Terence R. Coates (0085579)
Dylan J. Gould (0097954)
Joseph M. Lyon (0076050)
Kevin M. Cox (0099584)
Jeffrey S. Goldenberg (0063771)
Counsel for Plaintiffs

[Additional counsel listed on signature page]

IN THE COURT OF COMMON PLEAS
HAMILTON COUNTY, OHIO

IN RE THE CHRIST HOSPITAL PIXEL LITIGATION	**Case No. A 2204749** **Judge Christian A. Jenkins** **CONSOLIDATED CLASS ACTION COMPLAINT** **(Jury Trial Demanded)**

Plaintiffs A.T, G.W, and W.B. (collectively "Plaintiffs"),[1] at all times relevant herein, have been patients of The Christ Hospital ("Christ Hospital" or "Defendant"), and bring this class action individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions, their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this case to address Defendant's unlawful practice of disclosing Plaintiffs' and Class Members' confidential personally identifiable information ("PII") and

[1] On January 4, 2023, Plaintiff A.T. filed a motion for leave to proceed under a pseudonym in public filings so as not to compound the loss of privacy already suffered. This motion remains pending. However, Plaintiffs intend to file an amended motion on behalf of all Plaintiffs shortly.

protected health information ("PHI") (collectively referred to as "Private Information") to third parties, including Meta Platforms, Inc. ("Facebook" or "Meta") and Google LLC ("Google"), without consent, via tracking software Defendant installed on www.thechristhospital.com (the "Website" it owns and controls) and its MyChart Patient Portal (collectively referred to as Defendant's "Web Properties").

2. Defendant encourages its patients, and it encouraged the Plaintiffs, to use the Web Properties for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, signing up for events and classes, obtaining forms related to their medical care, finding payment information, accessing the Patient Portal, and more.

3. Defendant also encourages its patients, and it encouraged the Plaintiffs, to register for and use the Patient Portal to book appointments, review their health records and test results, pay bills, communicate with service providers, request prescription refills, and complete medical forms virtually and remotely, and more.

4. Plaintiffs used Defendant's Web Properties for the purposes stated above in relation to the medical care they each sought, scheduled, and ultimately obtained from Defendant and communicated their Private Information via the Web Properties to obtain necessary medical services.

5. Defendant both expressly and impliedly promised to maintain the privacy and confidentiality of the Private Information that patients—including Plaintiffs—submitted, communicated, and exchange with Defendant via its Web Properties.

6. Despite this, Defendant installed tracking technologies ("Tracking Tools") onto its Web Properties and, upon information and belief, the Patient Portal.[2] These Tracking Tools, such as pixels, web beacons, or cookies, track and collect communications with the Defendant via the Web Properties and surreptitiously force the user's web browser to send those communications to undisclosed third parties, such as Facebook or Google.[3]

7. Plaintiffs and Class Members used the Web Properties to submit information related to their past, present, or future health conditions, including, for example, searches for specific health conditions and treatment and the booking of medical appointments with specific physician. Such Private Information would allow the third party (e.g., Facebook or Google) to know that a specific patient was seeking confidential medical care from Defendant, as well as the type of medical care being sought. This disclosure would also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, or addiction.

8. Facebook connects user data from Defendant's Web Properties to the individual's Facebook ID ("FID"). The FID is a unique identifier that links the user to his/her Facebook profile, which contains detailed information about the profile owner's identity.

---

[2] The MyChart Patient Portal is hosted by a third party, Epic Software Systems (Epic), which permits its partners to deploy "custom analytics scripts." Thus, healthcare providers can deploy tracking technologies by embedding them into the code. The means that impermissible tracking can occur on the login page and password-protected webpages within the portal. Plaintiffs have included images demonstrating the Facebook Pixel was embedded on the portal, and those images were taken from their personal Facebook accounts after using the portal. Upon information and belief, Plaintiffs aver that tracking technologies, including the Facebook Pixel, were deployed on the login page and within Defendant's MyChartPortal. This allegation is reasonable in light of Defendant's pervasive use of tracking technologies that improperly disseminate PHI and PII.

[3] Limited discovery obtained during the parties' previous dispute over CAFA jurisdiction indicates that at least 596,037 Christ Hospital patients have accessed both the Website *and* the Patient Portal during the relevant time period. *Doe v. Christ Hosp.*, No. 1:23-CV-27, 2023 WL 4757598, at *4 (S.D. Ohio July 26, 2023).

9. Like Facebook, Google can identify specific individuals and connect their Private Information for use in marketing via the Google Analytics tool, and this occurs even when the person is not using Google's Chrome browser or a Google device. That's because, like Facebook, Google tracks and records individuals and their devices anytime they've used the device to access their Google email account ("Gmail"), YouTube, and nearly a dozen other platforms it owns and controls, associating their PHI with other information even if they are not using its web browser.

10. Simply put, the health information disclosed through the tracking technologies is personally identifiable.

11. Defendant is a healthcare entity and thus its disclosure of health and medical communications is tightly regulated. 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 health care providers must safeguard and protect Private Information. Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

12. In addition, as explained further below, HHS has specifically warned healthcare regulated entities that tracking technologies like those used by Defendant transmit personally identifying information to third parties, both on the public portion of the website and within the password-protection patient portal, and that such information should not be transmitted without a HIPAA-acceptable written authorization from patients.

13. The Federal Trade Commission ("FTC") has also warned hospitals and other entities that "even if you are not covered by HIPAA, you still have an obligation to protect against

impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule."

14. Additionally, state statutes, such as R.C. 3798.04, prohibit the unlawful interception and/or disclosure of the Plaintiffs' protected medical information.

15. Despite these warnings, Defendant embedded hidden Tracking Tools on its Web Properties, essentially planting a bug on patients' web browsers that forced them disclose private and confidential communications to third parties. Defendant did not disclose the presence of these Tracking Tools to its patients.

16. Healthcare patients simply do not anticipate or expect 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 patients' consent. Neither Plaintiffs nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook or Google.

17. Defendant breached its statutory and common law obligations to Plaintiffs and Class Members by, inter alia: (i) intentionally installing the Tracking Tools on the Web Properties for the purpose of sharing Plaintiffs' and Class Members' Private Information with unauthorized third parties; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Tracking Tools like the Facebook Pixel or Google Analytics; (v) failing to warn Plaintiffs and Class Members; and (vi)

otherwise failing to design, and monitor its Web Properties to maintain the confidentiality and integrity of patient Private Information.

18. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) interference with a confidential relationship; (iii) lost benefit of bargain, (iv) diminution in value of Private Information, and (v) the continued and ongoing risk to their Private Information.

19. Plaintiffs seek to remedy these harms and brings causes of action for (1) breach of confidence (*Biddle*); (2) invasion of privacy; (3) breach of implied contract; (4) unjust enrichment; (5) negligence; (6) breach of fiduciary duty; and (7) violations of the Ohio Wiretapping law, R.C. 2933.52, *et seq.*; (8) and violations of the Ohio Consumer Sales Practices Act, R.C. 1345.01, *et seq.*

PARTIES

20. Plaintiffs A.T., G.W., and W.B., are natural persons and citizens of Ohio where they intend to remain.

21. Defendant The Christ Hospital is a 501(c)(3) non-profit corporation incorporated in the State of Ohio. Defendant is headquartered at 2139 Auburn Avenue, Cincinnati, Ohio 45219.

22. Defendant operates a health care network comprising two medical centers, 1,200 physicians, and 6,500 employees, across more than 100 locations in the greater Cincinnati area.[4] Defendant is a covered entity under HIPAA (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164).

[4] https://www.thechristhospital.com/about-the-network (last visited: October 4, 2023).

JURISDICTION & VENUE

23. This Court has subject matter jurisdiction over this action under R.C. 2305.01 and R.C. 1345.04.

24. This Court has personal jurisdiction over Defendant because it's headquartered in Cincinnati, Ohio, and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this state.

25. Venue is proper in Hamilton County under Civ.R. 3(C)(2) because Defendant's principal place of business is in this county.

COMMON FACTUAL ALLEGATIONS

The U.S. Department of Health and Human Services and Federal Trade Commission Have Warned about Use of Tracking Tools by Healthcare Providers

26. In December 2022, HHS issued a bulletin (the "HHS Bulletin") warning regulated entities like Defendant about the risks presented using Tracking Tools on their websites:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. **For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.**[5]

27. In other words, HHS has expressly stated that entities like Defendant that implement the Facebook Pixel and Google Analytics and disclose patient information have violated HIPAA Rules unless those entities obtain a HIPAA-complaint authorization, which requires Affirmative Express Consent.

---

[5] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited October 5, 2023) (emphasis added).

28. "Affirmative Express Consent" means any freely given, specific, informed, and unambiguous indication of an individual's wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the individual, apart from any "privacy policy," "terms of service," "terms of use," or other similar document, of all information material to the provision of consent. *See U.S. v. Easy Healthcare Corp. d/b/a Easy Healthcare*, No. 1:23-cv-310 (N.D. Ill. June 22, 2023) (Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief).[6]

29. The HHS Bulletin further warns that:

> While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, **because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.** [7]

30. Additionally, HHS has warned healthcare providers that Protected Information is not limited exclusively to patient portals like MyChart, and thus Defendant still has an obligation to protect information on non-password protected (i.e., "unauthenticated") webpages :

> Tracking technologies on a regulated entity's unauthenticated webpage that addresses 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.**[8]

[6]https://www.ftc.gov/system/files/ftc_gov/pdf/2023.06.22_easy_healthcare_signed_order_2023.pdf (last visited Oct. 12, 2022).

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

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

31. In addition, HHS and the FTC have recently issued a letter, once again admonishing entities like Defendant to stop using Tracking Tools:

> If you are a covered entity or business associate ("regulated entities") under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium. **The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI. . .** Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. . . As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app. The disclosure of such information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule.[9]

The Underlying Web Technology

32. To understand Defendant's unlawful data-sharing practices, it is important first to understand basic web design and tracking tools.

33. Devices (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

34. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

35. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

[9] *Re: Use of Online Tracking Technologies*, U.S. Dept. of Health & Hum. Servs. and Fed. Trade. Comm'n (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

- **Universal Resource Locator ("URL")**: a web address.
- **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, 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.[10]

36. 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. Source code is essentially the back of the website, and the user does not see what happens in the source code.

