

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF WISCONSIN**

---

IN RE ADVOCATE AURORA HEALTH  
PIXEL LITIGATION

Lead Case No. 22-CV-1253-JPS

(Consolidated with Case Nos. 22-CV-1278-  
JPS; 22-CV-1305-JPS; 23-CV-00259-JPS;  
23-CV-00260-JPS)

This Document Relates to: All Actions

---

**SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**

---

Plaintiffs Shyanne John, Richard Webster, Deanna Danger, James Gabriel, Katrina Jones, Derrick Harris, Amber Smith, Bonnie LaPorta, Alistair Stewart, and Angel Ajani (collectively, “Plaintiffs”), on behalf of themselves and on behalf of all others similarly situated (“Class Members”), bring this Second Amended Consolidated Class Action Complaint against Advocate Aurora Health, Inc. (“Advocate” or “Defendant”) and allege, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows:

**INTRODUCTION**

1. Plaintiffs bring this case to address Defendant’s transmission and disclosure of Plaintiffs’ and Class Members’ confidential personally identifiable information (“PII”) and protected health information (“PHI”) (collectively referred to as “Private Information” or “PII and PHI”) to Meta Platforms, Inc. d/b/a Meta (“Facebook”) and/or Google LLC d/b/a Google (“Google”) via tracking pixels (“Tracking Pixels” or “Pixel”) installed on Defendant’s website, LiveWell App, and MyChart Portal (collectively referred to as “Website”).

2. Plaintiffs' and Class Members' Private Information was unlawfully intercepted, and the information transmitted to and received by third-parties included the following: IP addresses and cookie identifiers; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about specific providers; types of appointments or procedures; the buttons, links, pages, and tabs that patients click and view; communications between patients and others through MyChart, which may have included first and last names and medical record numbers; insurance information; and, if a patient had a proxy MyChart account, the first name and the first name of the proxy.

3. Defendant admits that the Private Information of at least 3,000,000 individuals was improperly and unlawfully disclosed to Facebook and Google without those individuals' knowledge or consent.<sup>1</sup>

4. Defendant is a non-profit healthcare system with 26 hospitals and 500 care sites located in Illinois and Wisconsin.<sup>2</sup> Defendant is one of the largest healthcare providers in the United States and employs approximately 75,000 individuals.

5. In order to provide medical treatment and care, Defendant collects and stores patients' Private Information and medical records. In doing so, Defendant has statutory, regulatory, contractual, fiduciary, and common law duties to safeguard that Private Information from disclosure and ensure it remains private and confidential. Defendant is duty bound to maintain the confidentiality of patient medical records and information and is further required to do so by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and by Wisconsin and Illinois statutes.<sup>3</sup>

---

<sup>1</sup> [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) (last visited Nov. 14, 2022).

<sup>2</sup> <https://www.aurorahealthcare.org/about-aurora/> (last visited Jan. 12, 2023).

<sup>3</sup> The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No.

6. Plaintiffs and Class Members are individuals who are seeking or have sought medical services and/or treatment from Defendant. Defendant advertises its online services on its Website, including the LiveWell App and MyChart Portal, to assist patients with their medical care, and Defendant encouraged its patients to use its online services.

7. As a result, Plaintiffs used Defendant's Website to: (1) search for physicians, information about specific medical conditions, treatment options, services, and locations; (2) schedule appointments and procedures; (3) receive and discuss medical diagnoses and treatment from their healthcare providers; and (4) receive lab results, review medical records, and exchange insurance information.

8. Defendant's Privacy Policies ("Privacy Policies") unequivocally states that it will not share its patients' Private Information for marketing purposes without first obtaining their written permission.<sup>4</sup>

9. As explained below, however, Defendant did disclose Plaintiffs' and Class Members' Private Information to third parties, such as Facebook and Google, and in doing so violated its own Privacy Policy. Defendant's disclosure of Plaintiffs' and Class Members' Private Information constitutes a gross violation of common law and statutory data privacy laws.

10. Defendant did not acknowledge or otherwise disclose its use of the Tracking Pixel and its widespread and blatant disclosures of Plaintiffs' and Class Members' Private Information until October 22, 2022, at which time it posted the following statement on its website (hereinafter referred to as the "Notice of Data Security Incident"):

---

104-191, 110 Stat. 1936 (1996), ("HIPAA"), and regulations of the United States Department of Health and Services ("HHS") promulgated thereunder, are designed to protect the confidentiality and guard against the unauthorized disclosure of medical records, patient health care information, and other individually identifiable healthcare information.

<sup>4</sup> See [https://www.advocatehealth.com/privacy-policy/?\\_ga=2.190713003.182618276.1583955525-240549872.1583955525](https://www.advocatehealth.com/privacy-policy/?_ga=2.190713003.182618276.1583955525-240549872.1583955525) (last visited Jan. 23, 2023).

