IN THE COURT OF COMMON PLEAS
SUMMIT COUNTY, OHIO

JOHN DOE, Individually, and as Next Friend of A.D., B.D., and C.D., Minors, c/o Stranch, Jennings & Garvey, PLLC 223 Rosa L. Parks Ave., Ste 200 Nashville, TN 37203,	)	
and on behalf of all others similarly situated,	)	
Plaintiff,	)	**JURY DEMAND**
	)	**Case No. _____**
v.	)	
CHILDREN'S HOSPITAL MEDICAL CENTER OF AKRON D/B/A AKRON CHILDREN'S HOSPITAL, Registered Agent for Service of Process Christopher Gessner, One Perkins Square, Akron, Ohio 44308.	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff, JOHN DOE, Individually, and as Next Friend of A.D., B.D., and C.D., Minors, ("Plaintiff") and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant, CHILDREN'S HOSPITAL MEDICAL CENTER OF AKRON D/B/A AKRON CHILDREN'S HOSPITAL (hereinafter, "ACH" or "Defendant"), and alleges, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiff brings this class action to address Defendant's improper practice of

disclosing the confidential Personally Identifying Information ("PII")[1] and/or Protected Health Information ("PHI")[2] (collectively referred to as "Private Information") of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"),[3] Google, LLC ("Google"), TVSquared, LinkedIn, Cision, and Siteimprove, and potentially others via tracking technologies used on its website ("the Disclosure").

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

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

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

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

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

avoidable by and largely unknown to users."[5] OCR and FTC warn that "[i]mpermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others."[6]

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

4. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable

[5] *Id.*
[6] Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20, 2023) **Exhibit A.**

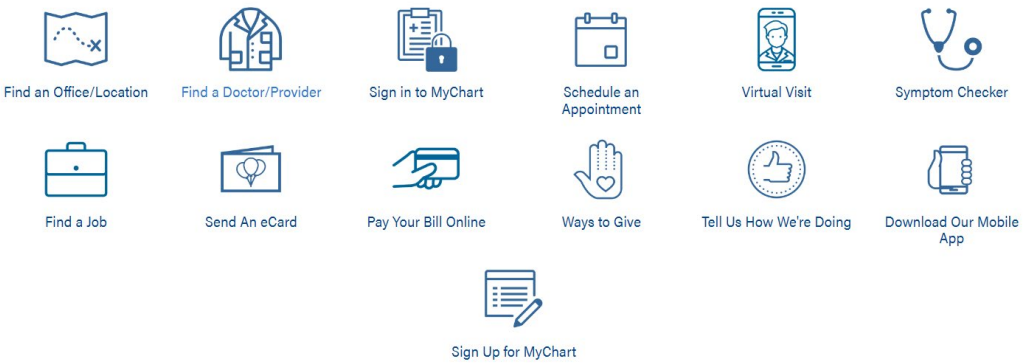
protected health information to a third party without express written authorization.

5. ACH is a hospital and medical system providing care to children which provides medical care to children in Akron and the surrounding region Northeastern Ohio, "[w]ith more than a million patient visits a year, [which is] leading the way to healthier futures for children through quality patient care, education, advocacy, community service and medical discovery."[7]

6. Despite its unique position as a massive and trusted healthcare provider, ACH knowingly configured and implemented into its website, https://www.akronchildrens.org/ (the "Website") code-based tracking devices known as "pixels" (also referred to as "trackers" or "tracking technologies"), which collected and transmitted patients' Private Information to Facebook and other third parties, without patients' knowledge or authorization.

7. Defendant encourages patients, and their parents, to use its Website, along with its various web-based tools and services (collectively, the "Online Platforms"), to research ACH via its main homepage, to find providers,[8] to search for medical conditions, treatment information, educational videos, departments, providers and more,[9] to research medical services,[10] to find health information,[11] to find locations,[12] to access a patient portal, MyChart, via a "pre-portal login page,"[13] and more:

[7] https://www.akronchildrens.org/pages/About-Us.html (last accessed November 17, 2023)
[8] https://www.akronchildrens.org/cgi-bin/providers/new_find_a_provider.pl (last acc. Nov. 17, 2023)
[9] See, e.g., search for "anxiety," avail. at https://www.akronchildrens.org/search-answers.html?query=anxiety&referrerPageUrl=https://www.akronchildrens.org/ (last acc. Nov. 17, 2023)
[10] See, e.g., "Services," "Departments and Programs," avail. at https://www.akronchildrens.org/pages/Medical-Services.html (last acc. Nov. 17, 2023)
[11] https://www.akronchildrens.org/Health-Info.html (last acc. Nov. 17, 2023)
[12] https://www.akronchildrens.org/cgi-bin/loc_search/new_search.pl#allLocs (last acc. Nov. 17, 2023)
[13] https://www.akronchildrens.org/pages/MyChart.html (last acc. Nov. 17, 2023)



14

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

9. A pixel (also referred to as a "tracker" or "tracking technology") is a snippet of code embedded into a website that tracks information about its visitors and their website interactions.[15] When a person visits a website with an embedded pixel, the pixel tracks "events" (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted.[16] Then, the pixel transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing.[17]

10. Among the trackers Defendant embedded into its Website is the Facebook Pixel (also referred to as the "Meta Pixel" or "Pixel"). By default, the Meta Pixel tracks information

[14] https://www.akronchildrens.org/ (last acc. Nov. 17, 2023)
[15] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[16] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[17] *Id.*

about a visitor's device, including their IP address, and the pages viewed.[18] When configured to do so, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[19] Additionally, the Meta Pixel can link a visitor's website interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to be linked with their Facebook profile.[20]

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

12. Facebook encourages and recommends use of its Conversions Application Programming Interface ("CAPI") alongside use of the Meta Pixel.[21]

13. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website

[18] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).
[19] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[20] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." What are Cookies?, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).
[21] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, How to Implement Facebook Conversions API (In Shopify), FETCH & FUNNEL https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[22, 23]

14. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[24]

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

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

17. The information that Defendant's Meta Pixel and possibly CAPI sent to Facebook can include the Private Information that Plaintiff and Class Members submitted to Defendant's Website, including details about the pages users browsed; users' paths of navigation through the Website; users' keyword searches including for doctors, medical conditions, and treatment; the buttons they clicked; and their identities.

---

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

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

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

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

19. In addition to the Facebook tracker and CAPI, on information and belief, Defendant installed other tracking technology which operate similarly to the Meta Pixel and transmit a website user's Private Information to other third parties.

20. Healthcare patients simply do not anticipate that their trusted healthcare provider will send Personal Health Information ("PHI") or other 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.

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

22. Despite willfully and intentionally incorporating tracking technology, including the Meta Pixel, potentially CAPI, and other tracking technology, into its Website and servers, ACH has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications and Private Information with third parties including Facebook, Google, TVSquared, LinkedIn, Cision, and Siteimprove, and possibly others.

23. Defendant further made express and implied promises to protect Plaintiff's and

Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendant, including in its privacy policies and elsewhere.

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

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

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

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

28. Plaintiff seeks to remedy these harms and brings causes of action for

(I) Breach of Confidence, Unauthorized Disclosure of Nonpublic Medical Information, pursuant to *Biddle v. Warren Gen. Hosp.,* 1999-Ohio-115, 86 Ohio St. 3d 395, 715 N.E.2d 518 (1999); (II) Negligence; (III) Negligence *Per Se*; (IV) Invasion of Privacy; (V) Breach of Implied Contract; (VI) Unjust Enrichment; and, (VII) Interception and Disclosure of Electronic Communications in Violation of R.C. § 2933.52.

PARTIES

29. Plaintiff, JOHN DOE, is a natural person and a resident and citizen of Ohio where he intends to remain, with a principal residence in Akron, Summit County, Ohio, and the father of A.D., B.D., and C.D., Minors.

30. Defendant, CHILDREN'S HOSPITAL MEDICAL CENTER OF AKRON D/B/A AKRON CHILDREN'S HOSPITAL ("ACH" or "Defendant") is a non-profit corporation organized and existing under the laws of the State of Ohio with its principal place of business at One Perkins Square, Akron, Ohio 44308 in Summit County.

31. ACH's Registered Agent for Service of Process is Christopher Gessner, One Perkins Square, Akron, Ohio 44308.

JURISDICTION & VENUE

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

33. This Court has personal jurisdiction over Defendant because it is incorporated under Ohio law, its principal place of business is in this State, and the acts and omissions giving rise to Plaintiff's claims occurred in this State.