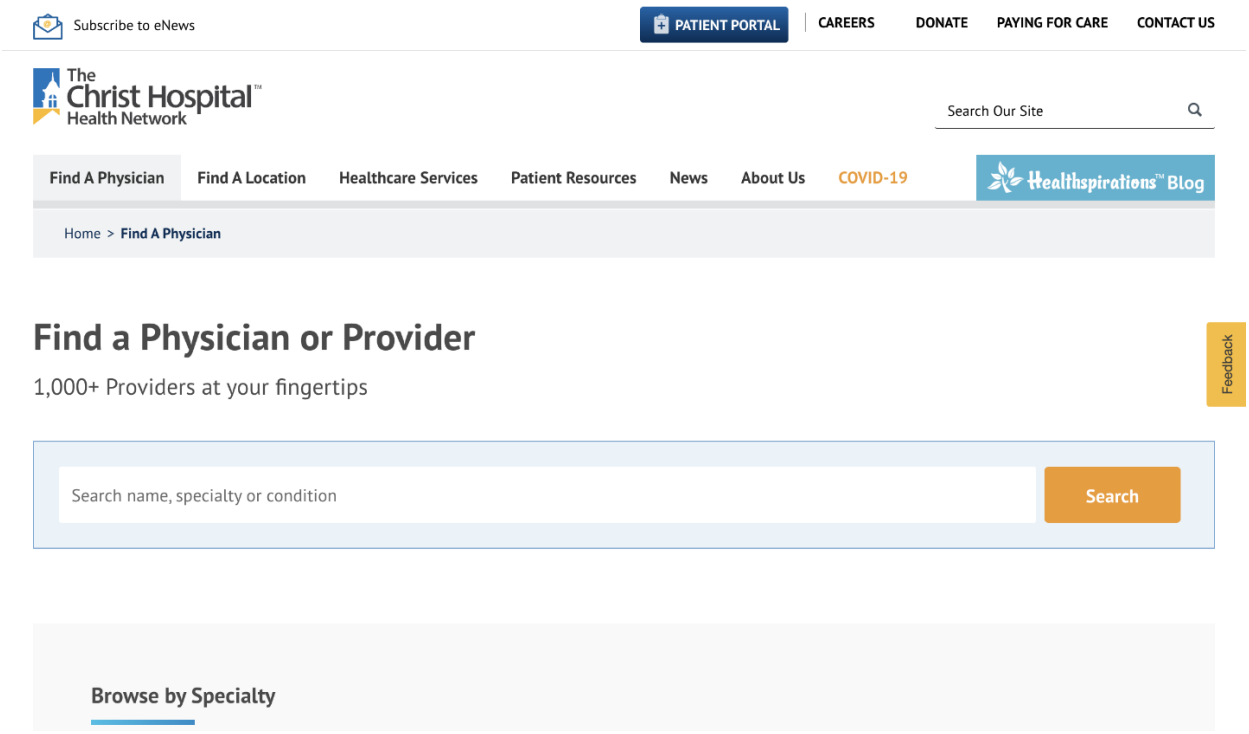
37. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the

[10] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

web browser's user. Pixels are embedded in the Source Code and instructs the Web Properties to send a second set transmissions to the third party's servers, i.e., Facebook and Google.

38. By contrast, the Markup is the façade of the Web Properties and what the user sees.

39. As an example, when a patient's HTTP Request seeks specific information from the Defendant's Website (e.g., "Find a Doctor" page), and the HTTP Response provides the requested information in the form of "Markup," forming the webpage's content and features:



40. When a patient visits www.thechristhospital.com and selects the "Find a Location" button, the patient's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that webpage. The user only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

41. Christ Hospital uses a 'POST' Request, a kind of HTTP Request that includes data and requests that the host server accept that data. This POST Request sends data to

"https://facebook.com/tr/" and includes numerous cookies. Among these cookies is the patient's c_user id, an identifier that can be used to uniquely identify the patient by their Facebook account.

42. Behind the scenes and in the backdoor of the webpage, tracking technologies like the Facebook Pixel are embedded in the Source code, automatically transmitting what the patient does on the webpage and effectively opening a hidden spying window into the patients' browser.[11]

The Tracking Tools

43. Third parties, like Facebook, offer Tracking Tools as software that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user communications and activity on those platforms. The Tracking Tools are used to gather, identify, target, and market products and services to individuals.

44. In general, Tracking Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's URL and metadata, button clicks, etc. Advertisers, such as Defendant, can track other user actions and communications and can create their own tracking parameters by customizing the software on their website.

45. When a user accesses a webpage that is hosting Tracking Tools, the user's communications with the host webpage are instantaneously and surreptitiously duplicated and sent to the third party. For example, the Facebook Pixel on Defendant's Web Properties causes the user's web browser to instantaneously duplicate the contents of the communication with the Web Properties and send the duplicate from the user's browser directly to Facebook's or Google's server.

[11] When used in the context of a screen or visual display, a "pixel" is the smallest unit in such a digital display. An image or video on a device's screen can be made up of millions of individual pixels. For example, the Facebook Pixel is a tiny image file that is so small as to be invisible to website users. It is purposefully designed and camouflaged in this manner so that website users remain unaware of it.

46. Notably, transmissions only occur on webpages that contain Tracking Tools.[12] Thus, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook via this technology but for Defendant's decisions to install the Tracking Tools on its Web Properties.

47. Sometimes a particularly tech-savvy user attempts to circumvent browser-based wiretap technology, so a website operator can also transmit data directly to Facebook by first-party cookies (CAPI server-to-server transmission). Users cannot detect or prevent transmissions through first-party cookies.

48. CAPI is another Facebook tool that functions as a redundant measure to circumvent any ad blockers or other denials of consent by the website user by transmitting information directly from Defendant's servers to Facebook's servers.[13, 14] 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."[15]

49. The third parties to whom a website transmits data through Tracking Tools and associated workarounds (CAPI) do not provide any substantive Website content relating to the

[12] Defendant's Facebook Pixel has its own unique identifier, which can be used to identify which of Defendant's webpages contain the Facebook Pixel.

[13] *What is the Facebook Conversions API and how to use it*, Realbot (last updated May 20, 2022), https://revealbot.com/blog/facebook-conversions-api/ (last visited October 4, 2023).

[14] "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.", https://developers.facebook.com/docs/marketing-api/conversions-api (last visited October 4, 2023).

[15] *About Conversions API*, Meta Business Help Center, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited October 4, 2023).

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

50. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

Defendant Disclosed Plaintiffs' and Class Members' Private Information to Facebook Using Tracking Tools

51. In this case, Defendant employed Tracking Tools, including the Facebook Pixel and Conversions API, to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook.

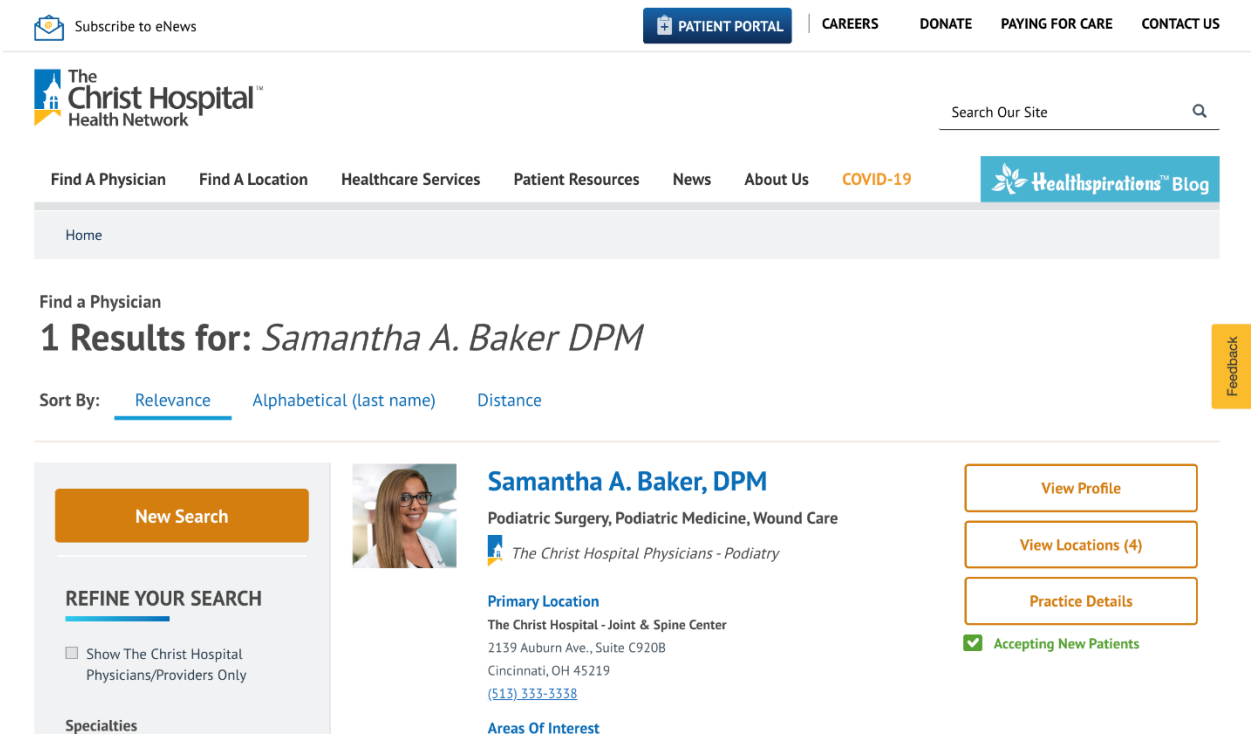
52. Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to send those communications to Facebook. These transmissions occur contemporaneously, invisibly, and without the patient's knowledge.

53. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" its patients' computing devices, allowing Facebook and other third parties to listen in on all of their communications with Defendant and thereby intercept those communications, including Private Information.