Advocate Aurora Health is writing to provide transparency in its previous use of the Internet tracking technologies, such as Google and Meta (Facebook), that we and many others in our industry had implemented to understand how patients and others interact with our websites. These technologies disclose certain details about interactions with our websites, particularly for users that are concurrently logged into their Google or Facebook accounts and have shared their identity and other surfing habits with these companies. When using some Advocate Aurora Health sites, certain protected health information (“PHI”) would be disclosed in particular circumstances to specific vendors because of pixels on our websites or applications.

### **What happened?**

In an effort to deliver high quality services to its community, Advocate Aurora Health uses the services of several third-party vendors to measure and evaluate information concerning the trends and preferences of its patients as they use our websites. To do so, pieces of code known as “pixels” were included on certain of our websites or applications. These pixels or similar technologies were designed to gather information that we review in aggregate so that we can better understand patient needs and preferences to provide needed care to our patient population. We learned that pixels or similar technologies installed on our patient portals available through MyChart and LiveWell websites and applications, as well as on some of our scheduling widgets, transmitted certain patient information to the third-party vendors that provided us with the pixel technology. We have disabled and/or removed the pixels from our platforms and launched an internal investigation to better understand what patient information was transmitted to our vendors.

### **How do I know if I was affected?**

Out of an abundance of caution, Advocate Aurora Health has decided to assume that all patients with an Advocate Aurora Health MyChart account (including users of the LiveWell application), as well as any patients who used scheduling widgets on Advocate Aurora Health’s platforms, may have been affected. Users may have been impacted differently based on their choice of browser; the configuration of their browsers; their blocking, clearing or use of cookies; whether they have Facebook or Google accounts; whether they were logged into Facebook or Google; and the specific actions taken on the platform by the user.

### **What information was involved?**

The following information may have been involved: your IP address; dates, times, and/or locations of scheduled appointments; your proximity to an Advocate Aurora Health location; information about your provider; type of appointment or procedure; communications between you and others through MyChart, which may have included your first and last name and your medical record number; information about whether you had insurance; and, if you had a proxy MyChart account, your first name and the first name of your proxy. Based on our investigation, no social security number, financial account, credit card, or debit card information was involved in this incident.

11. Parsing out Defendant's Notice of Data Security Incident, Defendant admitted that its Website, including its LiveWell App and MyChart Portal, contained Tracking Pixels that secretly enabled the unauthorized transmission and disclosure of Plaintiffs' and Class Members' Private Information to third parties such as Facebook or Google.

12. Defendant also acknowledged the Notice of Security Incident pertains to "all patients with an Advocate Aurora Health MyChart account (including users of the LiveWell application), as well as any patients who used scheduling widgets on Advocate Aurora Health's platforms, may have been affected."

13. Third parties, like Facebook or Google, in turn, use Plaintiffs' and Class Members' Private Information to target advertisements to Plaintiffs and Class Members based on the Private Information disclosed by Plaintiffs and Class Members to Defendant.

14. At present, Defendant has not provided an exhaustive or fulsome list identifying every analytics tools it used, and it is unclear if Defendant also transmitted its patients' information to additional third parties such as LinkedIn, Pinterest, TikTok, YouTube, or Twitter, each of whom offers their own analytics tools and tracking pixels.

15. Accordingly, the purpose of this lawsuit is to enforce Plaintiffs' and Class Members' right to protect their Private Information and seek remedies for the harm caused by Defendant's intentional, reckless, or negligent disclosure to third parties.

### **BACKGROUND**

16. When an individual visits Defendant's Website and submits Private Information to Defendant, its Tracking Pixels transmit that Private Information to third parties, such as Facebook and Google. A pixel is a piece of code that "tracks the people and [the] type of actions they take."<sup>5</sup>

---

<sup>5</sup> FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited Nov. 14, 2022).

Pixels are routinely used to target specific customers by utilizing the data transmitted via pixels to build profiles for the purposes of retargeting<sup>6</sup> and future marketing.

17. With respect to Defendant’s implementation and use of the Facebook Pixel, patients’ interactions and communications were transmitted to Facebook via both first-party and third-party cookies acting in tandem. In conjunction with this process, a patient’s unique and persistent Facebook ID (“FID”) was transmitted alongside other Private Information Defendant sent to Facebook, thereby linking their communications and online interactions to their specific Facebook account for future use and marketing purposes.

18. Entities that use Facebook’s Pixel and other Business Tools—such as Defendant—are required “to have lawful rights to collect, use, and share your data before providing any data to [Facebook].” See Facebook Data Policy, <https://www.facebook.com/privacy/policy/version/20220104/>.

19. Moreover, Facebook’s policies expressly provide that businesses using the Facebook Pixel will not share data that they “know or reasonably should know... includes health, financial information or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines).” See Facebook Business Tools, Term 1(h), <https://www.facebook.com/legal/terms/businessstools>; Meta Commercial Term 3, [https://www.facebook.com/legal/commercial\\_terms](https://www.facebook.com/legal/commercial_terms).