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

COMMON FACTUAL ALLEGATIONS

A. Background

35. Founded in 1890, Defendant is a hospital and medical system based in Akron, Ohio, which "…is dedicated to improving the health of children through outstanding quality patient care, education, advocacy, community service and research."[25] ACH promises to:

1. To treat every child as we would our own.
2. To treat others as they would like to be treated.
3. To turn no child away for any reason.[26]

36. ACH includes two (2) children's hospitals, including Akron Children's Hospital Main Campus, 214 West Bowery Street, Akron, Ohio 44308; thirty-nine (39) pediatrician offices, four (4) urgent care centers, and fifty (50) primary and specialty care locations.[27,28]

37. Defendant represents having: 98,621 emergency room visits; 572,606 primary care visits; over 1.3 million total outpatient visits; 38,206 urgent care visits; having performed 17,898 surgeries; having 10,946 inpatient admissions.[29]

38. Defendant operates Primary Care/Pediatrician offices, Specialty Locations, Urgent Care centers, Emergency Care locations, Inpatient Hospitals, Health Centers, and School Health and Sports Health clinics across Ohio, in Akron, as well as in Alliance, Amherst, Ashland, Austintown, Barberton, Beachwood, Belpre, Boardman, Boston Heights, Brecksville, Canton, Cleveland, Concord, East Liverpool, East Palestine, Hudson, Lisbon, Lorain, Lowellville, Mansfield, Mantua, Marietta, Massillon, Mayfield Heights, Medina, Millersburg, Mount Eaton, New Philadelphia, North Canton, Norwalk, Oberlin, Peninsula, Ravenna, Sagamore Hills,

[25] https://www.akronchildrens.org/pages/About-Us.html (last acc. Nov. 17, 2023).
[26] *Id*.
[27] *Id*.
[28] https://www.akronchildrens.org/locations/Akron-Childrens-Hospital.html (last acc. Dec. 19, 2023).
[29] https://www.akronchildrens.org/pages/About-Us.html (last acc. Dec. 19, 2023).

Sandusky, Sebring, Stow, Streetsboro, Tallmadge, Twinsburg, Wadsworth, Warren, Windham, Wooster, and Youngstown, Ohio.[30]

39. At these locations, ACH provides medical services in numerous departments and programs, including: Emergency Medicine; Surgery (including General Surgery, Bariatric Surgery, Cardiovascular Surgery, Neurosurgery, and Plastic and Reconstructive Surgery); Pediatrics; Addiction Services Program; Adolescent and Young Adult Cancer Program; Adolescent Medicine; Adoptive Health Services; Adult Congenital Heart Service; Akron Children's Health Collaborative; Akron Children's Home Care; Allergy and Immunology; Anesthesiology; Arrhythmia Center; Audiology; Augmentative and Alternative Communication Program; Autism Diagnostic Clinic; Behavioral Health; Behavioral Sleep Medicine; Bowel Management Program; Brachial Plexus Treatment; Brain Tumor Program; Breastfeeding and Lactation Program; Burn Center; Cancer and Blood Disorders; Cancer Survivorship Program; Cardiac Neurodevelopmental Follow-Up Program; Cardiology; CARE Center (Child Abuse); Chaplaincy Services; Children's Home Care; Chronic Care Education and Support; Clubfoot Clinic; Cochlear Implant Program; Community Outreach; Contact Lens Program; Cosmetic & Reconstructive Laser Program; Cranio-Orbital Meeting; Craniofacial Center; Critical Care Medicine (PICU); Cystic Fibrosis Center; Day Rehabilitation Program; Deformational Plagiocephaly Clinic; Dental Clinic; Dermatology; Developmental and Behavioral Pediatrics; Diabetes Services; Down Syndrome Program; Ear Molding Clinic; Ear, Nose and Throat; Eating Disorder Program; Endocrinology; Eosinophilic Esophagitis Clinic; Epilepsy Program; Expressive Therapy; Eye Care; Family Child Learning Center; Family Library; Feeding Disorders Program; Fetal Cardiology; Fetal Treatment Center; Fracture Clinic; Gastroenterology; Gender Affirming

[30] https://www.akronchildrens.org/cgi-bin/loc_search/new_search.pl#allLocs (last acc. Nov. 17, 2023)

Medicine; Genetics; Hand and Upper Extremity Clinic; Hand Therapy; Head Injury Clinic; Headache Clinic; Healthy Active Living; Heart Center; Hemostasis and Thrombosis Center; Hereditary Cancer Program; High-Risk Pregnancy; Hospital Medicine; Hypertension Clinic; In-Home Speech Therapy Services; Infant Safety; Infant Therapy; Infectious Disease; Infusion and Sedation Center; Injury Prevention; Inpatient Psychiatry; Inpatient Rehabilitation Program; Intensive Outpatient Program; Interventional Radiology; Kidney Stone Clinic; Laboratory Services; Lead Clinic; Locust Pediatric Care Group; Maternal Fetal Medicine; Metabolic Disorders Clinic; Mitochondrial Center; Motility Program; Motion Analysis Lab; Myelo Clinic; Neonatal and Perinatal Medicine; Neonatal Follow-Up Clinic; Neonatology; Nephrology; Neurobehavioral Health; NeuroDevelopmental Science Center; Neurofibromatosis (NF) Clinic; Neurology; Neuromuscular Clinic; Nurturing Families Program; Nutrition Services; Occupational Therapy; Operational Excellence; Ophthalmology; Orthopedics; Osteogenesis Imperfecta Clinic; Pain Center; Palliative Care; Partial Hospitalization Program; Pharmacy; Physical Medicine and Rehabilitation; Physical Therapy; Psychology and Psychiatry; Pulmonary Medicine; "Quick Care;" Radiology; Rehabilitative Services; Rheumatology; School Health Services; School Success; Scleral Lens Clinic; Sedation Services; Sickle Cell Program; Single Ventricle Program; Skeletal Dysplasia Center; Sleep Medicine; Spasticity Clinic; Speech Resonance Clinic; Speech Therapy; Spine Center; Sports Health; Sports Medicine; Sports Orthopedics; Sports Rehab; Stem Cell Transplant Program; Syncope Clinic; Thyroid Program; Tic and Tourette Service; Transport Services; Tuberous Sclerosis Clinic; Turner Syndrome Center; Urgent Care; Urology; Uveitis Clinic; Vascular Anomalies Clinic; Vasculitis Clinic; Vision Center; and Youth Programs.[31]

40. ACH serves many of its patients via its Website and Online Platforms, which it

[31] https://www.akronchildrens.org/pages/Medical-Services.html (last acc. Nov. 17, 2023)

encourages patients, and their parents, to use its Website, along with its various web-based tools and services (collectively, the "Online Platforms"), to research ACH via its main homepage, to find providers,[32] to search for medical conditions, treatment information, educational videos, departments, providers and more,[33] to research medical services,[34] to find health information,[35] to find locations,[36] to access a patient portal, MyChart, via a "pre-portal login page,"[37] and more.

41. In furtherance of its goal of increasing sales and profitability, and to improve the success of its advertising and marketing, Defendant purposely installed the Meta Pixel and other trackers onto its Website, for the purpose of gathering information about Plaintiff and Class Members to further its marketing efforts. But Defendant did not only generate information for its own use: it also shared patient information, including Private Information belonging to Plaintiff and Class Members, with Facebook and other unauthorized third parties.

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

i. Facebook's Business Tools and the Meta Pixel

43. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[38]

[32] https://www.akronchildrens.org/cgi-bin/providers/new_find_a_provider.pl (last acc. Nov. 17, 2023)
[33] See, e.g., search for "anxiety," avail. at https://www.akronchildrens.org/search-answers.html?query=anxiety&referrerPageUrl=https://www.akronchildrens.org/ (last acc. Nov. 17, 2023)
[34] See, e.g., "Services," "Departments and Programs," avail. at https://www.akronchildrens.org/pages/Medical-Services.html (last acc. Nov. 17, 2023)
[35] https://www.akronchildrens.org/Health-Info.html (last acc. Nov. 17, 2023)
[36] https://www.akronchildrens.org/cgi-bin/loc_search/new_search.pl#allLocs (last acc. Nov. 17, 2023)
[37] https://www.akronchildrens.org/pages/MyChart.html (last acc. Nov. 17, 2023)
[38] Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

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

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

46. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[39] Businesses that want to target customers and advertise their services, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[40]

47. One such Business Tool is the Meta Pixel, a tool that "tracks the people and type of actions they take."[41] When a user accesses a webpage that is hosting the Meta Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook—traveling from the user's browser to Facebook's server.

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

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

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

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

(such as Defendant's "Find-a-Provider page[42]).

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

50. Facebook's own website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[44]

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

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** (emphasis added).
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
>
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[45]

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

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.

[42] https://www.akronchildrens.org/cgi-bin/providers/new_find_a_provider.pl (last acc. Nov. 17, 2023)
[43] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[44] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).
[45] Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.

- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[46]

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

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

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

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

56. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.[47]

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

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

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

embedded inside the URL and can include cookies.

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

59. 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.

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

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

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

63. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. To counteract this, third parties bent on gathering data and Private Information implement workarounds that are difficult to detect or evade. Facebook's workaround is its Conversions API tool, which is particularly effective because the data transmitted via this tool does not rely on the website visitor's web browsers. Rather, the information travels directly from the entity's server to Facebook's server.