54. For instance, from the "https://www.thechristhospital.com/physician" pictured below, the patient can enter in the name of a physician, "Samantha A. Baker DPM." In doing so, the patient's web browser sends an HTTP Request to Defendant's server with the URL:

"https://www.thechristhospital.com/physician-search-results?Type=providername&PhysicianID=%23000KG7B59&PhysicianName=Samantha%20A.%20Baker,%20DPM&ExactMatch=name".

55. Defendant's server in turn sends an HTTP Response which displays the physician's information to the patient:



56. This is not the only HTTP Request Defendant's web page sends, however. In fact, at the very same time the web page is instructed to send an HTTP Request to Defendant requesting the specified doctor's information, the embedded Facebook Pixel acting as a tap is triggered, whereby Defendant's web page is also instructed to send an HTTP Request directly to Facebook notifying the social media giant of the patient's exact search:

method: GET
url: https://www.facebook.com/tr/?id=631586183931039&ev=PageView&dl=https://www.thechristhospital.com/physician-search-results?Type=_removed_&PhysicianID=_removed_&PhysicianName=Samantha+A.+Baker%2C+DPM&ExactMatch=name&_filteredParams=%7B%22unwantedParams%22%3A%5B%5D%2C%22sensitiveParams%22%3A%5B%22baaddf70fb5d432b8bd948ef91d6f910124a6d138edae4d5f000c4610ddc8eae%22%2C%2275622d2c4b480bffa55f0187fc11b769629a970b37a2394e42aaf6d3de93c5f5%22%5D%7D&rl=https://www.thechristhospital.com/physician?_filteredParams=%7B%22unwantedParams%22%3A%5B%5D%2C%22sensitiveParams%22%3A%5B%5D%7D&if=false&ts=1670496191110&sw=1366&sh=768&v=2.9.89&r=stable&ec=0&o=30&fbp=fb.1.1670496157951.955238516&it=1670496190958&coo=false&rqm=GET
httpVersion: http/1.1
headers:

[{'name': ':authority', 'value': 'www.facebook.com'}, {'name': ':method', 'value': 'GET'}, {'name': ':path', 'value': '/tr/?id=631586183931039&ev=PageView&dl=https%3A%2F%2Fwww.thechristhospital.com%2Fphysician-search-results%3FType%3D_removed_%26PhysicianID%3D_removed_%26PhysicianName%3DSamantha%2BA.%2BBaker%252C%2BDPM%26ExactMatch%3Dname%26_filteredParams%3D%257B%2522unwantedParams%2522%253A%255B%255D%252C%2522sensitiveParams%2522%253A%255B%2522baaddf70fb5d432b8bd948ef91d6f910124a6d138edae4d5f000c4610ddc8eae%2522%252C%252275622d2c4b480bffa55f0187fc11b769629a970b37a2394e42aaf6d3de93c5f5%2522%255D%257D&rl=https%3A%2F%2Fwww.thechristhospital.com%2Fphysician%3F_filteredParams%3D%257B%2522unwantedParams%2522%253A%255B%255D%252C%2522sensitiveParams%2522%253A%255B%255D%257D&if=false&ts=1670496191110&sw=1366&sh=768&v=2.9.89&r=stable&ec=0&o=30&fbp=fb.1.1670496157951.955238516&it=1670496190958&coo=false&rqm=GET&dt=f2u2wuenx7658756u3a1vxe7b1bp36xm'}, {'name': ':scheme', 'value': 'https'}, {'name': 'accept', 'value': 'image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8'}, {'name': 'accept-encoding', 'value': 'gzip, deflate, br'}, {'name': 'accept-language', 'value': 'en-US,en;q=0.9'}, {'name': 'cookie', 'value': 'sb=ewMyYqaTMtIs-sx4Y6lmlkwj; datr=ewMyYtQzmmMstZpZmB22bB2u; locale=en_US; c_user=100011152182075; xs=32%3AKXXdrGmNyj5DlA%3A2%3A1670391700%3A-1%3A5353%3A%3AAcWAt6T2cS1Jzf86Q2hvwWyPRn4f2EWdDdTWOXQm3Q; fr=0poLy6y7Px5iLs1z9.AWVcoTT_jfOHJWVfksaCCSrND4I.BjkbLi.f8.AAA.0.0.BjkbLi.AWU1Ef1rFuc'}, {'name': 'referer', 'value': 'https://www.thechristhospital.com/'}, {'name': 'sec-ch-ua', 'value': '"Not?A_Brand";v="8", "Chromium";v="108", "Google Chrome";v="108"'}, {'name': 'sec-ch-ua-mobile', 'value': '?0'}, {'name': 'sec-ch-ua-platform', 'value': '"Windows"'}, {'name': 'sec-fetch-dest', 'value': 'image'}, {'name': 'sec-fetch-mode', 'value': 'no-cors'}, {'name': 'sec-fetch-site', 'value': 'cross-site'}, {'name': 'user-agent', 'value': 'Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36'}]

queryString:

[{'name': 'id', 'value': '631586183931039'}, {'name': 'ev', 'value': 'PageView'}, {'name': 'dl', 'value': 'https%3A%2F%2Fwww.thechristhospital.com%2Fphysician-search-results%3FType%3D_removed_%26PhysicianID%3D_removed_%26PhysicianName%3DSamantha%2BA.%2BBaker%252C%2BDPM%26ExactMatch%3Dname%26_filteredParams%3D%257B%2522unwantedParams%2522%253A%255B%255D%252C%2522sensitiveParams%2522%253A%255B%2522baaddf70fb5d432b8bd948ef91d6f910124a6d138edae4d5f000c4610ddc8eae%2522%252C%252275622d2c4b480bffa55f0187fc11b769629a970b37a2394e42aaf6d3de93c5f5%2522%255D%257D'}, {'name': 'rl', 'value': 'https%3A%2F%2Fwww.thechristhospital.com%2Fphysician%3F_filteredParams%3D%257B%2522unwantedParams%2522%253A%255B%255D%252C%2522sensitiveParams%2522%253A%255B%255D%257D'}, {'name': 'if', 'value': 'false'}, {'name': 'ts', 'value': '1670496191110'}, {'name': 'sw', 'value': '1366'}, {'name': 'sh', 'value': '768'}, {'name': 'v', 'value': '2.9.89'}, {'name': 'r', 'value': 'stable'}, {'name': 'ec', 'value': '0'}, {'name': 'o', 'value': '30'}, {'name': 'fbp', 'value': 'fb.1.1670496157951.955238516'}, {'name': 'it', 'value': '1670496190958'}, {'name': 'coo', 'value': 'false'}, {'name': 'rqm', 'value': 'GET'}]

cookies:
[{'name': 'sb', 'value': 'ewMyYqaTMtIs-sx4Y6lmlkwj', 'path': '/', 'domain': '.facebook.com', 'expires': '2024-01-11T05:41:36.444Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}, {'name': 'datr', 'value': 'ewMyYtQzmmMstZpZmB22bB2u', 'path': '/', 'domain': '.facebook.com', 'expires': '2024-03-15T03:34:14.128Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}, {'name': 'locale', 'value': 'en_US', 'path': '/', 'domain': '.facebook.com', 'expires': '2022-12-14T05:40:31.231Z', 'httpOnly': False, 'secure': True, 'sameSite': 'None'}, {'name': 'c_user', 'value': '[redacted]', 'path': '/', 'domain': '.facebook.com', 'expires': '2023-12-08T09:48:17.695Z', 'httpOnly': False, 'secure': True, 'sameSite': 'None'}, {'name': 'xs', 'value': '32%3AKXXdrGmNyj5DlA%3A2%3A1670391700%3A-1%3A5353%3A%3AAcWAt6T2cS1Jzf86Q2hvwWyPRn4f2EWdDdTWOXQm3Q', 'path': '/', 'domain': '.facebook.com', 'expires': '2023-12-08T09:48:17.695Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}, {'name': 'fr', 'value': '0poLy6y7Px5iLs1z9.AWVcoTT_jfOHJWVfksaCCSrND4I.BjkbLi.f8.AAA.0.0.BjkbLi.AWU1Ef1rFuc', 'path': '/', 'domain': '.facebook.com', 'expires': '2023-03-08T09:48:16.695Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}]
headersSize: -1
bodySize: 0

57. This HTTP Request is a GET Request, a kind of Request that includes data in the URL itself. In this case, the URL contains the exact name of the Physician included in the patient's search. This information, along with the patient's personally identifying cookies, are sent directly to Facebook without the patient's knowledge or consent, and at the same time the information is being sent to Defendant's own server.

58. In this way, any information a patient enters into Christ Hospital's Web Properties can be secretly transmitted to Facebook while it is also being transmitted to Defendant's own server.

59. The third parties to whom a website transmits data through pixels do not provide any substantive content relating to the user's communications with the owner of the Web Properties. Instead, these third parties are typically procured to track user data and communications for marketing purposes.

60. The Tracking Tools allow Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs. However, Defendant's Web Properties do not rely on the Tracking Tools to function.

61. While seeking and using Defendant's services as a medical provider, Plaintiffs and Class Members communicated their Private Information to Defendant via its Web Properties.

62. Plaintiffs and Class Members were not aware that their Private Information would be shared with third parties as it was communicated to Defendant because, amongst other things, Defendant did not disclose this fact.

63. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to third parties, nor did they intend for anyone other than Defendant to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

64. Defendant's Tracking Tools sent non-public Private Information to unauthorized third parties, including but not limited to Plaintiffs' and Class Members': (1) status as medical patients; (2) health conditions; (3) desired medical treatment or therapies; (4) desired locations or facilities where treatment was sought and/or scheduled; (5) phrases and search queries (such as searches for symptoms, treatment options, or types of providers); and (6) names of the physicians they searched for along with their specialties.

65. Importantly, the Private Information Defendant's Tracking Tools sent to third parties included personally identifying information that allowed those third parties to connect the Private Information to a specific patient. Information sent to Facebook was sent alongside the Plaintiffs' and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts and therefore their identity.[16]

[16] Defendant's Web Properties track and transmit data via first party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

66. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including location, pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

67. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented Tracking Tools that surreptitiously intercepted, recorded, and disclosed patients' Private Information submitted via the Web Properties; (2) sent the Private Information to unauthorized third parties via server-to-server tools (i.e. technology that does not rely on third-party cookies and is instead transmits information to Facebook and Google directly from Defendant's server, not Plaintiffs' web browsers or devices); (3) enabled and participated in the exploitation of this private information for marketing purposes; and (4) undertook this pattern of conduct without notifying Plaintiffs or Class Members and without obtaining their affirmative express written consent.