20. Instead of taking proactive steps to verify that businesses using Facebook Pixels obtain the required consent, Facebook uses an “honor system” under which Facebook assumes these businesses “represent and warrant that [they have] provided robust and sufficient prominent

---

<sup>6</sup> “Retargeting” or “remarketing” is a form of advertising that displays ads or sends emails to previous visitors of a particular website who did not “convert” the visit into a sale or otherwise meet a marketing goal of the website owner.

notice to users regarding the Business Tool Data collection, sharing, and usage.” *See* Facebook Business Tools Terms, <https://www.facebook.com/legal/terms/businessstools>.

21. Upon information and belief, Defendant utilized the Pixel data to improve and save costs on its marketing campaign, improve its data analytics, attract new patients, and market new services and/or treatments to its existing patients. In other words, Defendant implemented the Tracking Pixel to bolster its profits.

22. Pixels are routinely used to target advertising to specific customers by utilizing the data gathered through the pixel to build profiles for future marketing and retargeting. By design, their purpose and function is to transmit information about an individual website visitor’s use of a particular website, app, or webpage, including the individual’s communications and interactions.

23. Operating as designed, Defendant’s Tracking Pixels allowed the Private Information that Plaintiffs and Class Members submitted to Defendant to be unlawfully disclosed to third parties.

24. For example, when a website user visits a webpage containing Tracking Pixels, their device is commandeered, and their communications are surreptitiously duplicated and transmitted to third parties. Stated differently, Defendant’s Website and Tracking Pixels purposely altered patients’ web browsers, forcing them to duplicate and redirect HTTP requests to third-party web servers.

25. The information sent to third parties as a result of Defendant’s Tracking Pixels included the Private Information that Plaintiffs and Class Members submitted to Defendant’s Website related to their past, present, or future health conditions, including, for example, the type and date of a medical appointment and physician. Such Private Information would allow the third party (e.g., Facebook or Google) to know that a specific patient was seeking confidential medical

care and the type of medical care being sought. This disclosure would also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, or HIV.

26. The third party, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who online target<sup>7</sup> Plaintiffs and Class Members based on communications obtained via the Tracking Pixel.

27. Plaintiffs submitted medical information related to their past, present, and future health conditions to Defendant's Website, including the LiveWell App and MyChart Portal, and used the Website to search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from their healthcare providers, receive lab results, review medical records, and exchange insurance information.

28. Defendant regularly encouraged Plaintiffs and Class Members to use its digital tools, including its Website, LiveWell App, and MyChart Portal, to receive healthcare services. In doing so, Defendant also directed Plaintiffs and Class Members to its Privacy Policies, which preclude the transmission or disclosure of Private Information to unauthorized third parties, such as Facebook or Google.

29. Plaintiffs and Class Members provided Private Information to Defendant in order to receive medical services and with the reasonable expectation that Defendant would protect their Private Information.

30. At all times that Plaintiffs and Class Members visited and utilized Defendant's Website, they had a reasonable expectation of privacy in the Private Information collected through

---

<sup>7</sup> "Online Targeting" is "a process that refers to creating advertisement elements that specifically reach out to prospects and customers interested in offerings. A target audience has certain traits, demographics, and other characteristics, based on products or services the advertiser is promoting." See <https://digitalmarketinggroup.com/a-guide-to-online-targeting-which-works-for-your-business/> (last visited Jan. 23, 2023).

Defendant's Website, including that it would remain secure and protected and only utilized for medical purposes. Plaintiffs' and Class Members' expectations were entirely reasonable because (1) they are patients; and (2) Defendant is a healthcare provider which is required by common and statutory law to protect its patients' Private Information. Moreover, Plaintiffs and Class Members also relied on Defendant's Privacy Policies, which do not permit the transmission or disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties.

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

32. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiffs' and Class Members' Private Information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

33. However, as set forth more fully below, Defendant failed in its obligations and promises by using Tracking Pixels while knowing that doing so would result in the transmission and disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties with a long history of privacy violations and misconduct—i.e. Facebook.

34. Plaintiffs and Class Members Private Information can—and likely will—be further exploited and disseminated for retargeting, marketing, or insurance companies utilizing the information to set insurance rates.

35. While Defendant willfully and intentionally incorporated the Tracking Pixel into its Website, Defendant did not disclose to Plaintiffs or Class Members that it shared their sensitive

and confidential communications via the Tracking Pixel to Facebook or Google until on or around October 22, 2022.<sup>8</sup> As a result, Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted and/or disclosed to Facebook and Google as they communicated with their healthcare provider via the Website.

36. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure Defendant's Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the consent of Plaintiffs and Class Members to disclose their Private Information to Facebook, Google, or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Tracking Pixels; (v) failing to warn Plaintiffs and Class Members; and (vi) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

37. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy, (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Tracking Pixel, (iii) loss of benefit of the bargain, (iv) diminution or deprivation of value of the Private Information, (v) statutory damages, and (vi) the continued and ongoing risk of exposure of their Private Information.