64. Conversions API "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[48] Thus, the entity receives and stores its communications with patients on its server before Conversions API collects and sends those communications—and the Private Information contained therein—to Facebook.

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

66. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the host server, Facebook instructs companies like Defendant to "[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website events [with Facebook] that the pixel may lose."[49] Thus, if an entity implemented the Meta Pixel in accordance with Facebook's documentation, it is also reasonable to infer that it implemented the Conversions API tool on its Website.

67. The third parties to whom a website transmits data through pixels and other tracking technology do not provide any substantive content on the host website. In other words, Facebook

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

and others like it are not providing anything to the user relating to the user's communications. Instead, these third parties are typically procured to track user data and communications only to serve the marketing purposes of the website owner (i.e., to bolster profits).

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

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

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

71. ACH also employed other trackers, Google Analytics with Google Tag Manager, TVSquared, LinkedIn, Cision, and Siteimprove, which, on information and belief, likewise transmitted Plaintiff's and the Class Members' Private Information to third parties without Plaintiff's and Class Members' knowledge or authorization.

iii. Defendant Violated its own Privacy Policies

72. ACH maintains and is covered under privacy policies, including its Notice of Privacy Practices,[50] and a website Terms and Conditions,[51] which are posted on Defendant's

[50] Akron Children's Hospital, Notice of Privacy Practices, effective September 23, 2013, available at https://www.akronchildrens.org/pages/Privacy-Policy.html (last acc. Nov. 17, 2023), **attached as Exhibit B.**

[51] Akron Children's Hospital, Terms and Conditions, avail. at https://www.akronchildrens.org/pages/Terms-of-Use.html (last acc. Nov. 17, 2023**), attached as Exhibit C.**

website (collectively "Privacy Policies").

73. On information and belief, Defendant does not maintain any other privacy policy concerning its Website.

74. In its Notice of Privacy Practices, ACH states, "**[t]his notice describes how medical information about you may be used and disclosed and how you can get access to this information.**"[52]

75. Defendant's Notice of Privacy Practices applies to "[a]ll of our hospitals, employed physicians, doctors' offices, entities, foundations, facilities, home care programs, other services and affiliated facilities…" as set forth therein, *to wit*:

- Akron Children's Hospital Akron Campus
- Akron Children's Hospital Beeghly Campus
- Akron Children's Hospital Pediatrics (ACHP)
- Children's Home Care Group
- Family Child Learning Center
- Inpatient locations including Akron Children's at East Liverpool City Hospital, MedCentral Hospital, Robinson Memorial Hospital, Aultman Hospital
- Pediatric Emergency Services at Akron General Wellness Center (Montrose) and Children's at Hudson
- Neonatal Intensive Care Units at Akron General Medical Center, Summa Akron City Hospital,
- St. Elizabeth Health Center
- Maternal Fetal Medicine at Summa Health System, Akron General Medical Center, Mercy Medical Center, Wooster Community Hospital
- Specialty Office locations in Beachwood, Boardman, Hudson, Medina and at Fisher-Titus Medical Center in Norwalk, MetroHealth System in Cleveland and TriPoint Medical Center in Concord.
- Find all Akron Children's locations at akronchildrens.org/locations.[53]

76. In the Notice of Privacy Practices, ACH states its "pledge" that:

> …[W]e believe your health information is personal. We keep records of the care and services you receive at our facilities. **We are committed to keeping your**

[52] Notice of Privacy Practices, **Exhibit B** (bold emphasis in original).
[53] *Id*.

> **health information private, and we are also required by law to respect your confidentiality**.
>
> This Notice describes the privacy practices of Akron Children's and its affiliated facilities. This Notice applies to all health records that Akron Children's maintains about you. If you are under 18 years of age, your parents or guardian must sign for you and handle your privacy rights for you. **We are legally required to give you this Notice, to notify you if there is a breach of your protected health information and to follow the terms of this Notice, which may be amended from time to time**.[54]

77. In its Notice of Privacy Practices, ACH represents, and promises that:

> **Marketing Activities.** We may use your health information for marketing purposes without your authorization only when we discuss such products or services with you face to face or provide you with a gift of nominal value related to the product or service. For other types of marketing activities, we will obtain your written authorization. We will not sell your name or other information to others. [55]

78. Further, in the Notice of Privacy Practices, Defendant enumerates how it may use and disclose health information outside of ACH, including for treatment; to facilitate payment; for Health Care Operations ("…to maintain and improve patient care…"); to Business Associates who perform services for ACH, in which case the Business "Associate must agree in writing to protect the confidentiality of the information."); to contact patients; for fundraising; for Health-Related Services ("We may use and disclose health information about you to send you mailings about health-related products and services available at Akron Children's"); to individuals involved in patient care or payment for care; for Patient Information Directories; and for research.[56]

79. In addition, ACH's Notice of Privacy Practices provided for other uses and disclosures of PHI as required or permitted by law, including Health Oversight Activities; to law enforcement "if we receive a court order, subpoena, summons, warrant or similar process; to

[54] *Id*.
[55] *Id*. (bold emphasis in original; underline emphasis added).
[56] *Id*.

identify or locate a suspect, fugitive, material witness or missing person; when the patient is the victim of a crime if we are unable to obtain the person's agreement; when we believe the patient's death may be the result of criminal conduct; if there is suspected criminal conduct at any of our facilities; and in emergency circumstances to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime"); in legal matters; with medical examiners or coroners; as required by military command authorities for members of the armed forces and veterans; in connection with organ and tissue donations; and for Public Health Activities. [57]

80. None of the above purposes enumerated in ACH's Notice of Privacy Practices permit Defendant to disclose patients' PHI/Private Information to third-parties for marketing purposes without their written authorization.

81. In fact, in the Notice of Privacy Practices, Defendant reiterates that:

> As described above, we will use your health information and disclose it outside Akron Children's for treatment, payment, healthcare operations, and when permitted or required by law. **We will not use or disclose your health information for other reasons without your written authorization. For example, most uses and disclosures of […] marketing require your authorization.**[58]

82. In addition, Defendant maintains Terms and Conditions applicable to the use of its Website, which states, "[a]ll visitors to Akron Children's Hospital's website are being provided access to the site, free of charge, subject to the following terms and conditions:" [59]

83. Defendant's Terms and Conditions fail to notify Website users and patients that ACH utilizes the Meta Pixel and other tracking technologies to disclose PHI/Private Information to third parties such as Facebook for marketing purposes without their consent.

---

[57] *Id*.
[58] *Id*. (bold emphasis added).
[59] Akron Children's Hospital, Terms and Conditions, **Exhibit C.**

84. In fact, in the Terms and Conditions, ACH states:

> Do not send Akron Children's Hospital confidential or proprietary information. Any feedback, data, answers, questions, comments, suggestions, ideas, or the like that you send to Akron Children's will be treated as being non-confidential and nonproprietary, and you agree that any such information you choose to provide may be reproduced, used and distributed by Akron Children's Hospital for any purpose without restriction.[60]

85. Nothing in ACH's website Terms and Conditions permits Defendant to disclose Private Information to third-parties for marketing purposes without their written authorization.

86. Despite these express, specific representations and promises, ACH does indeed transfer Private Information to third parties. Using the Meta Pixel, Defendant used and disclosed Plaintiff's and Class Member's Private Information and confidential communications to Facebook, and other unauthorized third parties, without written authorization, in violation of its Privacy Policies.

iv. ACH Unauthorizedly Disclosed Plaintiff's and the Class's Private Information

87. Defendant disclosed Plaintiff's and Class Members' Private Information and confidential communications to third parties for marketing purposes, including Facebook, Google, TVSquared, LinkedIn, Cision, and Siteimprove.

88. Through its use of the Meta Pixel, installed via Google Tag Manager, as of March 2023 if not thereafter, ACH disclosed to Facebook Plaintiff's and Class Members' Private Information communicated via its Website, including details about the pages users browsed; users' paths of navigation through the Website; users' keyword searches including for doctors, medical conditions, and treatment; the buttons they clicked; and their identities.

ACH Shared Users' Browsing Details

89. ACH disclosed users' browsing details to Facebook. From the moment a user

[60] *Id*.

arrived on ACH's homepage, ACH began its tracking and disclosures about the user by sending PageView and Microdata events. Meta Pixel PageView and Microdata events disclose the URLs of pages that users viewed. For example, both the PageView and Microdata events transmitted upon the user loading ACH's homepage disclose that the user was on "www.akronchildrens.org."

90. In addition to the URL of the page that the user was on, Microdata events also include additional details about pages that users viewed, such as the page title and open graph description. As an example, the Microdata event transmitted upon the user's arrival on the ACH homepage discloses the page's title, "For Families & Patients | Akron Children's Hospital" and the open graph data, "Akron Children's Hospital."