68. By installing and implementing Facebook tools, Defendant caused Plaintiffs and Class Member's communications to be intercepted by and/or disclosed to Facebook.

69. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

Defendant's Tracking Tools Disseminated Patient Information

70. When Plaintiffs submitted Private Information via the Web Properties, it was transmitted to third parties without their knowledge and in a manner which allowed those third-parties to infer additional information about their individual identities, devices, physical locations,

financial information, demographics, and more.

71. This all occurred as a result of Defendant's decision to knowingly install and use the Facebook Pixel and Facebook Business Tools (as well other Tracking Tools).

72. The Pixel code was embedded in the Web Properties, and it sent a secret set of instructions back to patients' web browsers when they visited the Web Properties, which caused Plaintiffs' and other patients web browsers to secretly duplicate their communications with Defendant.

73. These communications—which contained Plaintiffs' Private Information—were then sent to Facebook's servers and received alongside additional information that revealed Plaintiffs' identities and corresponding Facebook profile, thereby linking that information together as one data point. Simultaneously, a second copy of this information was sent directly to Facebook from Defendant's web server.

74. The Private Information Facebook received is not meta data—it was the contents of Plaintiffs actual communications and medical information. During the same transmissions, Facebook received the patient's Facebook ID, IP address and/or device ID or other the information they input into Defendant's website, like their home address or phone number.

75. Plaintiffs are ordinary patients who had no way of knowing the Tracking Tools were implemented throughout the Web Properties, which they undoubtedly used to communicate Private Information for the purpose of seeking and obtaining medical treatment.

76. Plaintiffs did not know that Defendant's Tracking Tools would send Facebook and other third-parties every communication they made, nor did they expect that it would track their every action and record their keystrokes—thereby allowing Facebook to receive the exact text and phrases they communicated.

77. Similarly, they did not expect that the exact text and phrases they typed into the Web Properties would be exploited and monetized by both Defendant and Facebook to Plaintiffs detriment and at the cost of their protected privacy rights.

78. Several different methods allow marketers and third parties to identify individual website users. When this happens, the website user's identity is revealed via third-party cookies that work in conjunction with the Pixel. For example, the Pixel transmits the user's c_user cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

79. Facebook receives at least six cookies when Defendant's website transmits information via the Pixel.

80. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies.

81. The fr cookie contains an encrypted Facebook ID and browser identifier.[17] Facebook, at a minimum, uses the fr cookie to identify users, and this cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.[18]

82. The cookies listed are commonly referred to as third-party cookies because they were "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. Although Facebook created these cookies, Defendant is ultimately responsible because individual website users were identified via these cookies, and Facebook would not have received this data but for Defendant's implementation and use of the Pixel throughout its website.

---

[17] Data Protection Commissioner, Facebook Ireland Ltd: Report of Re-Audit (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited Oct. 4, 2023).

[18] *Cookies & other storage technologies*, FACEBOOK, https://www.facebook.com/policy/cookies/ (last visited Oct. 4, 2023).

83. Defendant also revealed its website visitors' identities via first-party cookies such as the _fbp cookie that Facebook uses to identify a particular browser and a user:[19]

84. Importantly, the _fbp cookie is transmitted to Facebook even when the user's browser is configured to block third-party tracking cookies because, unlike the fr cookies and c_user cookie, the _fbp cookie functions as a first-party cookie—i.e., a cookie that was created and placed on the website by Defendant.[20]

85. The Pixel uses both first- and third-party cookies.

86. In summation, Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link website visitors' communications and online activity with their corresponding Facebook profiles, and, because the Pixel is automatically programmed to transmit data via both first-party and third-party cookies, patients' information and identities are revealed to Facebook even when they have disabled third-party cookies within their web browsers.

87. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but other evidence suggests Defendant was using additional Tracking Tools to transmit its patients' Private Information to additional third parties.

Plaintiff A.T.'s Experience

88. Plaintiff A.T. is a patient that has received medical care from Defendant several times since October 2022, most notably for the treatment of a broken toe from October 2022 through December 2022, during which time he used the Web Properties extensively.

---

[19] *Id.*

[20] The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

89. Plaintiff A.T. sought and obtained treatment from physicians at Christ Hospital's Christ Urgent Care location and at Christ Hospital in connection with his broken toe, and he used the Website to locate an urgent care location, get information about their services, which he later obtained. Afterward, he also used the Website to search for specialists and treatment information and treatment options. In each of these instances, he communicated PHI via the Website.

90. Plaintiff A.T. recalls using both the Website and the password-protected MyChart Portal regularly throughout the two-month timespan during which he sought and obtained medical treatment for his broken toe.

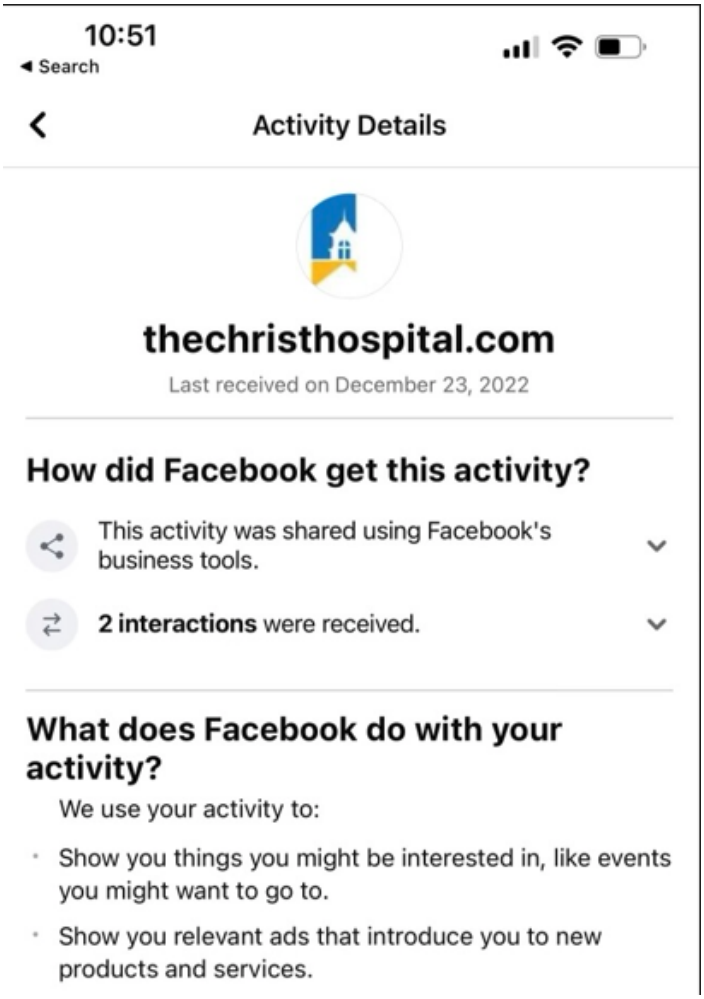
91. During this time, he used the Website's "Find a Physician" tool and used filters and tools to enter information about his medical condition; used the website's search bar to find treatment information for his toe (including by typing specific phrase such as "how long is the recovery time for a broken toe"); accessed details concerning his scheduled medical appointments; downloaded medical forms relevant to his upcoming appointments; and accessed webpages related to the payment of his medical bills.

92. On the password protected MyChart portal, accessed through Defendant's website, Plaintiff A.T. recalls opening and completing required medical forms, which involved entering specific personal information and medical information into text fields, and opening and reviewing specific medical records in preparation for upcoming medical appointments.

93. In the course of using both the website and the patient portal, he communicated with Defendant and its agents, including his specialist and his other care providers, via Defendant's Online Platforms and reasonably expected that—as a patient seeking and actively receiving treatment—his communications were confidential and would not be received by Facebook,

Google, and other unknown third-parties, or used for marketing purposes, without his express written consent. That was not the case.

94. The image below is a screenshot captured by Plaintiff A.T. while accessing his personal Facebook account, specifically his "Off-Site Activity" log, which demonstrates that—at a minimum—Facebook received and viewed his communications and protected health information when he used www.thechristhospital.com to obtain medical care in December 2022.



95. The image demonstrates Meta obtained Plaintiff A.T.'s communications with Defendant (and protected health information embedded in those communications) via the Pixel, Conversions API, SDK, and related Facebook business tools—and used specific details pertaining to his health record for marketing—as a direct result of Defendant installing the Analytics Code

and using those tools on sensitive web pages it encouraged its patients, including Plaintiff, to use in conjunction with obtaining medical care.

96. The image also demonstrates Meta linked Plaintiff's Private Information to his unique Facebook account, thereby allowing Meta to connect and associate it with other information in its possession and for retargeting and other marketing purposes.

97. Plaintiff A.T. received several targeted ads on Facebook and Instagram related to his specific medical symptoms, conditions, and treatment he received from Defendant.

98. For example, beginning in October 2022, Plaintiff A.T. noticed advertisements in his Facebook and Instagram feeds for air casts and medical boots used to treat broken toes, just like the one he was prescribed by his care team at Defendant's hospital a few days prior, which he had also learned about when searching for treatment options on the Website.

99. Since he only consulted with Defendant in pursuit of care for his broken toe, and the advertisements he saw specifically referenced that medical condition and the treatment he obtained from Defendant, Plaintiff A.T. believes Meta obtained, viewed, and used his PHI for targeted advertising.

100. The timing and specificity of these and other marketing attempts is not simply a coincidence. Meta and its agents viewed and used his medical information because: (1) the off-site activity report associated with his Facebook account specifically states that Meta will use his communications with www.thechristhospital.com to show him things he "might be interested in" and "relevant ads"; (2) the targeted ads he received were specifically for medical devices used to treat the medical condition about which he consulted Defendant and its agents; and (3) he did not directly or purposely communicate this information to Meta or otherwise give it permission to intercept, view, or obtain his PHI from Defendant.

101. Plaintiff A.T. is not presently aware of the full scope of Defendant's past or continuing privacy violations, but its Web Properties undoubtedly commandeered his web browser(s) and caused his communications to be intercepted, replicated, and obtained by Meta, Google, and other unknown third parties without his knowledge or affirmative express consent.