38. Plaintiffs seek to remedy these harms and bring causes of action for (1) invasion of privacy – intrusion upon seclusion; (2) invasion of privacy – publication of private facts; (3) unjust enrichment; (4) breach of implied contract; (5) breach of confidence; (6) violations of the

---

<sup>8</sup> <https://www.wpr.org/data-breach-advocate-aurora-health-system-may-have-exposed-3m-patients-information> (last visited Jan. 20, 2023).

Electronics Communication Privacy Act (“ECPA”) 18 U.S.C. § 2511(1) – unauthorized interception, use, and disclosure; (7) failure to maintain Confidentiality of Patient Healthcare Records Act under Wisconsin law, Wis. Stat. § 146.81, *et seq.*; (8) violations of the Wisconsin Deceptive Trade Practices Act, Wis. Stat. §§ 100.18, *et seq.*; (9) failure to maintain Confidentiality of Patient Healthcare Records Act under Illinois law, § 410 ILCS 50, *et seq.*; (10) violations of the Illinois Consumer Fraud and Deceptive Business Practices Act; and (11) violation of the Illinois Deceptive Trade Practices Act.

## **PARTIES**

### ***Plaintiff Shyanne John***

39. Plaintiff Shyanne John is a citizen and resident of Wisconsin.

40. Plaintiff John has received healthcare services since 1999 at one of the hospitals in Defendant’s network and has used Defendant’s Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions since 2018.

41. Plaintiff John used Defendant’s Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

42. Plaintiff John has been a Facebook user since 2013.

43. Plaintiff John accessed Defendant’s Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant or Defendant’s affiliates at Defendant’s direction and with Defendant’s encouragement.

44. As Defendant’s patient, Plaintiff John reasonably expected that her online communications with Defendant were solely between herself and Defendant, and that such

communications would not be transmitted or intercepted by a third party. Plaintiff John also relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff John would not have disclosed her Private Information to Defendant.

45. During her time as a patient, Plaintiff John never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

46. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff John's Private Information to third parties, such as Facebook and Google.

***Plaintiff Richard Webster***

47. Plaintiff Richard Webster is a citizen and resident of Wisconsin that has received healthcare services from Defendant since 2008, and he has used Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions since 2014 or earlier.

48. At Defendant's direction and with Defendant's encouragement, Plaintiff Webster used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from his healthcare providers, receive lab results, and review medical records.

49. Plaintiff Webster has been a Facebook user since 2012.

50. As a patient in Defendant's healthcare network, Plaintiff Webster reasonably expected that his online communications with Defendant were solely between himself and Defendant, and that such communications would not be transmitted or intercepted by a third party.

Plaintiff Webster also relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard his Private Information. But for his status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Webster would not have disclosed his Private Information to Defendant.

51. During his time as a patient, Plaintiff Webster never consented to the use of his Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

52. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Webster's Private Information to third parties, such as Facebook and Google.

***Plaintiff Deanna Danger***

53. Plaintiff Deanna Danger is a citizen and resident of Wisconsin.

54. Plaintiff Danger has received healthcare services since 2006 from one of the hospitals in Defendant's network and has used Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

55. Plaintiff Danger used Defendant's Website, including the LiveWell App and MyChart Portal, since 2013.

56. Plaintiff Danger used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

57. Plaintiff Danger has been a Facebook user since 2011.

58. Plaintiff Danger accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant or Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

59. As a patient in Defendant's healthcare network, Plaintiff Danger reasonably expected that her online communications with Defendant were solely between herself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Danger also relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Danger would not have disclosed her Private Information to Defendant.

60. During her time as a patient, Plaintiff Danger never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

61. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Danger's Private Information to third parties, such as Facebook and Google.

***Plaintiff James Gabriel***

62. Plaintiff James Gabriel is a citizen and resident of Wisconsin that has received healthcare services from Defendant since the 1970's and has relied on Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions since 2018.

63. Plaintiff Gabriel used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from his healthcare providers, receive lab results, and review medical records.

64. Plaintiff Gabriel has had a Facebook account since at least 2012.

65. Plaintiff Gabriel accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

66. As a patient in Defendant's healthcare network, Plaintiff reasonably expected that his online communications with Defendant were solely between himself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Gabriel also relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard his Private Information. But for his status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Gabriel would not have disclosed his Private Information to Defendant.

67. During his time as a patient, Plaintiff Gabriel never consented to the use of his Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

68. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Gabriel's Private Information to third parties, such as Facebook and Google.