91. ACH continued to track and share information about users' browsing activities as users moved beyond the homepage to view other content such as ACH's patient portal[61] and medical services.[62]

92. When a user navigated from the homepage to browse ACH's page about its patient portal (the "Patient Portal Landing Page"), for example, ACH disclosed that activity through a pair of PageView and Microdata events. Both events reveal that the user was on a page with the URL, "https://www.akronchildrens.org/pages/MyChart.html," and that the user navigated to that page from the homepage, "akronchildrens.org." Moreover, the Microdata event also provides Facebook the title of the page that the user was viewing, "MyChart – Secure. Access. Anywhere. | Akron Children's Hospital."

93. Similarly, when the user navigated to the Medical Services page from the homepage, ACH transmitted another set of PageView and Microdata events. The events here also

[61] https://www.akronchildrens.org/pages/MyChart.html (last acc. Nov. 17, 2023)
[62] See, e.g., "Services," "Departments and Programs," avail. at https://www.akronchildrens.org/pages/Medical-Services.html (last acc. Nov. 17, 2023)

disclose the user's path of navigation, revealing that the user navigated to the page about the "Departments & Programs | Akron Children's Hospital," at the URL, https://www.akronchildrens.org/pages/Medical-Services.html from the homepage, "akronchildrens.org."

94. On information and belief, ACH disclosed information about the user's activities as the user interacted further with the Medical Services page.

95. For instance, as of December 7, 2023, the user could select "Addiction Services Program," to learn more about ACH's addiction services. Because ACH previously had Automatic Setup configured, enabling SubscribedButtonClick events, ACH would likely have sent a SubscribedButtonClick event upon the user's click to view the Addition Services Program page. Next, upon the loading of the Addiction Services Program page, ACH would also likely have sent a pair of PageView and Microdata events. The pair of events would have disclosed that the user navigated to the page on "https://www.akronchildrens.org/departments/Addiction-Services-Program.html," after viewing a page on "https://www.akronchildrens.org/pages/Medical-Services.html." The Microdata event would have included the detail that the user was viewing a page with the title, "Addiction Services Program | Akron Children's Hospital."

ACH Shared Users' Search Activities, including Keywords and Medical Providers

96. In addition to details about the users' browsing details, ACH also disclosed details about users' search activities.

97. Users could conduct keyword searches as well as searches for medical practitioners on ACH's website. ACH reported details about both types of user search activities to Facebook.

98. For instance, when the user searched for the keyword, "anxiety," ACH reported that activity via PageView and Microdata events, in which both events disclose that the user

searched for the "query=anxiety." The Microdata event also discloses that the user was viewing a page with the title, "Akron Children's Hospital Answers | Facilities, Providers, FAQs, Departments | Ask any question to find the answer you need from Akron Children's Hospital today."

99. ACH also disclosed when the user navigated to find a medical provider at ACH.

100. Upon the user loading the Find a Doctor or Provider page, ACH sent a pair of PageView and Microdata events, which both disclose that the user was on the page, "https://www.akronchildrenms.org/cgi-bin/providers/new_find_a_provider.pl."

101. The Microdata event also provides additional details, such as the title of the page that the user was viewing, "Find a Doctor, Provider, Pediatrician at Akron Children's Hospital," as well as the page description, "Staff Directory: Find a Doctor, Provider, Pediatrician by name or department at Akron Children's Hospital."

102. Based on ACH's pattern of sending PageView and Microdata events, on information and belief, ACH continued to send information to Facebook about the user's search related activities if the user used the medical provider search. For instance, as of December 7, 2023, the user could click to view pediatric neurologist, Abdalla Abdalla, MD's profile from the medical provider search page. The PageView and Microdata events that ACH would have sent would include the URL, "https://www.akronchildrens.org/people/Abdalla-Abdalla.html. Furthermore, the Microdata event would also include the page's title, e.g., "Abdalla Abdalla, MD | Akron Children's Hospital."[63]

103. In addition to this information, the Meta Pixel collects and transmits to Facebook other identifying information. As a general matter, users' "c_user" cookies, which Facebook uses to identify users, are transmitted in Meta Pixel events. Therefore, the Meta Pixel events ACH sent

[63] https://www.akronchildrens.org/people/Abdalla-Abdalla.html

likely allowed for Facebook to connect users' identities with the details reported within the events.

104. Upon information and belief, Defendant also transmitted IP address information, browser and device information, and, if applicable, a person's Facebook ID.

105. As explained above, the Meta Pixel collects and packages Private Information, gathered from Defendant's Website, and transmits it to Facebook.

106. After receiving this information from Defendant, Facebook processes it, analyzes it, and assimilates it into its own massive datasets, before selling access to this data in the form of targeted advertisements. Employing "Audiences"—subsections of individuals identified as sharing common traits—Facebook promises the ability to "find the people most likely to respond to your ad."[64] Advertisers can purchase the ability to target their ads based on a variety of criteria: "Core Audiences," individuals who share a location, age, gender, and/or language;[65] "Custom Audiences," individuals who have taken a certain action, such as visiting a website, using an app, or buying a product bought a product;[66] and/or "Lookalike Audiences," groups of individuals who "resemble" a Custom Audience, and who, as Facebook promises, "are likely to be interested in your business because they're similar to your best existing customers.[67]

107. As of December 3, 2023, ACH employed trackers of Google Analytics with Google Tag Manager, TVSquared, LinkedIn, Cision, and Siteimprove.

108. Google and other companies process data in a similar manner and use it to build marketing and other data profiles allowing for targeted advertising.

109. Defendant could have chosen not to use the Meta Pixel, or it could have configured

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

it to limit the information that it communicated to third parties, but it did not. Instead, it intentionally selected and took advantage of the features and functionality of the Pixel that resulted in the Disclosure of Plaintiff's and Class Members' Private Information.

110. Along those same lines, Defendant could have chosen not to use other tracking technologies such as Google Analytics with Google Tag Manager, TVSquared, LinkedIn, Cision, and Siteimprove to track Plaintiff and Class Members private communications and transmit that information to unauthorized third parties. It did so anyway, intentionally taking advantage of these trackers despite the harm to Plaintiff's and Class Members' privacy.

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

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

113. Plaintiff and the Class Members never consented, agreed, authorized, or otherwise permitted Defendant ACH to intercept their communications or to use or disclose their Private Information for marketing purposes. Plaintiff and the Class were never provided with any written notice that Defendant disclosed its patients' Protected Health Information to Facebook and others, such as Google, TVSquared, LinkedIn, Cision, and Siteimprove, nor were they provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiff's Protected Health Information to unauthorized entities.

114. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes

only, and to make only authorized disclosures of this information.

115. Furthermore, Defendant actively misrepresented that it would preserve the security and privacy of Plaintiff's and Class Members' Private Information. In actuality, Defendant shared data about Plaintiff's and Class Members' activities on the Online Platforms alongside identifying details about the Plaintiff and Class Members, such as their IP addresses.

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

B. Plaintiff's Experience

117. Plaintiff John Doe's children, A.D., B.D., and C.D. have been patients of Defendant since 2007, each receiving healthcare services from ACH and physicians in ACH's network for medical conditions including endocrine medical issues, gastrointestinal conditions, and for primary care treatment. A.D., B.D., and C.D. have been treated at ACH's main campus, Akron Children's Pediatrics—Akron East, and ACH's allergy testing center.

118. Plaintiff John Doe relied on ACH's Website and Online Platforms to communicate confidential patient information relating to A.D., B.D., and C.D., beginning in 2007, and last in 2023, including to search for endocrine and gastrointestinal doctors for A.D., B.D., and C.D.; to search for information on "IBS," (Irritable Bowel Syndrome), to search for a neurodevelopmental

center, and to search for and research medical treatments. He also utilized Defendant's patient portal to make appointments, communicate with doctors, and request medications for his minor children, A.D., B.D., and C.D.

119. Plaintiff John Doe accessed Defendant's Website and Online Platforms at Defendant's direction and encouragement on behalf of A.D., B.D., and C.D. Plaintiff reasonably expected that his online communications with ACH were confidential, solely between himself and ACH, and that, as such, those communications would not be transmitted to or intercepted by a third party.

120. Plaintiff provided his and A.D.'s, B.D.'s, and C.D.'s Private Information to Defendant and trusted that the information would be safeguarded according to ACH's Privacy Policies and the law.

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

a. Plaintiff's and A.D.'s, B.D.'s, and C.D.'s identities;

b. Plaintiff's seeking of medical treatment for A.D., B.D., and C.D.;

c. A.D.'s, B.D.'s, and C.D.'s statuses as patients;

d. Plaintiff's browsing activities on the Online Platforms;

e. The pages Plaintiff visited for A.D., B.D., and C.D., such as the patient portal and for medical services, the content Plaintiff viewed, and activities on those pages;

f. Plaintiff's searches for doctors for A.D., B.D., and C.D.;

g. The doctors Plaintiff viewed for A.D., B.D., and C.D.; and,

h. A.D.'s, B.D.'s, and C.D.'s health conditions and the treatment Plaintiff searched for on behalf of his children.

122. By failing to receive the requisite consent, ACH breached confidentiality and unlawfully disclosed Plaintiff's and A.D.'s, B.D.'s, and C.D.'s Private Information.

