and the loss of the benefit of the bargain they had struck with Defendant.

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

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

229. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

230. This claim is pleaded solely in the alternative to Plaintiffs' breach of implied contract claims.

231. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiffs 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 Class Members conferred a benefit on Defendant in the form of monetary compensation.

232. Plaintiffs and Class Members would not have used Defendant's services or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to third parties.

233. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

234. As a result of Defendant's conduct, Plaintiffs 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 Plaintiffs and Class Members

paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

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

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

COUNT VI
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

237. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

238. A relationship existed between Plaintiffs and the Class Members on the one hand and Defendant on the other in which Plaintiffs and the Class Members put their trust in Defendant to protect the Private Information of Plaintiffs and the Class Members, and Defendant accepted that trust.

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

240. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiffs and the Class Members.

241. But for Defendant's breach of fiduciary duty, the damage to Plaintiffs and the Class Members would not have occurred.

242. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiffs and the Class Members.

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

COUNT VII
Violation of the Indiana Deceptive Consumer Sales Act
(On Behalf of Plaintiffs and the Class)

244. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

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

> (A) simplify, clarify, and modernize the law governing deceptive and unconscionable consumer sales practices;
>
> (B) protect consumers from suppliers who commit deceptive and unconscionable consumer sales practices; and
>
> (C) encourage the development of fair consumer sales practice.[60]

246. The General Assembly has instructed courts to construe the DCSA liberally to promote these purposes and policies.[61]

247. Defendant is a "supplier" as defined in the DCSA because it is a seller or other person who regularly engages in or solicits consumer transactions, which are defined to include

[60] IND. CODE § 24-5-0.5-1(b).

[61] *Id.* § 24-5-0.5-1(a).

sales of personal property, *services*, and intangibles that are primarily for a personal, familial, or household purpose, such as those at issue in this action.[62]

248. The DCSA provides that "[a] supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Such an act, omission, or practice by a supplier is a violation of [the DCSA] whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations."[63]

249. An "incurable deceptive act" is a "deceptive act done by a supplier as part of a scheme, artifice, or device with the intent to defraud or mislead."[64]

250. The DCSA further provides:

> Without limiting the scope of subsection (a) the following acts, and the following representations as to the subject matter of a consumer transaction, made orally, in writing, or by electronic communication, by a supplier, are deceptive acts:
>
> (A) That such subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have.
>
> (B) That such subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not. . . .[65]

251. Defendant committed deceptive acts, including but not limited to:

a. Encouraging patients to use Defendant's Online Platform while representing to patients that Defendant is committed to protecting the

[62] *Id.* § 24-5-0.5-2(1), (3) (emphasis added).

[63] *Id.* § 24-5-0.5-3(a).

[64] *Id.* § 24-5-0.5-2(a)(8).

[65] *Id.* § 24-5-0.5-3.

privacy and confidentiality of the Private Information patients provide. Defendant also promised patients that it will never sell their medical information without patients' written authorization.

b. Despite these representations, Defendant disclosed information relating to Plaintiffs' and Class Members' medical treatment to third parties without their knowledge, consent or authorization as part of a scheme, artifice or device with the intent to mislead patients.

c. Plaintiffs and Class Members relied on Defendant's representations in using its Online Platform and thought they were communicating only with their trusted healthcare provider.

d. By installing and implementing Facebook's Pixel, Conversion API tools, and other tracking technologies, Defendant knew or reasonably should have known it intercepted and transmitted Plaintiffs' and Class Member's communications from Plaintiffs' and Class Members' browsers directly to Facebook and other third parties, or recorded on Defendant's servers and then transferred to Facebook via Conversions API.

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

253. The DCSA provides that "[a] person relying upon an uncured or incurable deceptive act may bring an action for the damages actually suffered as a consumer as a result of the deceptive act or five hundred dollars ($500), whichever is greater. The court may increase damages for a willful deceptive act in an amount that does not exceed the greater of: (i) three (3)

times the actual damages of the consumer suffering the loss; or (ii) one thousand dollars ($1,000).”[66]

254. The DCSA provides that “[a]ny person who is entitled to bring an action under subsection (a) on the person’s own behalf against a supplier for damages for a deceptive act may bring a class action against such supplier on behalf of any class of persons of which that person is a member . . . .”[67]

255. Had Plaintiffs and Class Members been aware that their Private Information would be transmitted to unauthorized third-parties, Plaintiffs and Class Members would not have entered into such transactions and would not have provided payment or confidential medical information to Defendant.