***Plaintiff Katrina Jones***

69. Plaintiff Katrina Jones is a citizen and resident of Illinois.

70. Plaintiff Jones has received healthcare services from Defendant since the early 2000s and has relied on Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

71. Plaintiff Jones has been using Defendant's LiveWell App and MyChart Portal since 2017.

72. Plaintiff Jones used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and

procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

73. Plaintiff Jones has been a Facebook user since 2009.

74. Plaintiff Jones accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant or Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

75. As a patient in Defendant's healthcare network, Plaintiff Jones reasonably expected that her online communications with Defendant were solely between herself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Jones also relied on Defendant's Privacy Policy in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Jones would not have disclosed her Private Information to Defendant.

76. During her time as a patient, Plaintiff Jones never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

77. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Jones' Private Information to third parties, such as Facebook and Google.

***Plaintiff Derrick Harris***

78. Plaintiff Derrick Harris is a citizen and resident of Illinois.

79. Plaintiff Harris has received healthcare services from Defendant since 2019 from one of the hospitals in Defendant's network and has relied on Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

80. Plaintiff Harris has been using Defendant's LiveWell App and MyChart Portal since 2019.

81. Plaintiff Harris used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from his healthcare providers, receive lab results, and review medical records.

82. Plaintiff Harris has been a Facebook user since 2010.

83. Plaintiff Harris accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

84. As a patient in Defendant's healthcare network, Plaintiff Harris reasonably expected that his online communications with Defendant were solely between himself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Harris also relied on Defendant's Privacy Policy in reasonably expecting Defendant would safeguard his Private Information. But for his status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Harris would not have disclosed his Private Information to Defendant.

85. During his time as a patient, Plaintiff Harris never consented to the use of his Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

86. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Jones' Private Information to third parties, such as Facebook and Google.

***Plaintiff Amber Smith***

87. Plaintiff Amber Smith is a citizen and resident of Illinois.

88. Plaintiff Smith has received healthcare services since 2019 from one of the hospitals in Defendant's network and has relied on Defendant's digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

89. Plaintiff Smith has been using Defendant's LiveWell App since 2019.

90. Plaintiff Smith used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

91. Plaintiff Smith has had a Facebook account since at least 2008.

92. As a patient in Defendant's healthcare network, Plaintiff reasonably expected that her online communications with Defendant were solely between herself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Jones also relied on Defendant's Privacy Policy in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Smith would not have disclosed her Private Information to Defendant.

93. During her time as a patient, Plaintiff Smith never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

94. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Jones' Private Information to third parties, such as Facebook and Google

***Plaintiff Bonnie LaPorta***

95. Plaintiff Bonnie LaPorta is a citizen and resident of Illinois.

96. Plaintiff LaPorta has received healthcare services from Defendant since 2014 from one of the hospitals in Defendant's network and has relied on Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

97. Plaintiff LaPorta has been using Defendant's LiveWell App and MyChart Portal since 2014.

98. Plaintiff LaPorta used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

99. Plaintiff LaPorta has been a Facebook user since 2009.

100. Plaintiff LaPorta accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

101. As a patient in Defendant's healthcare network, Plaintiff LaPorta reasonably expected that her online communications with Defendant were solely between herself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff LaPorta also relied on Defendant's Privacy Policy in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff LaPorta would not have disclosed her Private Information to Defendant.

102. During her time as a patient, Plaintiff LaPorta never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

103. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff LaPorta's Private Information to third parties, such as Facebook and Google.

***Plaintiff Alistair Stewart***

104. Plaintiff Alistair Stewart is a citizen and resident of Illinois.

105. Plaintiff Stewart has received healthcare services from Defendant since at least 2018 from one of the hospitals in Defendant's network and has relied on Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

106. Plaintiff Stewart has been using Defendant's MyChart Portal since at least 2018.

107. Plaintiff Stewart used Defendant's Website, including the MyChart Portal, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from his healthcare providers, receive lab results, and review medical records.

108. Plaintiff Stewart has been a Facebook user since 2012.

109. Plaintiff Stewart accessed Defendant's Website, including the MyChart Portal, to receive healthcare services from Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

110. As a patient in Defendant's healthcare network, Plaintiff Stewart reasonably expected that his online communications with Defendant were solely between himself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Stewart also relied on Defendant's Privacy Policy in reasonably expecting Defendant would safeguard his Private Information. But for his status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Stewart would not have disclosed his Private Information to Defendant.

111. During his time as a patient, Plaintiff Stewart never consented to the use of his Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

112. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Stewart's Private Information to third parties, such as Facebook and Google.

***Plaintiff Angel Ajani***

113. Plaintiff Angel Ajani was a resident and citizen of the State of Illinois during all times relevant to this Complaint.

114. Plaintiff Ajani has received healthcare services from Defendant since at least 2015 from one of the hospitals in Defendant's network and has relied on Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

115. Plaintiff Ajani has been using Defendant's MyChart Portal since at least September 2015

116. Plaintiff Ajani used Defendant's Website, including the MyChart Portal, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

117. Plaintiff Ajani has been a Facebook user since 2007.

118. Plaintiff Ajani accessed Defendant's Website, including the MyChart Portal, to receive healthcare services from Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

119. As a patient in Defendant's healthcare network, Plaintiff Ajani reasonably expected that her online communications with Defendant were solely between herself and Defendant, and

that such communications would not be transmitted or intercepted by a third party. Plaintiff Ajani also relied on Defendant's Privacy Policy in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Ajani would not have disclosed her Private Information to Defendant.