123. Plaintiff first discovered that Defendant was using the Meta Pixel and other tracking technologies to gather and disclose his and A.D.'s, B.D.'s, and C.D.'s Private Information in December of 2023.

124. As a result of ACH's Disclosure of Plaintiff's and A.D.'s, B.D.'s, and C.D.'s Private Information via the Meta Pixel and other tracking technologies to third parties without authorization, he now receives targeted health-related advertisements reflecting their private medical treatment information.

125. Plaintiff paid ACH for medical services for A.D., B.D., and C.D., and the services he paid for included reasonable privacy and data security protections for his and his children's Private Information, but Plaintiff did not receive the privacy and security protections for which he paid, due to Defendant's Disclosure.

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

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

127. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party

developers to access this data.[68] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

128. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective . . . at preventing the receipt of sensitive data."[69]

129. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[70] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook,

[68] Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.
[69] New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.
[70] Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.

as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[71]

130. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[72]

131. Furthermore, in June 2022, an investigation by The Markup[73] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[74] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[75] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[76]

132. During its investigation, The Markup found that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article

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

found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[77]

133. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the Meta Pixel inside their password-protected patient portals.[78]

134. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals capturing and sharing patient data in this way.[79]

D. Defendant Violated HIPAA Standards

135. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[80]

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

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

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to

[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

> 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.[81]

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

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written 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).[82]

139. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology.[83]

140. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[84]

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

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies**

[81] U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.
[82] U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.
[83] *See* U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html.
[84] *Id.*

> **in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules**. For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [85]

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

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

143. The Federal Trade Commission ("FTC") has also recognized that implementation of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[86]

144. On July 20, 2023, the FTC and HHS sent a "joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online activities."[87]

---

[85] *Id.* (emphasis in original) (internal citations omitted).
[86] Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **Exhibit A.**
[87] FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks

145. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules"[88] and that "[t]his is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes."[89]

146. Entities that are not covered by HIPAA also face accountability for disclosing consumers' sensitive health information under the Health Breach Notification Rule. 16 C.F.R. § 318. This Rule requires that companies dealing with health records notify the FTC and consumers if there has been a breach of unsecured identifiable health information, or else face civil penalties for violations. *Id*. According to the FTC, "a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, *including sharing of covered information without an individual's authorization*, triggers notification obligations under the Rule."[90]

147. Additionally, the FTC Act makes it unlawful to employ "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" 15 U.S.C. § 45(a). According to the FTC, "the disclosure of [sensitive health] information without a consumer's authorization can, in some circumstances, violate the FTC Act

---

from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.

[88] *Id.*

[89] *Id.*

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

as well as constitute a breach of security under the FTC's Health Breach Notification Rule."[91]

148. As such, the FTC and HHS have expressly stated that conduct like Defendant's runs afoul of the FTC Act and/or the FTC's Health Breach Notification Rule.

F. Defendant Violated Industry Standards

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

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

151. 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).

152. 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.

[91] *See, e.g.,* U.S. v. Easy Healthcare Corp., Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legallibrary/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; In the Matter of BetterHelp, Inc., FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; U.S. v. GoodRx Holdings, Inc., Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; In the Matter of Flo Health Inc., FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/casesproceedings/192-3133-flo-health-inc.

153. AMA Code of Medical Ethics Opinion 3.3.2 provides:

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

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

154. At all times when Plaintiff and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial marketing and sales purposes, unrelated to patient care.

H. IP Addresses are Personally Identifiable Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

167. The data concerning Plaintiff and Class Members, collected and shared by Defendant, has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook,

are the "people most likely to respond to your ad."[92] Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain online content.[93] Facebook's "Lookalike Audiences" go further, targeting individuals who resemble current customer profiles and whom, according to Facebook, "are likely to be interested in your business."[94]

168. Data harvesting is big business, and it drives Facebook's profit center, its advertising sales. In 2019, Facebook generated nearly $70 billion dollars in advertising revenue alone, constituting more than 98% of its total revenue for that year.[95]

169. This business model is not limited to Facebook. Data harvesting one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

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

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

lucrative and a significant risk to privacy.[96]

171. 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."[97]

TOLLING, CONCEALMENT, AND ESTOPPEL

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

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

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

175. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. ACH's illegal interception and disclosure of Plaintiff's and A.D.'s, B.D.'s, and C.D.'s Private Information has continued unabated, at least up until March 2023 if not later. What is more, ACH was under a duty to disclose the nature and

[96] *See* Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry, TIME, (Jan. 9, 2017 at 9:00 a.m.) https://time.com/4588104/medical-data-industry/.
[97] *See* Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

significance of their data collection practices but did not do so. ACH is therefore estopped from relying on any statute of limitations defenses.

CLASS ALLEGATIONS

176. Plaintiff brings this statewide class action individually, and as Next Friend of A.D., B.D., and C.D. (hereinafter, collectively, "Plaintiff") and on behalf of all other similarly situated persons.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

i. whether Defendant intentionally and/or negligently or recklessly breached its duty of confidence to Plaintiff and Class Members by disclosing their nonpublic medical information, Private Information, to third parties;

j. whether Defendant breached its duties of care to Plaintiff and the Class Members and was negligent;

k. whether Defendant's conduct amounts to negligence per se;

l. whether Defendant committed invasion of privacy;

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

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

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

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

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

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

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

187. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

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

190. Further, Defendant has acted or refused to act on grounds generally applicable to the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

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

a. whether Defendant owed a legal duty to Plaintiff and the Class Members to not disclose their nonpublic medical information, Private Information, to third parties without Plaintiff's or the Class Members' informed consent or other legal privilege;
b. whether Defendant disclosed Plaintiff's and the Class Members' nonpublic medical information, Private Information, to third parties without their informed consent or applicable legal privilege;
c. whether Defendant intentionally and/or negligently or recklessly breached its duty of confidence to Plaintiff and Class Members by disclosing their nonpublic medical

information, Private Information, to third parties;

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

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

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

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

h. whether Defendant breached the implied contract;

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

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

k. whether Defendant committed an invasion of privacy;

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

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

COUNT I
BREACH OF CONFIDENCE,
UNAUTHORIZED DISCLOSURE OF NONPUBLIC MEDICAL INFORMATION,
BIDDLE V. WARREN GENERAL HOSPITAL
(On Behalf of Plaintiff and the Class)

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

193. In Ohio, medical providers have a duty to their patients to keep any nonpublic medical information learned within the physician-patient relationship confidential, and to not disclose this information to third parties without a patient's informed consent or other applicable legal privilege entitling the provider to do so.

194. Defendant had the duty to its patients, Plaintiff and the Class Members, to keep confidential their Private Information, including PHI, and their communications which were transmitted via the Website and Online Platforms, and to not disclose this nonpublic medical information to third parties uninvolved in their treatment without their authorization or applicable legal privilege.

195. In light of this well-known duty of confidentiality owed by medical providers, Plaintiff and the Class Members had reasonable expectations of privacy in their Private Information and communications when interacting with Defendant through the Online Platforms.

196. Defendant intentionally and/or negligently, or recklessly, breached its duty of confidentiality to Plaintiff and the Class Members by disclosing their Private Information and confidential communications to third parties, including Facebook, via the Meta Pixel and related tracking technologies, without Plaintiff's or the Class Members' consent.

197. As a direct and proximate result of Defendant's breaches of confidence in unauthorizedly disclosing Plaintiff's and the Class Members' patient Private Information to third parties, Plaintiff and the Class Members suffered injury and damages, including, without

limitation, unauthorized access of their Private Information by third parties; improper disclosure of their Private Information; monetary damages; inappropriate advertisements and use of their Private Information for advertising purposes; increased risk of future harm; embarrassment, humiliation, frustration, and emotional distress; lost value of their Private Information; lost benefit of their bargain; and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendant's breaches of confidence.

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

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

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

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

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

202. Private Information is highly valuable, and Defendant knew, or should have known,

the harm that would be inflicted on Plaintiff and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendant by way of data harvesting, advertising, and increased sales.

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

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

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

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

and C.D., and the Class.

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

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

208. Plaintiff alleges this negligence *per se* theory as alternative to his other negligence claim.

209. Pursuant to the laws set forth herein, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, Defendant was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Private Information.

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

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

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

213. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiff's and Class Members' PII and PHI in compliance with applicable laws would result in an unauthorized third-party such as Facebook gaining access to

Plaintiff's and Class Members' PII and PHI, resulting in Defendant's liability under principles of negligence *per se*.

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

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

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

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

218. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' PII and PHI, and as a result, Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek actual, compensatory, and

punitive damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence *per se*.

COUNT IV
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

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

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

221. Plaintiff and Class Members communicated sensitive PHI and PII—Private Information—that they intended for only Defendant to receive and that they understood Defendant would keep private.