102. Through the process detailed in this Complaint, Defendant unlawfully assisted third parties with intercepting Plaintiff A.T.'s communications and health information, breached confidentiality, violated Plaintiff A.T.'s right to privacy, and unlawfully disclosed his personally identifiable information and protected health information.

103. The conduct described herein is and was highly offensive to an ordinary person because, and it is and was highly offensive to Plaintiff A.T.

104. Plaintiff A.T. was unaware of Defendant's use of the Pixel or any other tracking tools on its Web Properties until approximately December 2022, shortly before he filed his complaint.

105. Plaintiff A.T.'s counsel has gathered and incorporated screenshots evidencing Defendant's use of the Pixel on its website and patient portal prior to its removal, but this preliminary investigation was limited in scope and there has not yet been an opportunity to conduct discovery or obtain network traffic reports from within the password-protected patient portal.

106. Nonetheless, based on information and belief, Plaintiff A.T. alleges Defendant was using tracking technologies throughout its Web Properties, including any password-protected patient portals and webpages, and this belief is reasonable because: (1) Defendant was in control of its Web Properties and the source code installed, implemented, or otherwise used on its Web Properties, including its MyChart patient portals which was customizable; (2) its use of the Pixel would have presumably been uniform across its Web Properties, and this is supported by the fact

that it was installed on sensitive appointment-booking webpages outside password-protected portions of the website or patient portals (i.e. it was being used without regard to the sensitive nature of patients' communications); and (3) the Pixel's removal would have likely been uniform across its Web Properties.

Plaintiff G.W.'s Experience

107. Plaintiff G.W. is a patient that has received medical care from Defendant several times, on a regular basis since 2019, including for COVID-19, medical issues concerning his digestive health and related symptoms, and his sleep health.

108. His primary care physician is also part of Defendant's network.

109. Plaintiff G.W. first used Defendant's Web Properties during the COVID-19 pandemic in order to obtain necessary medical care and information concerning testing sites. He specifically recalls using the Website to locate information related to his symptoms, testing location information, and related medical information.

110. Plaintiff G.W. also used the Website's physician finder tools to identify physicians and specialists who ultimately treated his digestive problems and sleep issues, and in doing so, he submitted his Private Information, including specific symptoms associated with sleep disorders and digestive problems, desired treatments and medications to treat these specific conditions, the types of specialists he was seeking (and who he ultimately obtained treatment from), and the types of treatment he was seeking.

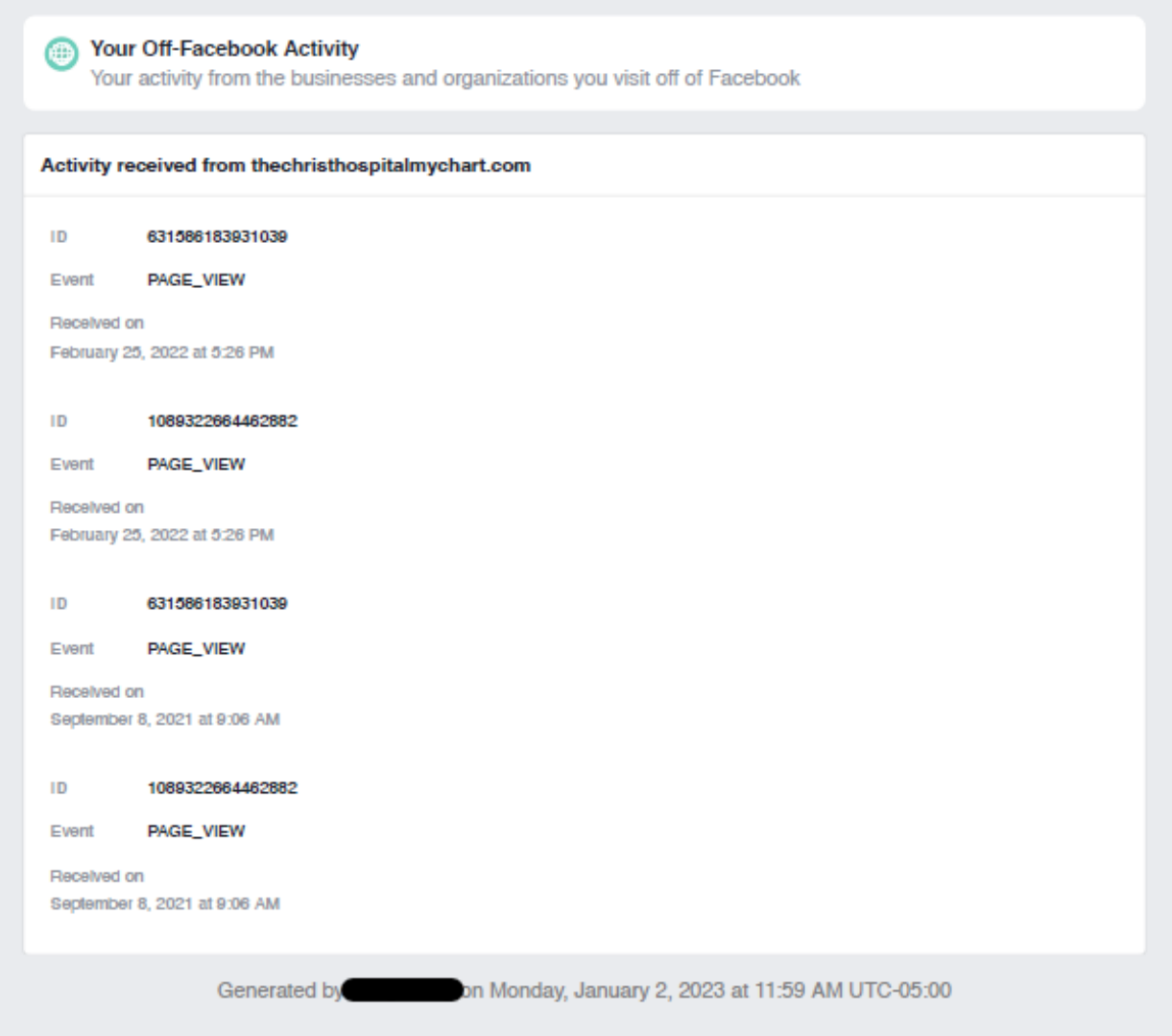
111. As a patient, and in order to obtain medical treatment from Defendant, Plaintiff G.W. also recalls using the Web Properties to identify information regarding treatment and testing of COVID-19 and to identify and locate specific medical providers who specialized in the issues he was experiencing. He has also used the Web Properties routinely, for several years, in order to

obtain treatment and care from this family doctor and has communicated extensively with his family doctor.

112. Plaintiff G.W. also recalls logging in to password-protected portions of Defendant's Web Properties as early as 2018 or 2019 in order to access his medical records, review test results, manage his prescriptions for Pantoprazole and Trazodone, schedule appointments with his family doctor, and exchange messages directly with his doctors regarding specific symptoms, treatment options, and recommendations for other specialist care.

113. In doing so, Plaintiff G.W. communicated with Defendant and its agents, including his family doctor and specialist doctors, via Defendant's Web Properties and reasonably expected that—as a patient seeking and receiving treatment—his communications were confidential and would not be received by Facebook, Google, and other unknown third-parties, or used for marketing purposes, without his express written consent. That was not the case.

114. The image below is a screenshot captured by Plaintiff G.W. while accessing his personal Facebook account, specifically his "Off-Site Activity" log, which demonstrates that—at a minimum—Facebook received and viewed his Private Information when he used the Patient Portal to obtain medical care on September 8, 2021 and February 25, 2022.



115. The image demonstrates Meta obtained Plaintiff G.W.'s communications with Defendant (and protected health information embedded in those communications) via the Pixel, Conversions API, SDK, and related Facebook business tools—and used specific details pertaining to his health record for marketing—as a direct result of Defendant installing the Analytics Code and using those tools on sensitive web pages it encouraged its patients, including Plaintiff G.W., to use in conjunction with obtaining medical care. The image also demonstrates Meta linked his Private Information to his unique Facebook account, thereby allowing Meta to connect and associate it with other information in its possession and for retargeting and other marketing

purposes.

116. Finally, Plaintiff G.W. also believes Google intercepted, received, learned the contents and substance of, and ultimately used his specific medical information because, although Defendant purportedly removed the Facebook Pixel from its Online Platforms in or around December of 2022, it has used Google Analytics in the past and continues to use that tracking tool on a portion of its Online Platforms. Like the Pixel, the Google Analytics tool transmits sensitive information without patients' knowledge or consent and thereby constitutes an additional impermissible disclosure of patients' medical information.

117. Plaintiff G.W. recently used Defendant's Web Properties again to search for and obtain testing for COVID-19, as he has done in the past using Defendant's services.

118. Immediately thereafter, he received targeted ads from news agencies discussing the most recent surge of COVID-19 cases in the United States. The timing and specificity of this marketing attempt indicates that Defendant is still using Tracking Tools that disseminate its patients' information for marketing purposes, and that Google viewed medical information related to his most recent medical appointments.

119. Notably, Plaintiff G.W. maintains and accesses his Gmail on his phone and personal computer. Like Meta, Google can identify him, link information it receives about him to other information in its possession (including but not limited to device identifiers), and then send him targeted advertisements. He has not, however, given Google permission to intercept, view, and otherwise receive his communications with Defendant or obtain his PHI from Defendant.

Plaintiff W.B.'s Experience

120. Plaintiff W.B. has been Defendant's patient since 1988 and has routinely sought treatment for and obtained medical treatment from Defendant periodically since that time,

including mammograms, annual well visits, and related test/services at the following locations: Christ Base, Green Township, and Montgomery.

121. Most recently, she attended an Annual Well Visit on March 22, 2023, for the Fernald Workers Medical Monitoring Program.

122. Plaintiff W.B. has used the Website since at least November of 2018, and specifically recalls using it in or around that time to obtain information related to a mammogram appointment she scheduled that same month, including the facility location and relevant patient information. She has used the Website periodically since that time, accessing it from her phone and computer, in relation to her medical care and treatment as one of Defendant's patients.