120. During her time as a patient, Plaintiff Ajani never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

121. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Ajani's Private Information to third parties, such as Facebook and Google.

***Defendant Advocate Aurora Health, Inc.***

122. Defendant Advocate Aurora Health is a not-for-profit health corporation incorporated in Delaware with its principal place of business at 750 W. Virginia St., P.O. Box 341880, Milwaukee, Wisconsin 53204 and with headquarters in Milwaukee, Wisconsin and Downers Grove, Illinois.

123. Advocate Children's Hospital, Aurora Health Care, Advocate Cancer Institute, Advocate Heart Institute, Advocate Brain and Spine Institute and Orthopedic Center, and other facilities identified herein that were frequented by Plaintiffs, among various others, are all part of the Advocate Health system of health providers. Advocate encourages patients to utilize its Advocate LiveWell patient portal to communicate with their healthcare providers.

**JURISDICTION**

124. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or

value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

125. This Court has federal question jurisdiction under 29 U.S.C. § 1331 because this Complaint alleges violations of the ECPA (28 U.S.C. § 2511, *et seq.*).

126. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and many of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

127. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

### **COMMON FACTUAL ALLEGATIONS**

#### ***Defendant Improperly Disclosed Plaintiffs' and Class Members' Private Information via the Tracking Pixel.***

128. Defendant utilizes its Website to connect Plaintiffs and Class Members to Defendant's digital healthcare platform with the goal of increasing profitability.

129. In conjunction with this, Defendant installed Tracking Pixels on its Website to advertise its services to Plaintiffs and Class Members, and in doing so, secretly tracked, recorded, transmitted, and disseminated, its patients activities, communications, and experiences on Defendant's Website and electronic platforms.

130. While seeking and using Defendant's services as a medical provider via its Website, Plaintiffs' and Class Members' Private Information was intercepted by third parties via the Tracking Pixels, and it was also transmitted to third parties by Defendant via first-party cookies and conversions API tools.

131. Plaintiffs and Class Members did not intend or have any reason to suspect the Private Information would be shared with Facebook, Google, or other third parties, or that

Defendant was tracking their every communication and disclosing the same to third parties when they entered highly sensitive information on Defendant's Website, the LiveWell App, and MyChart portal.

132. Defendant did not disclose to or warn Plaintiffs or Class Members that Defendant used Plaintiffs' and Class Members' confidential electronic medical communications and Private Information for marketing purposes.

133. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information.

134. Upon information and belief, Defendant intercepted and disclosed Plaintiffs' and Class Members': (1) status as medical patients; (2) communications with Defendant through its Website; and (3) information about their medical appointments, location of treatments, specific medical providers, specific medical conditions and treatments, and related information.

135. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Tracking Pixel) that surreptitiously tracked, recorded, and disclosed Plaintiffs' and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook, Google, and/or other unauthorized third-parties; and (3) undertook this pattern of conduct without notifying Plaintiffs or Class Members and without obtaining their express written consent.

***Defendant's Pixel, Source Code, and Interception of HTTP Requests***

136. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accessed 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).

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

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

- **HTTP Request:** an electronic communication sent from the client device’s browser to the website’s server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies:** a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are “third-party cookies” which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response:** an electronic communication that is sent as a reply to the client device’s web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

139. A patient’s HTTP Request essentially asks Defendant’s Website to retrieve certain information (such as a physician’s “Book an Appointment” page), and the HTTP Response renders

or loads the requested information in the form of “Markup” (the pages, images, words, buttons, and other features that appear on the patient’s screen as they navigate Defendant’s Webpage(s)).

140. Every webpage is comprised of Markup and “Source Code.” Source Code is a set of instructions invisible to the website’s visitor that commands the visitor’s browser to take certain actions when the webpage first loads or when a specified event triggers the code.

141. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser’s user. Defendant’s Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When patients visit Defendant’s website via an HTTP Request to Aurora’s server, Defendant’s server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant’s Pixel. Thus, Defendant is in essence handing patients a tapped phone, and once the Webpage is loaded into the patient’s browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook and Google.

142. Third-parties, like Facebook or Google, place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the Private Information intercepted.

143. Defendant intentionally configured the Pixels installed on its Website to capture both the “characteristics” of individual patients’ communications with the Defendant’s Websites (*i.e.*, their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers)

and the “content” of these communications (*i.e.*, the buttons, links, pages, and tabs they click and view).