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

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

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

225. Plaintiff and Class Members have been damaged as a direct and proximate result

of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

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

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

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

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

229. As a condition of receiving medical care from Defendant, Plaintiff and the Class provided their Private Information and paid compensation for the treatment received, a portion of which was for data security. In so doing, Plaintiff and Class Members entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Policies and elsewhere, to "notify [them] if there is a breach of [their] protected health information" and not to disclose their PHI/Private Information for marketing purposes without written authorization and not to sell their names or other information to others.[98]

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

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

[98] Notice of Privacy Practices, **Exhibit B.**

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

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

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

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

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

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

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

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

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

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

contract claim.

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

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

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

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

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

246. ACH should be compelled to disgorge into a common fund for the benefit of

Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the unauthorized Disclosure alleged herein.

COUNT VII
INTERCEPTION AND DISCLOSURE OF ELECTRONIC COMMUNICATIONS IN VIOLATION OF R.C. § 2933.52
(on behalf of Plaintiff and the Class)

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

248. Under R.C. § 2933.65(A):

> A person whose wire, oral, or electronic communications are intercepted, disclosed, or intentionally used in violation of sections 2933.51 to 2933.66 of the Revised Code may bring a civil action to recover from the person or entity that engaged in the violation any relief that may be appropriate and that includes, but is not limited to, the following:
>
> (1) The preliminary and other equitable or declaratory relief that is appropriate;
>
> (2) Whichever of the following is greater:
>
> (a) Liquidated damages computed at a rate of two hundred dollars per day for each day of violation or liquidated damages of ten thousand dollars, whichever is greater;
>
> (b) The sum of actual damages suffered by the plaintiff and the profits, if any, made as a result of the violation by the person or entity that engaged in the violation.
>
> (3) Punitive damages, if appropriate;
>
> (4) Reasonable attorney's fees and other litigation expenses that are reasonably incurred in bringing the civil action.

249. Plaintiff and Class Members are individuals, and Defendant is a corporation, and all parties to this action are "persons" within the meaning of R.C. § 2933.52(A), as defined by R.C. § 2933.51(K) and R.C. § 1.59(C).

250. It is a violation of R.C. § 2933.52(A)(1) for a person to "[i]ntercept, attempt to intercept, or procure another person to intercept or attempt to intercept a wire, oral, or electronic communication."

251. It is a violation of R.C. § 2933.52(A)(3) to "[u]se, or attempt to use, the contents of

a wire, oral, or electronic communication, knowing or having reason to know that the contents were obtained through the interception of a wire, oral, or electronic communication in violation of sections 2933.51 to 2933.66 of the Revised Code."

252. The exceptions set forth in R.C. § 2933.52(B)(4) are not applicable to Defendant's Disclosure complained of herein, even though Defendant was party to the communications, as Plaintiff and the Class Members did not give their consent, and because the interceptions were for the purpose of committing tortious act in violation of the laws of Ohio and for the purpose of committing other injurious acts.

253. Plaintiff's and Class Members' activities on the Website and Online Platforms are electronic communications within the meaning of R.C. § 2933.52, defined in R.C. § 2933.51(N) as "a 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."

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

a. those to which Plaintiff's and Class Members' communications were disclosed;

b. Plaintiff's and Class Members' personal computing devices;

c. Plaintiff's and Class Members' web browsers;

d. Plaintiff's and Class Members' browser-managed files;

e. the Meta Pixel;

f. internet cookies;

g. other pixels, trackers, and/or tracking technology installed on Defendant's Website and/or server;

h. Defendant's computer servers;

i. third-party source code utilized by Defendant; and

j. computer servers of third parties (including Facebook).

255. These constitute interception devices within the meaning of R.C. 2933.52, defined in R.C. 2933.51(D) as "an electronic, mechanical, or other device or apparatus that can be used to intercept a wire, oral, or electronic communication".

256. Given that Defendant acquired the contents of Plaintiff's and Class Members' communications on the Website for tortious and other injurious purposes, their acts in so acquiring those communications constitute interception within the meaning of R.C. § 2933.52, defined in R.C. § 2933.51(C) as "the … acquisition of the contents of any … electronic communication through the use of an interception device."

257. Given that Defendant acquired the contents of Plaintiff's and Class Members' communications on the Website for tortious and otherwise injurious purposes, and knew that Facebook would also use them for tortious and otherwise injurious purposes, Defendant's actions in transmitting those communications to Facebook by installing the Meta Pixel on its Website and Online Platforms constitutes procuring another person to intercept electronic communications, in violation of R.C.2933.52(A)(3).

258. As a result of Defendant's knowing and intentional interceptions of their electronic communications, Plaintiff and Class Members are entitled to preliminary and permanent injunctive relief, declaratory judgment, liquidated damages or actual damages in amounts to be proved under R.C. § 2933.65(A)(2) but not less than $10,000.00 each, punitive damages, and their reasonable attorney's fees and expenses.

259. In addition to statutory damages, Defendant's violations caused Plaintiff 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 Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

d. Plaintiff 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.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, JOHN DOE, Individually, and as Next Friend of A.D., B.D., and C.D., and on behalf of all others similarly situated, prays for judgment as follows:

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

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

C. for equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and

Class Members' Private Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

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

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

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

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

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury as to all matters so triable.

Dated: January 5, 2024

Respectfully submitted,

Caleb Harbison (103883)
J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)

STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
charbison@stranchlaw.com
gstranch@stranchlaw.com
amize@stranchlaw.com

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

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

Counsel for Plaintiff and the Proposed Class

EXHIBIT A

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,[1] news reports,[2] FTC enforcement actions,[3] and an OCR bulletin[4] have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

[1] *See, e.g.,* Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, Proceedings of the 21st Workshop on Privacy in the Electronic Society (Nov. 7, 2022), https://dl.acm.org/doi/10.1145/3559613.3563190.
[2] *See, e.g.,* Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.
[3] *U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; *In the Matter of Flo Health Inc.*, FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.
[4] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users.

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

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

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. HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules. OCR's December 2022 bulletin about the use of online tracking technologies by HIPAA regulated entities provides a general overview of how the HIPAA Rules apply.[5] This bulletin discusses what tracking technologies are and reminds regulated entities of their obligations to comply with the HIPAA Rules when using tracking technologies.

FTC Act and FTC Health Breach Notification Rule

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. This is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes. 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.[6] 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.[7] Within the last

[5] *Id.*
[6] *See supra* note 3.
[7] *See* Federal Trade Comm'n, *Statement of the Commission on Breaches by Health Apps and Other Connected Devices* (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

few months, the FTC has issued a series of guidance pieces addressed to entities collecting, using, or disclosing sensitive health information.[8]

OCR and the FTC remain committed to ensuring that consumers' health privacy remains protected with respect to this critical issue. Both agencies are closely watching developments in this area. To the extent you are using the tracking technologies described in this letter on your website or app, we strongly encourage you to review the laws cited in this letter and take actions to protect the privacy and security of individuals' health information.[9]

Sincerely,

/s/

Melanie Fontes Rainer
Director
Office for Civil Rights
U.S. Department of Health and Human Services

/s/

Samuel Levine
Director
Bureau of Consumer Protection
Federal Trade Commission

[8] *See, e.g.*, FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking* (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking; Lesley Fair, *First FTC Health Breach Notification Rule case addresses GoodRx's not-so-good privacy practices* (Feb. 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/first-ftc-health-breach-notification-rule-case-addresses-goodrxs-not-so-good-privacy-practices; Federal Trade Comm'n and the U.S. Department of Health & Human Services' Office of the National Coordinator for Health Information Technology (ONC), Office for Civil Rights (OCR), and Food and Drug Administration (FDA), *Mobile Health App Interactive Tool* (Dec. 2022), https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool; Kristin Cohen, *Location, health, and other sensitive information: FTC Committed to fully enforcing the law against illegal use and sharing of highly sensitive data* (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[9] In addition to the HIPAA Rules, the FTC Act, and the FTC Health Breach Notification Rule, you may also be subject to other state or federal statutes that prohibit the disclosure of personal health information.

Akron Children's Hospital > **Notice of Privacy Practices**

Notice of Privacy Practices

This notice describes how medical information about you may be used and disclosed and how you can get access to this information.

OUR PLEDGE TO YOU

Privacy Policy

Notice of Privacy Practices

Effective September 23, 2013

This notice describes how medical information about you may be used and disclosed and how you can get access to this information.

OUR PLEDGE TO YOU

At Akron Children's Hospital, we believe your health information is personal. We keep records of the care and services you receive at our facilities. We are committed to keeping your health information private, and we are also required by law to respect your confidentiality.

This Notice describes the privacy practices of Akron Children's and its affiliated facilities. This Notice applies to all health records that Akron Children's maintains about you. If you are under 18 years of age, your parents or guardian must sign for you and handle your privacy rights for you. We are legally required to give you this Notice, to notify you if there is a breach of your protected health information and to follow the terms of this Notice, which may be amended from time to time.