123. Plaintiff W.B. used the Website to find details about upcoming medical appointments, find location details, and download/print patient web forms (such as treatment authorization forms, medical records request forms, and forms related to medical bills).

124. Plaintiff W.B. has also used the MyChart patient portal since approximately 2014, accessing it from her laptop and Android mobile phone, to obtain information related to her patient health records, past and future appointments, and prescriptions, including the following medications to which she has been prescribed: atorvastatin, pantoprazole, bupropion, citalopram, triamterene azide, carbidopa/levodopa, and magnesium oxide.

125. Plaintiff W.B. communicated her Private Information via the Web Properties and recalls using the Website's general search bar to type text and phrases that included her prescription medications (listed supra), medical conditions and symptoms, which include the following: Parkinson's, Ménière's, migraines, depression, and obesity.

126. Plaintiff W.B. has an active Facebook account that she stays logged into on her laptop and phone, which are the same devices that she has used to access the Web Properties.

127. In recent years, Plaintiff W.B. has noticed an influx of targeted Facebook ads shortly after communicating PHI via Defendant's Web Properties and attending medical appointments at its facilities. On multiple occasions, she has noticed an uptick in targeted marketing efforts that coincides with her use of Defendant's Web Properties and services. Plaintiff W.B. specifically recalls seeing targeted healthcare-related refencing diabetes and bipolar disorder and believes she was identified and targeted by these companies based on information she communicated via Defendant's Web Properties.

128. Although she has not been diagnosed with diabetes or bipolar disorder, she believes these targeted ads are the result of Defendant's privacy practices and use of Tracking Tools on its Web Properties—particularly considering the timing and the fact that several or her prescriptions and symptoms overlap with medical conditions referenced in the ads she received.

129. Plaintiff W.B. also has evidence that at least 18 individual interactions and communications were transmitted to Facebook because of the Tracking Tools installed on the Website when she used it in relation to her medical her medical treatment on December 13, 2022. The screenshot below was taken from Plaintiff W.B.'s Facebook account, and more specifically, her off-site activity report.

130. In addition to Facebook, Plaintiff W.B. has Gmail, LinkedIn, Twitter, and Reddit accounts she accesses on a regular and recurring basis. Each of these companies furnish online tracking tools that can be used for marketing and targeted advertising, transmitted to data brokers, and sold to private individuals and companies. Moreover, each of these entities can identify Plaintiff W.B. and link her PHI with other information in its possession.

131. Plaintiff W.B. is highly offended by Defendant's conduct and expected, as her trusted healthcare provider, it would not disseminate or allow third-parties to use her Private Information for marketing purposes without first obtaining her affirmative express consent.

Plaintiffs' Collective Experience, Expectations, and Harm

132. On numerous occasions, at Defendant's direction, and with its encouragement, Plaintiffs accessed the Web Properties from their personal computers and/or mobile devices for the purpose of obtaining medical treatment for their individual medical conditions.

133. Plaintiffs specifically accessed Defendant's Web Properties as patients to receive healthcare services from Defendant or Defendant's affiliates—they were not seeking generalized medical information, nor were they using the Website for anyone other than themselves.

134. Plaintiffs submitted medical information to Defendant via its Web Properties, which contained Tracking Tools Defendant purposely installed and controlled, and which subsequently commandeered their devices without their knowledge or express authorized consent.

135. Pursuant to the systematic process described in this Complaint, Plaintiffs' Private Information was disclosed to Facebook, and this data included their PII, PHI, and related confidential information. Defendant intercepted and/or assisted these interceptions without Plaintiffs' knowledge, consent, or express written authorization.

136. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiffs' Private Information.

137. As Defendant's patients, Plaintiffs reasonably expected that their online communications with Defendant were solely between themselves and Defendant and that such communications would not be transmitted to or disclosed to a third party. But for their status as Defendant's patients, Plaintiffs would not have disclosed their Private Information to Defendant.

138. Plaintiffs never consented to the use of their Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information.

139. Notwithstanding, through the Pixel and Conversions API, Defendant transmitted Plaintiffs' Private Information to third parties, such as Facebook.

140. Accordingly, during the same transmissions, the Web Properties routinely provide Facebook with its patients' FIDs, IP addresses, and/or device IDs or other information they input into Defendant's Web Properties, like their home address, zip code, or phone number. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients. Plaintiffs and Class Members identities could be easily determined based

on the FID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

141. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the Website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity. A user's Facebook Profile ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

142. Based on the presence of the Pixel and Conversions API, Defendant unlawfully disclosed Plaintiffs' Private Information to Facebook. The presence of Facebook advertisements and the images from Plaintiffs' own accounts confirms Defendant's unlawful transmission of Plaintiffs Private Information to Facebook.

143. Upon information and belief, as a "redundant" measure to ensure Plaintiffs' and Class Members' Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiffs' and Class Members' Private Information from electronic storage on Defendant's server directly to Facebook.

144. Plaintiffs suffered injuries in the form of (i) invasion of privacy; (ii) diminution of value of the Private Information; (iii) interference with a confidential relationship; (iv) the

continued and ongoing risk to their Private Information; and (v) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiffs medical conditions and other confidential information they communicated to Defendant via the Web Properties.

145. Plaintiffs have a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure, and likewise have a continuing interest in learning exactly which Tracking Tools were installed, and to whom those Tracking Tools disseminated information—i.e., an exhaustive list of who received their Private Information. Plaintiffs have a right to exercise control over their medical records and health information communicated during the course of the patient-provider relationship, and they seek to enforce this right.

Defendant Violated HIPAA

146. Under Federal Law, 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 patients' express written authorization.[21]

147. 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."[22]

148. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media;

---

[21] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

[22] HHS.gov, HIPAA For Professionals (last visited April 12, 2023), https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html.

maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

149. 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." 45 C.F.R. § 160.103.

150. 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) "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. Any other unique identifying number, characteristic, or code…;and"

The covered entity must not "have actual knowledge that the information could

> be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 160.514.

151. 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. 45 C.F.R. §§ 160.103, 164.502.

152. 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." 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." 42 U.S.C. § 1320d-6.

153. 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.

154. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 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."

155. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the 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.[23]

156. In its guidance for Marketing, the 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*. (Emphasis added).[24]

157. As alleged above, there is an HHS Bulletin that highlights the obligations of "regulated entities," which are HIPAA-covered entities and business associates, when using tracking technologies.[25]

158. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

---

[23]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Oct. 4**,** 2023).

[24]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Oct. 4, 2023).

[25] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

159. Defendant's actions violated HIPAA Rules per this Bulletin.

Defendant Violated Analogous Ohio Law

160. Ohio has made its laws governing the use and disclosure of protected health information consistent with HIPAA. *See* R.C. 3798.01, *et seq.* Ohio law adopts the same definitions of "covered entity," "disclosure," "health care provider," "health information," "protected health information," "individually identifiable health information," and "use" as provided by the HIPAA Privacy Rule. *See* R.C. 3798.01.

161. Defendant is a "covered entity" within the meaning of R.C. 3798.01.

162. Under R.C. 3798.03(A)(2), a covered entity shall "Implement and maintain appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information in a manner consistent with 45 C.F.R. 164.530(c)."

163. Under R.C. 3798.04, a covered entity shall not do either of the following:

> (A) Use or disclose protected health information without an authorization that is valid under 45 C.F.R. 164.508 and, if applicable, 42 C.F.R. part 2, except when the use or disclosure is required or permitted without such authorization by Subchapter C of Subtitle A of Title 45 of the Code of Federal Regulations and, if applicable, 42 C.F.R. part 2;
>
> (B) Use or disclose protected health information in a manner that is not consistent with 45 C.F.R. 164.502.

164. Under this statute and the federal standards, it incorporates, 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 patients' express written authorization, nor sell such information without disclosing that the disclosure will involve remuneration to the provider.[26]

[26] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

165. Ohio courts have long recognized that health care providers like Defendant owe a duty of confidentiality to patients, which prohibits them from disclosing patients' health information without patients' written consent. *Biddle v. Warren General Hospital*, 86 Ohio St.3d 395, 401 (1999). And Ohio law subjects medical providers who treat conditions such as HIV to heightened duties of confidentiality. R.C. 3701.243(1)-(3).

Defendant Violated Industry Standards

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

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

168. 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)

169. AMA Code of Medical Ethics Opinion 3.2.4 provides:

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

170. AMA Code of Medical Ethics Opinion 3.3.2 provides:

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

Plaintiffs' and Class Members' Expectation of Privacy

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

172. 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 their Private Information with third parties for a commercial purpose, unrelated to patient care.

173. Plaintiffs and Class Members would not have used Defendant's Web Properties, would not have provided their Private Information to Defendant, and would not have paid for Defendant's healthcare services, or would have paid less for them, had they known that Defendant would disclose their Private Information to third parties.

IP Addresses Are Protected PII

174. On information and belief, with the Tracking Tools on Defendant's Web Properties, Defendant also disclosed and otherwise assisted third parties with intercepting Plaintiffs' and Class Members' Computer IP addresses.

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

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

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

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

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

180. Under HIPAA, an IP address is considered PII:

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

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

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

Defendant Was Enriched and Benefitted from the Use of The Tracking Tools and Unauthorized Disclosures

182. The primary motivation and a determining factor in Defendant's interception and disclosure of Plaintiffs' and Class Members' Private Information was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the use of patient data for advertising in the absence of express written consent. Defendant's further use of their Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and analogous state law, and an invasion of privacy. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on its platform.

183. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

184. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients to use its services. Defendant did so

through use of the intercepted patient data it obtained, procured, and/or disclosed in the absence of express written consent.

185. By utilizing the Tracking Tools, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiffs and Class Members and violating their rights under federal and Ohio Law.

Plaintiffs' and Class Members' Private Information Had Financial Value

186. 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.

187. 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.

188. The value of health data 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 described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[27]

[27] *See* https://time.com/4588104/medical-data-industry/ (last visited Oct. 4, 2023).

189. 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."[28]

Facebook's Business Model: Exploiting User Data to Sell Advertising in Exchange for Providing "Free" Analytics Tools

190. Facebook, a social media platform founded in 2004 and today operated by Meta Platforms, describes itself as a "real identity" platform with 2.9 billion active users.[29] This means that users are permitted only one account and must share "the name they go by in everyday life."[30]

191. To that end, it requires users to provide their first and last name, along with their birthday, telephone number and/or email address, and gender, when creating an account.[31] Plaintiffs provided this information when they created their Facebook accounts.