144. Defendant also deposits cookies named `_fbp`, `_ga`, and `_gid` onto Plaintiffs’ and Class Members’ computing devices. These are cookies associated with the third-parties Facebook and Google but which Defendant deposits on Plaintiffs and Class Members’ computing devices by disguising them as first-party cookies. And without any action or authorization, Defendant commands Plaintiffs’ and Class Members’ computing devices to contemporaneously re-direct the Plaintiffs’ and Class Members’ identifiers and the content of their communications to Facebook and Google.

145. The `fbp` cookie is a Facebook identifier that is set by Facebook source code and associated with Defendant’s use of the Facebook Tracking Pixel program. The `fbp` cookie emanates from Defendant’s web properties as a putative first-party cookie, but is transmitted to Facebook through cookie synching technology that hacks around the same-origin policy. The `_ga` and `_gid` cookies operate similarly as to Google.

146. Furthermore, if the patient is also a Facebook user, the information Facebook receives is linked to the patient’s Facebook profile (via their Facebook ID or “`c_user id`”), which includes other identifying information.

147. As an example, anyone who visits one of Advocate’s websites such as, *advocateaurorahealth.com*, and clicks on the “Services & Specialties” tab is presented with a search bar that lists approximately 243 links to pages with information on specific conditions, treatments, services, and locations, ranging from “Abdominal and stomach pain causes & treatment” to “Zevalin therapy.” Someone who clicks on the “Cancer Care” button is directed to a page, <https://www.advocatehealth.com/health-services/cancer-institute/>, which includes buttons and

links that provide information about specific conditions, treatment options, services, locations, doctors, clinical trials, each with a separate link. Selecting any of these links, like “Breast Cancer,” directs them to a new page, <https://www.advocatehealth.com/health-services/cancer-institute/cancers-we-treat/breast-cancer/>, providing more information about breast cancer, treatment options, services, related providers and locations, many of which have additional links and associated pages.

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

149. As another example, when a patient visits the [www.advocateaurorahealth.org](http://www.advocateaurorahealth.org) homepage, navigates to the search bar, and types in specific search terms, that information is shared with Facebook through the Pixel in the form of full string URLs. Thus, on information and belief, if a patient types in “Crohn’s Disease” into the search bar, when the webpage loads into the patient’s browser, the Pixel code is triggered which secretly sends an HTTP Request to Facebook including the patient’s c\_user id and the URL, informing Facebook that the user is searching for information on Crohn’s Disease by transmitting the following URL to Facebook: “<https://www.advocateaurorahealth.org/site-search/?q=crohns%20disease.>”

150. On information and belief, additional content is intercepted and disclosed while users are logged into the patient portal. In its Notice of Data Security Incident, Defendant acknowledges that the following types of information were impacted: (1) dates, times, and/or

locations of scheduled appointments; (2) proximity to an Advocate Aurora Health location; (3) information about your provider; (4) type of appointment or procedure; (5) communications between you and others through MyChart, which may have included your first and last name and your medical record number; and (6) information about whether you had insurance. This information is unlawfully intercepted and re-directed to unintended third parties in real time through specific button/menu selections, content typed into free text boxes, and full string URLs. Thus, for example, Plaintiffs are informed and believe that patients logged in to the patient portal would have their patient status (i.e., current/former patient), specific treatment/condition (i.e., heart valve disease requiring surgery), and specific test results (i.e., positive or negative for a given condition) all improperly disclosed to third-parties along with the patients' names, IP addresses, and cookie identifiers.

151. To be sure, according to tests performed by The Markup on other hospital websites similar to Defendant's Website and which use the *same* MyChart portal as Defendant: "When The Markup clicked the 'Finish Booking' button on a Scripps Memorial Hospital doctor's page, the pixel sent Facebook not just the name of the doctor and her field of medicine but also the first name, last name, email address, phone number, zip code, and city of residence we entered into the booking form . . . When one real patient who participated in the Pixel Hunt study logged in to the MyChart portal for Piedmont Healthcare, a Georgia health system, the Meta Pixel installed in the portal told Facebook the patient's name, the name of their doctor, and the time of their upcoming appointment, according to data collected by the participant's Mozilla Rally browser extension. . . . When another Pixel Hunt participant used the MyChart portal for Novant Health, a North Carolina-based health system, the pixel told Facebook the type of allergic reaction the patient had to a specific medication. . . . The Markup created our own MyChart account through Novant

Health to further investigate and found the Meta Pixel collecting a variety of other sensitive information. Clicking on one button prompted the pixel to tell Facebook the name and dosage of a medication in our health record, as well as any notes we had entered about the prescription. The pixel also told Facebook which button we clicked in response to a question about sexual orientation.”<sup>9</sup>

152. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third-parties bent on gathering Private Information, like Facebook, implement workarounds that cannot be evaded by savvy users. Facebook’s workaround, for example, is called Conversions API. Conversions API is an effective workaround because it does not intercept data communicated from the user’s browser. Instead, Conversions API “is designed to create a direct connection between [Web hosts’] marketing data and [Facebook].” Thus, the communications between patients and Defendant, which are necessary to use Defendant’s Website, are actually received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

153. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like Conversions API without access to the host server, companies like Facebook instruct Defendant to “[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools,” because such a “redundant event setup” allows Defendant “to share website events [with Facebook] that the pixel may lose.”<sup>10</sup> Thus, it is reasonable to infer

---

<sup>9</sup> See <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> (last visited May 5, 2023).