For purposes of this Notice, the use of the words "we," "us" and "our" mean Akron Children's and all the people and entities that make up Akron Children's, which are listed at the end of this Notice. Note: In all cases when the words "you" or "patient" are used, it should be taken to mean "the patient or their parent/ legal guardian."

Who Follows This Notice of Privacy Practices?

All of our hospitals, employed physicians, doctors' offices, entities, foundations, facilities, home care programs, other services and affiliated facilities follow the terms of this Notice. These hospitals and locations are shown at the end of this Notice.

The doctors and other caregivers at Akron Children's who are not employed by Akron Children's exchange information about you as a patient with Akron Children's employees. These healthcare practitioners may also give you other privacy notices that describe their office practices.

All of these hospitals, doctors, entities, foundations, facilities, and services may share your health information with each other for reasons of treatment, payment and healthcare operations as discussed in this Notice.

How Akron Children's May Use and Disclose Your Health Information

When you become a patient of Akron Children's, we will use your health information within Akron Children's and disclose your health information outside Akron Children's for the reasons described in this Notice. The following categories describe some of the ways we will use and disclose your health information.

Treatment. We use your health information to provide you with healthcare services. We may disclose your health information to doctors, nurses, technicians, medical or nursing students or other persons at Akron Children's who need that information to take care of you. For example, if you have diabetes, the doctor may need to tell the dietitian about your condition so you get the kind of meals you need. In some situations, we may disclose health information about you to other healthcare facilities or providers who will be treating you. This may involve talking to doctors and others not employed by us. We also may disclose your health information to people outside Akron Children's who may be involved in your healthcare, such as treating doctors, home care providers, pharmacies, drug or medical device experts, and family members. We may use and disclose your information to provide you with a personal health record such as MyChart. We may also participate in electronic health information exchanges that facilitate access to personal, protected health information by other healthcare providers who provide you care. For example, if you receive care from another provider that participates in the health information exchange, this exchange will allow us to make your personal, protected health information available to the provider as needed for your treatment.

Payment. We may use and disclose your health information so the healthcare you receive may be billed and paid for by you, your insurance company or another third party. For example, we may give information about surgery you had here to your health plan so it will pay us or reimburse you for the surgery. We may also tell your health plan about a treatment you are going to receive so we can get prior payment approval or learn if your plan will pay for the treatment.

Health Care Operations. We may use your health information and disclose it outside Akron Children's for our healthcare operations. These uses and disclosures help us operate Akron Children's to maintain and improve patient care. For example, we may use your health information to review the care you received and evaluate the performance of our staff in caring for you. We also may combine health information about many patients to identify new services to offer, what services are not needed, whether certain therapies are effective, and to conduct our community health needs assessment. We may also disclose information to doctors, nurses, technicians, affiliated students and other persons at Akron Children's for learning and quality improvement purposes. We may remove information that identifies you so people outside Akron Children's may study your health data without knowing who you are.

Business Associates. We may disclose your health information to others who perform services on our behalf that we call "Business Associates." The Business Associate must agree in writing to protect the confidentiality of the information. For example, we may disclose your health information to a billing company that bills for the services we provided.

Contacting You. We may use and disclose health information to respond to your inquiries and reach you about appointments and other matters. We may contact you by mail, telephone or email. For example, we may leave voice messages at the telephone number you provide, and we may respond to your email address.

Fundraising. We may use limited portions of your health information, including your name, age, gender, date of birth, address, phone number, health insurance status, treating physician and department of service, outcome information, and the dates you or your child received treatment or services at Akron Children's in an effort to raise funds to support Akron Children's programs and operations. If you do not want Akron Children's to contact you about contribution or fundraising programs, please submit your request in writing to: Development Office, Akron Children's Hospital, One Perkins Square, Akron, Ohio, 44308. You may opt out of specific fundraising activities or all fundraising activities and if you opt out, you may request to opt back in at any time.

Health-Related Services. We may use and disclose health information about you to send you mailings about health-related products and services available at Akron Children's.

Individuals Involved in Your Care or Payment for Your Care. We may share your health information with a friend or family member who is involved in your medical care, unless you tell us in advance not to do so. Examples of ways we might disclose your information to family and friends involved with your care are: sharing information with your friend so they could pick up a prescription or medical supply, or telling your family or friends that you are in our hospital and your general condition. In addition, we may share your health information with an entity assisting in a disaster relief effort (such as the Red Cross) so your family can be notified about your condition, status and location.

Marketing Activities. We may use your health information for marketing purposes without your authorization only when we discuss such products or services with you face to face or provide you with a gift of nominal value related to the product or service. For other types of marketing activities, we will obtain your written authorization. We will not sell your name or other information to others.

Patient Information Directories. Akron Children's includes limited information about you in our patient directories, such as your name and possibly your location in the hospital and your general condition (for example: good, fair, serious, critical or undetermined). We usually give this information to people who ask for you by name. We also may include your religious affiliation in the directories and give this limited information to clergy from the community. We do not release this information if you are being treated on a psychiatric or behavioral health unit. Releasing directory information about you enables your family and others (such as friends, community-based clergy and delivery persons) to visit you in the hospital and generally know how you are doing. We will not release any of this information to these persons if you tell the hospital's admitting department not to.

Research. We perform medical research here. Our clinical researchers may look at your health records as part of your current care, or to prepare or perform research. They may share your health information with other Akron Children's researchers. All patient research conducted at Akron Children's goes through a special process required by law that reviews protections for patients involved in research, including privacy. We will not use your health information or disclose it outside Akron Children's for research reasons without either getting your prior written approval or determining that your privacy is protected.

Other Uses and Disclosures Required or Permitted by Law.

- **Health Oversight Activities.** We may share your health information with a health oversight agency for activities authorized by law. These activities include audits, investigations, inspections and licensure.

- **Law Enforcement.** We may share your health information if asked to do so by law enforcement officials if we receive a court order, subpoena, summons, warrant or similar process; to identify or locate a suspect, fugitive, material witness or missing person; when the patient is the victim of a crime if we are unable to obtain the person's agreement; when we believe the patient's death may be the result of criminal conduct; if there is suspected criminal conduct at any of our facilities; and in emergency circumstances to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime.

- **Legal Matters.** If you are involved in a lawsuit or a dispute, we may share your health information in response to an administrative order. We will disclose health information about you outside Akron Children's when required to do so by federal, state or local law or by the court process.

- **Medical Examiners, Coroners and Funeral Home Directors.** We may share your health information with a medical examiner or coroner. This may be necessary to identify a deceased person or determine the cause of death of a person. We also may share your information with funeral home directors as necessary to carry out their duties.

- **Military and Veterans.** If you are a member of the armed forces, we may share your health information as required by military command authorities.

- **Organ and Tissue Donation.** We may release health information about organ, tissue and eye donors, and transplant recipients to organizations that manage organ, tissue and eye donation and transplantation.

- **Public Health Activities.** We may disclose health information about you for public health reasons, like reporting births, deaths, child abuse or neglect, reactions to medications, problems with medical products, to notify people of recalls of products they may be using, or to notify a person who may have been exposed to a disease or may be at risk for contracting a disease or condition.

Authorizations for Other Uses and Disclosures

As described above, we will use your health information and disclose it outside Akron Children's for treatment, payment, healthcare operations, and when permitted or required by law. We will not use or disclose your health information for other reasons without your written authorization. For example, most uses and disclosures of psychotherapy notes and marketing require your authorization. You may give us authorization to use or disclose your health information to anyone for any purpose. You may revoke the authorization, in writing, at any time, but we cannot take back any uses or disclosures of your health information already made with your authorization.

Other Limitations on Disclosures

When applicable, we will comply with state and federal laws that are more stringent than the privacy regulations created under the Health Insurance Portability and Accountability Act of 1996. For example, Ohio and/or federal law require that we obtain an authorization from you in many instances before disclosing the performance or results of an HIV test, or diagnosis of AIDS or an AIDS-related condition; before disclosing information about drug or alcohol treatment you received in a drug or alcohol treatment program; and before disclosing information about mental health services you may have received.

Your Rights Regarding Health Information

Right to Accounting. You have the right to ask us for an accounting of disclosures. This is a list of certain disclosures of your health information made by Akron Children's or its Business Associates. We do not have to provide you with an accounting of disclosures when the information was disclosed for treatment, payment or healthcare operations; pursuant to your request or authorization; or for certain other disclosures permitted or required by law. You must include in your written request how far back in time you want us to go. It may not be longer than six years and may not include dates before April 14, 2003, which is the date when by law we are required to begin keeping track of the disclosures.

Right to Amend. If you feel that health information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to ask for an amendment for as long as the information is kept by or for Akron Children's. If you do not ask in writing or give your reasons in writing, we may refuse to review your request until you put it in writing. We have the right to refuse your request if you ask us to amend information that: 1) was not made by us, unless the person or place that originally made the information is no longer available to make the amendment; 2) is not part of the health information kept by or for Akron Children's; 3) is not part of the information you are permitted by law to see and copy; or 4) that we believe is correct and complete. Please note that even if we accept your request, we are not required to delete any information from your health record.