192. In 2007, realizing the value of having direct access to millions of consumers, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming this service to be a "completely new way of advertising online," that would allow "advertisers to deliver more tailored and relevant ads."[32] Facebook has since evolved into one of the largest advertising companies in the world.[33]

193. Facebook's ability to harvest, extract, and monetize individuals' data is at the heart of its business model, and it obtains this data from Tracking Tools, including the Pixel and related

---

[28] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Oct. 4, 2023).
[29] https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701#:~:text=Facebook%20said%20in%20its%20most,of%20them%20than%20developed%20ones.
[30] https://transparency.fb.com/policies/community-standards/account-integrity-and-authentic-identity/
[31] https://www.facebook.com/help/406644739431633
[32] https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/
[33] https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/

technologies Defendant implemented and used on its Website.[34]

194. In exchange for installing the Pixel and using its Business Tools, Defendant benefitted in the form of low-cost marketing and free software that it would have otherwise had to purchase from a HIPAA-compliant marketing company and skilled computer engineer capable of coding and implementing tools that protect patient privacy while providing the same analytics.

195. These surveillance practices allow Facebook to make inferences about users based on their interests, behavior, connections, and online activities on third-party websites, including Defendant's Web Properties.[35] In turn, and in exchange for hosting its Pixel, it provides advertising services on its own social media platforms, as well as other websites through its Facebook Audience Network.

196. Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications. These profiles are associated with personal identifiers, including IP addresses, cookies, and other device identifiers. Facebook also tracks non-users across the web through its internet marketing products and source code, and Plaintiffs allege that's exactly what happened int this case when they used the Website.

197. Facebook employs algorithms, powered by machine learning tools, to determine what advertisements to show users based on their habits and interests, and utilizes tracking software such as the Meta Pixel to monitor and exploit users' habits and interests.

198. Tracking information about users' and non-users' habits and interests is a critical part of Facebook's business model because its how the companies sells advertising space and monetizes data—thus giving it a strong motive to intrude into the private lives of Plaintiffs and Class Members.

[34] https://www.facebook.com/business/help/742478679120153?id=1205376682832142
[35] https://www.facebook.com/business/ads/ad-targeting

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

TOLLING

200. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know (and had no way of knowing) that their PII and PHI was intercepted and unlawfully disclosed to Facebook because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

201. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Ohio Rules of Civil Procedure.

202. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All individuals residing in the United States who are, or were, patients of Defendant or any of its affiliates, used Defendant's Website or Patient Portal, and as a result, had their Private Information disclosed to a third party without authorization or consent.**

In the alternative, Plaintiffs seek to represent a "Ohio Class" defined as:

> **All individuals residing in Ohio who are, or were, patients of Defendant or any of its affiliates, used Defendant's Website or Patient Portal, and as a result, had their Private Information disclosed to a third party without authorization**

or consent.

203. The Nationwide Class and Ohio Class are collectively referred to as the "Class."

204. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

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

206. Numerosity, Civ.R. 23(a)(1). Based on limited discovery obtained during the parties' dispute over CAFA jurisdiction, "the actual size of the putative class falls somewhere between 596,037 and 788,787." *Doe v. Christ Hosp.*, No. 1:23-CV-27, 2023 WL 4757598, at *4 (S.D. Ohio July 26, 2023). This is so numerous that joinder of all Class Members is impracticable.

207. Commonality, Civ.R. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

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

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

c. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

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

e. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

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

g. Whether Defendant's conduct violated the Ohio Wiretapping Act, R.C. 2933.52.

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

i. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced because of Defendant's disclosure of their Private Information.

208. Typicality, Civ.R. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised because of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

209. Adequacy, Civ.R. 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.

210. Superiority and Manageability, Civ.R. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation 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.

211. Policies Generally Applicable to the Class. Civ.R. 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.

212. 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 unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was 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.

213. The litigation of the claims is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members (which can be obtained from Defendant's records) demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

215. Unless a class-wide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

216. Further, 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 under Rule 23(b)(2) of the Ohio Rules of Civil Procedure.

217. Issue Certification, Civ.R. 23(c)(4). Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, the following:

a. Whether Defendant owed a legal duty to not disclose Plaintiffs and Class Members' Private Information;

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

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

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

COUNT I
Breach of Confidence (*Biddle*)
(On Behalf of Plaintiffs and the Class)

218. Plaintiffs incorporate all prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

219. Medical providers in Ohio have a duty to their patients to keep Private Information confidential and to not disclose Private Information to third parties without the patient's informed consent or other applicable legal privilege entitling them to do so.

220. Plaintiffs and Class Members had reasonable expectations of privacy when interacting with Defendant through the Web Properties, including communications made on the

Web Properties, in virtue of this well-known duty of confidentiality incumbent upon medical providers.

221. Contrary to its duty as a medical provider, Defendant deployed the Tracking Tools to secretly record and transmit nonpublic Private Information to third parties as described throughout this Complaint without patient authorization or consent.

222. The Private Information that Defendant transmitted to third parties without authorization was learned within a physician-patient relationship.

223. Defendant's breaches of confidence were committed negligently, recklessly, and/or intentionally.

224. Defendant's breaches of confidence were a direct and proximate cause of several injuries suffered by Plaintiffs and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains with Defendant. Plaintiffs and Class Members seek compensatory damages in an amount to be proved at trial. In the alternative, Plaintiffs and Class Members seek nominal damages.

COUNT II
Invasion of Privacy - Intrusion Upon Seclusion
(On Behalf of Plaintiffs and the Class)

225. Plaintiffs incorporate the prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

226. The Private Information of Plaintiffs and Class Members is private, confidential, and not intended to be shared with third parties absent authorization.

227. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and communications with Defendant, and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

228. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information and communications confidential.

229. Defendant's conduct constitutes a physical or sensory intrusion on Plaintiffs' and Class Members' privacy because Defendant installed the Tracking Tools on its Web Properties for the purpose of secretly recording the activity on Plaintiffs' and Class Members' browsers and then transmitting the Private Information learned from this activity to third parties for commercial purposes without authorization or consent.

230. The secret recording and transmission of Plaintiffs' and Class Members' Private Information and communications to third parties for commercial purposes without authorization or consent is highly offensive and/or outrageous to a reasonable person.

231. Defendant's conduct constitutes an interference with Plaintiffs' and Class Members' interest in solitude or seclusion.

232. Defendant's invasions of privacy were a direct and proximate cause of several injuries suffered by Plaintiffs and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains. Plaintiffs and Class Members seek compensatory damages in an amount to be proved at trial. In the alternative, Plaintiffs and Class Members seek nominal damages.

COUNT III
Breach of Implied Contract
(On behalf of Plaintiffs and the Class)

233. Plaintiffs incorporate the prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

234. As a condition of utilizing Defendant's Web Properties and receiving services from Defendant's healthcare facilities and professionals, Plaintiffs and Class Members provided their Private Information and compensation for their medical care.

235. When Plaintiffs and Class Members provided their Private Information to Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

236. Plaintiffs and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

237. Plaintiffs and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

238. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information without consent to third parties for commercial purposes.

239. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of Private Information.

240. Defendant's breaches of implied contract were a direct and proximate cause of several injuries suffered by Plaintiffs and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains with Defendant. Plaintiffs and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract. In the alternative, Plaintiffs and Class Members seek nominal damages.

COUNT IV
Unjust Enrichment
(On behalf of Plaintiffs and the Class)

241. Plaintiffs incorporate the prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

242. This claim is brought in the alternative to breach of implied contract.

243. Defendant benefits from the use of Plaintiffs' and Class Members' Private Information and unjustly retained those benefits at their expense.

244. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiffs and Class Members, without authorization and proper compensation to exceed the limited authorization and access to that information which was given to Defendant.

245. Defendant exceeded any authorization given and instead consciously disclosed and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

246. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class Members because Defendant's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs and Class Members.

247. The benefits that Defendant derived from Plaintiffs and Class Members was not offered by Plaintiffs and Class Members gratuitously and rightly belongs to Plaintiffs and Class Members. It would be against equity and good conscience for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

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

COUNT V
Negligence
(On behalf of Plaintiffs and the Class)

249. Plaintiffs incorporate the prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

250. This claim is brought in the alternative to breach of confidence (*Biddle*).

251. Defendant owed Plaintiffs and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

252. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Web Properties.

253. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third parties Plaintiffs' and Class Members' communications with Defendant, including Private Information and the contents of such information.

254. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent, or authorization, and were unprivileged.

255. Defendant's negligence was a direct and proximate cause of several injuries suffered by Plaintiffs and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains with Defendant. Plaintiffs and Class Members seek compensatory

damages in an amount to be proved at trial. In the alternative, Plaintiffs and Class Members seek nominal damages.

COUNT VI
Breach of Fiduciary Duty
(on behalf of Plaintiffs and the Class)

256. Plaintiffs incorporate the prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

257. This claim is brought in the alternative to breach of confidence (*Biddle*).

258. Defendant has a fiduciary duty to act primarily for the benefit of its patients, including Plaintiffs and Class Members by: (1) safeguarding Plaintiffs' and Class Members' Private Information; (2) timely notifying Plaintiffs and Class Members of disclosure of their Private Information to unauthorized third parties; and (3) maintaining complete and accurate records of what patient information (and where) Defendant did and does store and disclose.

259. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to protect and/or intentionally disclosing Plaintiffs' and Class Members' Private Information to third parties without authorization or consent.

260. Defendant's breach of fiduciary duty is evidenced by its failure to comply with federal and state privacy regulations, including:

a. By failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

b. By failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

c. By failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);

d. By failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiffs' and Class Members' PHI;

e. By failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. By failing to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);

g. By impermissibly and improperly using and disclosing Private Information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*, 45 C.F.R. § 164.508, *et seq.*, and R.C. 3798.04, *et seq.*;

h. By failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. By failing to comply with R.C. 3798.04, *et seq.*, regarding the use or disclosure of protected health information.