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

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

COUNT VIII
Violation of the Indiana Wiretapping Act
(On Behalf of Plaintiffs and the Class)

258. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

[66] *Id.* § 24-5-0.5-4(a).

[67] *Id.* § 24-5-0.5-4(b).

259. The Indiana Wiretapping Act (the "IWA") states that "a person who knowingly or intentionally intercepts a communication in violation of this article commits unlawful interception, a Level 5 felony."[68] The term "includes the intentional recording or acquisition of communication through the use of a computer[.]"[69]

260. For purposes of the IWA, "interception" is the "intentional recording or acquisition of the contents of an electronic communication by a person other than a sender or receiver of that communication, without the consent of the sender or receiver, by means of any instrument, device, or equipment under this article."[70]

261. Defendant intentionally recorded and/or acquired Plaintiffs' and Class Members' electronic communications, without the consent of the Plaintiffs and Class Members, using the Facebook Pixel and other tracking technologies.

262. Defendant intentionally recorded and/or acquired Plaintiffs' and Class Members' electronic communications for the purpose of disclosing those communications to third parties, including Facebook, without the knowledge, consent, or written authorization of Plaintiffs or Class Members.

263. Under the IWA, "[a] person whose communications are intercepted, disclosed, or used in violation of this article . . . has a civil cause of action against a person who intercepts, discloses, uses, or procures another person to intercept, disclose, or use a communication," and is entitled to recover from that person:

(A) The greater of:

---

[68] *Id.* § 35-33.5-5-5.

[69] *Id.*

[70] *Id.* § 35-31.5-2-176.

i. Actual damages;

ii. Liquidated damages computed at a rate of one hundred dollars ($100) each day for each day of violation; or

iii. One thousand dollars ($1,000).

(B) Court costs (including fees).

(C) Punitive damages, when determined to be appropriate by the court.

(D) Reasonable attorney's fees.[71]

264. Defendant is a "person" under the IWA.[72]

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

a. Plaintiffs' and Class Members' personal computing devices;

b. Plaintiffs' and Class Members' web browsers;

c. Plaintiffs' and Class Members browser-managed files;

d. Facebook's Pixel;

e. Internet cookies;

f. Defendant's computer servers;

g. Third-party source code utilized by Defendant; and

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

266. Defendant aided in the interception of communications between Plaintiffs and Class Members and Defendant that were redirected to and recorded by third parties without Plaintiffs' or Class Members' consent.

[71] *Id.* § 35-33.5-5-4.

[72] *Id.* § 35-31.5-2-234.

267. Under the IWA, Plaintiffs and the Class Members are entitled to recover actual damages, but not less than liquidated damages at a rate of $100 a day for each day of the violation or one thousand dollars ($1,000), whichever is greater, punitive damages, reasonable attorney's fees, and court costs.

268. In addition to statutory damages, Defendant's breach caused Plaintiffs and Class Members the following damages:

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;

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

c. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value;

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

e. Defendant's actions diminished the value of Plaintiffs' and Class Members' personal information.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Disclosure;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages under the IWA, as allowable by law;

h) For an award of attorneys' fees and costs under the IWA, DCSA, the common fund doctrine, and any other applicable law;

i) Costs and any other expense, including expert witness fees incurred by Plaintiffs 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 TRIAL DEMANDED

Plaintiffs, pursuant to Indiana Trial Rule 38(B), hereby demand a trial by jury on all issues so triable.

Dated: August 9, 2023

Respectfully Submitted,

/s/ Tyler B. Ewigleben
Tyler B. Ewigleben
Christopher D. Jennings*
Winston Hudson*
Laura Edmondson*
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, AR 72201
Tel: (501) 372-1300
chris@yourattorney.com
tyler@yourattorney.com
winston@yourattorney.com
ledmondson@yourattorney.com

*To be admitted *pro hac vice*
Counsel for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on August 9, 2023, a copy of the foregoing was filed electronically. Notice of this filing was served on the following counsel by operation of the Indiana electronic filing system and/or via email:

Tyler J. Moorhead
Philip R. Zimmerly
BOSE McKINNEY & EVANS LLP
111 Monument Circle, Suite 2700
Indianapolis, IN 46204
tmoorhead@boselaw.com
pzimmerly@boselaw.com

Attorneys for Defendant, Board of Trustees of the Hancock Regional Hospital

/s/ Tyler B. Ewigleben
Tyler B. Ewigleben