Right to Inspect and Obtain Copy. You have the right to ask to see and copy the health information we use to make decisions about your care. You may obtain an electronic copy of your health information if we maintain the health information electronically. If you ask to copy your health information, you may have to pay for copying costs whether in paper or electronic form, including supplies and labor, and postage for mailing. You may ask that we send the copy of your health information to another person if you clearly identify the designated person and where to send the copy of your health information. We may tell you that you cannot see or copy some or all of your health information. If we tell you this, you may ask that someone else review this decision. A licensed healthcare professional chosen by Akron Children's who was not involved in the denial will review this decision. We will follow the decision of this reviewer.

Right to Request Restrictions. You have the right to ask us to restrict the uses or disclosures we make of your health information for treatment, payment or healthcare operations, but we do not have to agree (except in certain situations if you ask us not to give your health plan information related to services you paid us for out of pocket in full). You also may ask us to limit the health information that we use or disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. Again, we do not have to agree. A request for a restriction must be signed and dated, and you must identify the Akron Children's Hospital or facility that maintains the information. The request should also describe the information you want restricted, say whether you want to limit the use or the disclosure of the information or both, and tell us who should not receive the restricted information. You must submit your request in writing to the Health Information Management department at Akron Children's Hospital or facility that maintains the information you want restricted or to the Privacy Office, Akron Children's Hospital, One Perkins Square, Akron, OH 44308. We will tell you if we agree with your request or not. If we do agree, we will comply with your request unless the information is needed to provide you with emergency treatment.

Right to Request Confidential Communications. You have the right to request that we communicate with you about your health in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail. Your request for confidential communications must be in writing, signed and dated. It must

identify Akron Children's Hospital or the facility making the confidential communications and specify how or where you wish to be contacted. You need not tell us the reason for your request, and we will not ask. You must send your written request to the Health Information Management department of Akron Children's Hospital or facility making the confidential communications or to the Privacy Office, Akron Children's Hospital, One Perkins Square, Akron, OH 44308. We will accommodate all reasonable requests.

Right to a Paper Copy of This Notice. You have the right to a paper copy of this Notice. You may ask us to give you a copy of this Notice at any time. Even if you have agreed to receive this Notice electronically, you are still entitled to a paper copy. You may obtain a paper copy of this Notice at any of our facilities or by calling the Akron Children's Privacy Officer at (330) 543-3065.

Complaints

If you believe your privacy rights have been violated, you may file a written complaint with Akron Children's Hospital or with the U.S. Secretary of the Department of Health and Human Services. To file a complaint with Akron Children's, contact Patient Relations at (330) 543-3534 to obtain a privacy complaint form (they will forward your written complaint to the Privacy Officer). Individuals wishing to file a complaint may also call the Corporate Compliance Helpline/Hotline at 1-877-820-3037. To file a complaint with the Region V Office for Civil Rights, contact the U.S. Department of Health and Human Services, 233 N. Michigan Ave., Suite 240, Chicago, Illinois 60601, in writing, within 180 days of a violation of your rights. You will not be penalized for filing a complaint.

Changes to this Notice

Akron Children's may change this Notice at any time. Any change in the Notice could apply to medical information we already have about you, as well as any information we receive in the future. We will post a copy of the current Notice at each of our facilities.

If you have questions about this Notice, please contact Patient Relations at 330-543-3534, or submit your question in writing to Akron Children's Hospital, Patient Relations, One Perkins Square, Akron, Ohio 44308. You may also contact the Privacy Officer at 330-543-3065.

Akron Children's Hospital and Affiliated Facilities

- Akron Children's Hospital Akron Campus
- Akron Children's Hospital Beeghly Campus
- Akron Children's Hospital Pediatrics (ACHP)
- Children's Home Care Group
- Family Child Learning Center
- Inpatient locations including Akron Children's at East Liverpool City Hospital, MedCentral Hospital, Robinson Memorial Hospital, Aultman Hospital
- Pediatric Emergency Services at Akron General Wellness Center (Montrose) and Children's at Hudson
- Neonatal Intensive Care Units at Akron General Medical Center, Summa Akron City Hospital,
- St. Elizabeth Health Center
- Maternal Fetal Medicine at Summa Health System, Akron General Medical Center, Mercy Medical Center, Wooster Community Hospital
- Specialty Office locations in Beachwood, Boardman, Hudson, Medina and at Fisher-Titus Medical Center in Norwalk, MetroHealth System in Cleveland and TriPoint Medical Center in Concord.
- Find all Akron Children's locations at akronchildrens.org/locations.

Akron Children's Hospital
One Perkins Square, Akron, Ohio 44308-1062
330-543-1000 • webmaster@akronchildrens.org
An Equal Opportunity Employer

EXHIBIT C

Akron Children's Hospital > **Terms of Use**

Terms and Conditions

All visitors to Akron Children's Hospital's website are being provided access to the site, free of charge, subject to the following terms and conditions:

---

1. Use of Akron Children's Hospital Materials

You may download, use, and copy the materials found on Akron Children's website for your personal, noncommercial use only, provided that all copies that you make of the material must bear any copyright, trademark or other proprietary notice located on the site that pertain to the material being copied.

Except as authorized in this paragraph, you are not being granted a license under any copyright, trademark, patent or other intellectual property right in the material or the products, services, processes or technology described therein.

All such rights are retained by Akron Children's Hospital, its affiliates and subsidiaries, and/or any third party owner of such rights. You may not create framed links to the Akron Children's Hospital site without express written permission from Akron Children's.

2. Use of Akron Children's Hospital Design Marks

The Akron Children's Hospital names and logos and all related product and service names, design marks and slogans are the trademarks or service marks of Akron Children's Hospital, or its subsidiaries or affiliates. You are not authorized to use any such name or mark in any advertising, publicity or in any other commercial manner without the prior written consent of Akron Children's Hospital. Requests for authorization should be submitted to webmaster@akronchildrens.org.

3. Using Information on the Site

Some of the information provided on this site is intended to educate the reader about certain medical conditions and certain possible treatments. This information is not a substitute for examination, diagnosis and medical care provided by a licensed and qualified health professional. If you believe you, your child, or someone you know, suffers from the conditions described on this site, please see your health care provider. Do not attempt to treat yourself, your child or anyone else without proper medical supervision.

4. Disclaimer of Liability

The materials on the Akron Children's Hospital site are provided to you free of charge, "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

IN NO EVENT SHALL AKRON CHILDREN'S HOSPITAL BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING SPECIAL, INDIRECT, CONSEQUENTIAL OR INCIDENTAL DAMAGES OR DAMAGES FOR LOSS OF PROFITS, REVENUE, USE, OR DATA WHETHER BROUGHT IN CONTRACT OR TORT, ARISING OUT OF OR CONNECTED WITH ANY AKRON CHILDREN'S HOSPITAL SITE OR THE USE, RELIANCE UPON OR PERFORMANCE OF ANY MATERIAL CONTAINED IN OR ACCESSED FROM ANY AKRON CHILDREN'S HOSPITAL SITE.

Akron Children's site is operated and managed in the State of Ohio, United States of America. Akron Children's makes no representation that materials found at the site are appropriate or available for use in other locations. If you access Akron Children's site from other locations, you are responsible for compliance with local laws.

5. Information Provided to Akron Children's Hospital

Do not send Akron Children's Hospital confidential or proprietary information. Any feedback, data, answers, questions, comments, suggestions, ideas, or the like that you send to Akron Children's will be treated as being non-confidential and nonproprietary, and you agree that any such information you choose to provide may be reproduced, used and distributed by Akron Children's Hospital for any purpose without restriction.

6. Endorsements

All product and service marks contained herein that are not Akron Children's Hospital marks are the trademarks of their respective owners. References that we may make to any names, marks, products or services of third parties do not necessarily constitute or imply Akron Children's endorsement, sponsorship or recommendation of the third party, information, product or service.

7. Links to Other Sites

Akron Children's Hospital is not responsible for and has no control over the contents of or information provided in the sites linked to or accessible from this site. Your linking to any other site is at your own risk, and Akron Children's accepts no liability for the contents, accuracy or currency of sites that link to this site or to which we link from this site.

Akron Children's Hospital does not endorse any linked site or has any association with any operators of such sites, and is not responsible for any transmission received from any linked site. Akron Children's assumes no responsibility, and shall not be liable for any damage to or any viral infection of your computer equipment or software on account of your access, use of or browsing in this or any other site.

8. Governing Law and Choice of Forum

The Akron Children's Hospital site is operated and managed in the State of Ohio, United States of America. Consequently, any disputes arising out of the use or operation of this site shall be governed exclusively by the laws of the State of Ohio without regard to its choice of law rules. Further, any visitor to this site hereby agrees

on behalf of themselves and any persons claiming by or through them that the sole location and venue for any litigation that may arise hereunder shall be an appropriate federal or state court located in the City of Akron, Ohio.