261. Defendant's breaches of fiduciary duty were a direct and proximate cause of several injuries suffered by Plaintiffs and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains. Plaintiffs and Class Members seek compensatory damages in an amount to be proved at trial. In the alternative, Plaintiffs and Class Members seek nominal damages.

COUNT VII
Interception and Disclosure of Electronic Communications in Violation of R.C. 2933.52
(on behalf of Plaintiffs and the Class)

262. Plaintiffs repeat and re-allege each and every paragraph in the Complaint as if fully set forth herein.

263. Plaintiffs bring this claim on behalf of themselves and all members of the Class.

264. All conditions precedent to this action have been performed or have occurred.

265. R.C. 2933.52(B)(4) provides that it is unlawful for a person not acting under law to intercept an electronic communication "for the purpose of committing a criminal offense or tortious act in violation of the laws or Constitution of the United States or this state for the purpose of committing any other injurious act."

266. Defendant intercepted Plaintiffs' and Class Members' electronic communications for the purpose of committing multiple tortious acts, including, but not limited to, the criminal and tortious acts as detailed throughout the complaint.

267. For example, Defendant intercepted Plaintiffs' and Class Members' electronic communications for the purpose of disclosing those communications to Facebook without the knowledge, consent, or written authorization of Plaintiffs or Class Members. The disclosure of Plaintiffs' and Class Members' Personal Health Information to Facebook without consent or proper authorization is an illegal or tortious act that violates multiple laws, including (but not

limited to) 42 U.S.C. § 1320d-6, 15 U.S.C. 45, R.C. 3798.04, R.C. 3798.03(2), 45 CFR § 164.508(a)(1), R.C. 1345.02(A), R.C. 1345.03(A), and R.C. 1347.05(g). Defendant's misconduct accordingly falls within the ambit of Ohio's wiretapping statute.

268. Further, as set forth above, Defendant's interception of Plaintiffs' and Class Members' electronic communications for the purpose of disclosing their Private Information to Facebook is also a tortious act that constitutes a breach of the fiduciary duty of confidentiality owed by doctors and hospital systems to their patients as set forth by the Ohio Supreme Court in *Biddle v. Warren General Hospital*, 86 Ohio St. 3d 395, 401 (1999).

269. Any person whose wire, oral, or electronic communications are intercepted, disclosed, or intentionally used in violation of the Wiretap Act may bring a civil action to recover from the person or entity that engaged in the violation. R.C. 2933.65.

270. Defendant violated the Ohio Wiretap Act by intercepting Plaintiffs' and Class Members' electronic communications in violation of R.C. 2933.52(A)(1).

271. Defendant separately violated the Ohio Wiretap Act by using the contents of a Plaintiffs' and Class Members' electronic communications, knowing or having reason to know, that the contents were obtained through the interception of an electronic communication in violation of R.C. 2933.52(A)(3). Specifically, Defendant knowingly used the contents of Plaintiffs' and Class Members' electronic communications to barter and/or sell that information to Facebook in return for access to the Tracking Tools.

272. Defendant qualifies as a person under the statute.

273. Ohio law defines "electronic communications" to mean "the transfer of a sign, signal, writing, image, sound, datum, or intelligence of any nature that is transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system." R.C.

2933.51(N). Plaintiffs' and Class Members' communications with Defendant constitute "electronic communications" under Ohio law because each communication is made using personal computing devices (e.g., computers, smartphones, tablets) that send and receive communications in whole or in part through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

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

275. The intercepting 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. The Tracking Tools;

e. Facebook's Meta Pixel;

f. Internet cookies;

g. Defendant's computer servers;

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

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

276. "Contents" under the Act, when used with respect to any electronic communication, includes "any information concerning the substance, purport, or meaning of the communication." R.C. 2933.51(G).

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

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

a. The parties to the communications;

b. The precise text of patient search queries;

c. PII such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;

d. The precise text of patient communications about specific doctors;

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

f. The precise text of patient communications about specific treatments;

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

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

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

j. The precise dates and times when patients click to Log-In on Defendant's Web Properties;

k. The precise dates and times when patients visit Defendant's Web Properties;

l. Information that is a general summary or informs third parties of the general subject of communications that Defendant sends back to patients in response

to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information; and

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

279. Plaintiffs and Class Members reasonably expected that their Private Information was not being intercepted, recorded, and disclosed to Facebook or other third-party advertising companies.

280. No legitimate purpose was served by Defendant's willful and intentional disclosure of Plaintiffs' and Class Members' Private Information to Facebook and similar third-party advertising companies. Neither Plaintiffs nor Class Members consented to the disclosure of their Private Information by Defendant to these third parties. Nor could they have consented, given that Defendant never sought Plaintiffs' or Class Members' consent, or even told visitors to its website that their every interaction was being recorded and transmitted to Facebook and other third parties via Tracking Tools so that these third parties could monetize their Private Information.

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

282. Under the Wiretapping Act, aggrieved persons are entitled to recover actual damages, but not less than liquidated damages computed at the rate of one hundred dollars a day for each day of the violation or ten thousand dollars whichever is greater, punitive damages, and reasonable attorney's fees and other litigation costs. R.C. 2933.65.

283. 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.

284. Plaintiffs and Class Members have been irreparably harmed by the loss of their privacy. Plaintiffs and Class Members will continue to face a substantial risk of irreparable harm from Defendant's actions if not enjoined. Defendant is a major medical provider. Depending on the type and severity of future illness or injury, Plaintiffs and Class Members may be required to seek Defendant's medical services. An injunction would serve the public interest because Plaintiffs and other Ohio residents should not be forced to choose between receiving necessary medical services and maintaining the confidentiality of their Private Information.

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

COUNT VIII
Violations of the Ohio Consumer Sales Practices Act, R.C. 1345.01, *et seq.*
(On behalf of Plaintiffs)

286. Plaintiffs incorporate the prior allegations as if fully set forth herein.

287. Plaintiffs bring this claim for declaratory judgment and injunctive relief under the Consumer Sales Practices Act individually and on behalf of the public as private attorneys general under R.C. 1345.09(D).

288. Plaintiffs are consumers who engaged in consumer transactions with Defendant because they reviewed the Website or Patient Portal and provided Defendant with their Private Information for purposes of locating and receiving medical services, and Defendant then used the information learned from these interactions to engage in commercial activities. Separately, a consumer transaction occurred each time Plaintiffs were targeted with advertisements for products and services belonging to Defendant or third parties.

289. Defendant is a supplier because it regularly supplies services to consumers like Plaintiffs for personal and/or family purposes. Furthermore, Defendant is a supplier because it secretly transmits its patients' Private Information to third parties for the purpose of effecting the solicitation of its patients with targeted advertising for commercial services by itself and third parties.

290. Defendant reprehensibly installed the Tracking Tools on its Web Properties to record, transmit, and profit from the Private Information of Ohio consumers without their knowledge or consent. This is unfair and unconscionable.

291. Separately, the failure to affirmatively disclose to its patients and website users that Private Information will be shared for commercial purposes with third parties is a deceptive omission.

292. Defendant's conduct described in this Complaint is immoral, inequitable, unethical, oppressive, likely to create a belief in the mind of a consumer that is not in accord with reality, and marked by injustice, partiality, and deception.

293. Plaintiffs and all other Ohio consumers continue to face a substantial risk of irreparable harm from Defendant's actions. Defendant is a major medical provider throughout the State of Ohio, where Plaintiffs reside. Depending on the type and severity of future illness or injury, Plaintiffs may be required to seek Defendant's medical services. An injunction would serve the public interest because Plaintiffs and other Ohio residents should not be forced to choose between receiving necessary medical services and maintaining the confidentiality of their Private Information.

294. Plaintiffs respectfully request the Court enter judgment declaring that Defendant has violated R.C. 1345.02(A) and R.C. 1345.03(A) by engaging in the acts and practices described herein.

295. Plaintiffs respectfully request that the Court enjoin Defendant from continuing to commit the unfair, deceptive, and unconscionable acts and practices described herein, and that it further award any other equitable relief deemed appropriate under R.C. 1345.09(D).

296. Plaintiffs respectfully request that the Court award attorneys' fees under R.C. 1345.09(F)(2) for Defendant's knowing violations of the CSPA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiffs and Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members:

D. For an award of damages exceeding $25,000, including, but not limited to, actual, consequential, statutory, punitive, and/or nominal damages, as allowed by law in an amount to be determined at trial;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For pre and post judgment interest on all amounts awarded at the highest rate allowed by law; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

DATE: October 12, 2023

Respectfully Submitted,

/s/ Dylan J. Gould
Terence R. Coates (0085579)
Dylan J. Gould (0097954)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Joseph M. Lyon (0076050)
Kevin M. Cox (0099584)
THE LYON FIRM

2754 Erie Ave.
Cincinnati, Ohio 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com
kcox@thelyonfirm.com

Jeffrey S. Goldenberg (0063771)
Todd B. Naylor (0068388)
Robert B. Sherwood (0084363)
GOLDENBERG SCHNEIDER, L.P.A.
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Telephone: (513) 345-8291
Facsimile: (513) 345-8294

Matthew R. Wilson (0072925)
MEYER WILSON, LPA
305 Nationwide Blvd.
Columbus, Ohio 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066
mwilson@meyerwilson.com

Bryan L. Bleichner*
Philip J. Krzeski (0095713)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Gary M. Klinger*
Glen L. Abramson*
Alexandra M. Honeycutt*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com
gabramson@milberg.com
ahoneycutt@milberg.com

Foster C. Johnson*
Justin Kenney*
AHMAD, ZAVITSANOS, & MENSING, P.C.
1221 McKinney Street, Suite 3460
Houston, Texas 77010
Telephone: (713) 655-1101
Facsimile: (713) 655-0062
fjohnson@azalaw.com
jkenney@azalaw.com

Counsel for Plaintiffs and the Putative Class

**pro hac vice* forthcoming

CERTIFICATE OF SERVICE

I hereby certify that on October 12, 2023, a copy of the foregoing was served via email on Defendant's counsel of record.

/s/ Dylan J. Gould
Dylan J. Gould (0097954)

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Up to $7M Christ Hospital Settlement Ends Class Action Lawsuit Over Alleged Data Sharing

---