<sup>10</sup> See <https://www.facebook.com/business/help/308855623839366?id=818859032317965> (last visited Jan. 23, 2023).

that Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

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

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

156. In this case, Defendant employed just such a device to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to third parties like Facebook and Google.

157. For example, Defendant secretly deployed Facebook's version of a Tracking Pixel, identified as 5725819999876598, on its Website.

158. The Facebook Pixel, a marketing product, is a "piece of code" that allowed Defendant to "understand the effectiveness of [their] advertising and the actions [patients] take on [their] site."<sup>11</sup> It also allowed Defendant to optimize the delivery of ads, measure cross-device conversions, create custom advertising groups or "audiences," learn about the use of its Website, and decrease advertising and marketing costs.<sup>12</sup>

159. Most importantly, it allowed Facebook to secretly intercept patients' communications on Defendant's Website and patient portal.

---

<sup>11</sup> <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited Nov. 14, 2022)

<sup>12</sup> *Id.*

***Facebook's Platform and its Business Tools***

160. Facebook operates the world's largest social media company.

161. In 2021, Facebook generated \$117 billion in revenue.<sup>13</sup> Roughly 97% of that came from selling advertising space.<sup>14</sup>

162. As a core part of its business, Facebook maintains profiles on users that include the user's real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, including IP addresses.

163. Facebook also tracks non-Facebook users through its widespread internet marketing products and source code.

164. Facebook then sells advertising space by highlighting its ability to target users.<sup>15</sup> Facebook can target users so effectively because it surveils user activity both on and off its site.<sup>16</sup> This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."<sup>17</sup> Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.<sup>18</sup>

165. Indeed, Facebook utilizes the precise type of information disclosed by Defendant to identify, target, and market products and services to individuals.

---

<sup>13</sup> FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, <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)

<sup>14</sup> *Id.*

<sup>15</sup> FACEBOOK, WHY ADVERTISE ON FACEBOOK, <https://www.facebook.com/business/help/205029060038706> (last visited Nov. 14, 2022).

<sup>16</sup> FACEBOOK, ABOUT FACEBOOK PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited Nov. 14, 2022).

<sup>17</sup> FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting> (last visited Nov. 14, 2022).

<sup>18</sup> FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, [https://www.facebook.com/business/news/Core-Audiences\\_](https://www.facebook.com/business/news/Core-Audiences_) (last visited Nov. 14, 2022).

166. Advertisers can also build “Custom Audiences.”<sup>19</sup> Custom Audiences enable advertisers to reach “people who have already shown interest in [their] business, whether they’re loyal customers or people who have used [their] app or visited [their] website.”<sup>20</sup> With Custom Audiences, advertisers can target existing customers directly, and they can also build “Lookalike Audiences,” which “leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities.”<sup>21</sup> Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook’s “Business Tools,” including the Facebook Pixel.<sup>22</sup>

167. As Facebook puts it, the Business Tools “help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services.”<sup>23</sup> Put more succinctly, Facebook’s Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept, collect, view, and use user activity on those platforms.

168. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage’s Universal Resource Locator (“URL”) and metadata, or

---

<sup>19</sup> FACEBOOK, ABOUT CUSTOM AUDIENCES, <https://www.facebook.com/business/help/744354708981227?id=2469097953376494> (last visited Nov. 14, 2022).

<sup>20</sup> FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting> (last visited Nov. 14, 2022).

<sup>21</sup> Facebook, About Lookalike Audiences, <https://www.facebook.com/business/help/164749007013531?id=401668390442328> (last visited Nov. 14, 2022).

<sup>22</sup> FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>; Facebook, Create a Website Custom Audience <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494> (last visited Nov. 14, 2022).

<sup>23</sup> FACEBOOK, THE FACEBOOK BUSINESS TOOLS, <https://www.facebook.com/help/331509497253087> (last visited Nov. 14, 2022).

when a user downloads a mobile application or makes a purchase.<sup>24</sup> Facebook’s Business Tools can also track other events. Facebook offers a menu of “standard events” from which advertisers can choose, including what content a visitor views or purchases.<sup>25</sup> Advertisers can even create their own tracking parameters by building a “custom event.”<sup>26</sup>

169. One such Business Tool is the Facebook Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their websites. As the name implies, the Facebook Pixel “tracks the people and the types of actions they take.”<sup>27</sup> When a user accesses a website hosting the Facebook Pixel, Facebook’s software script surreptitiously directs the user’s browser to send a separate message to Facebook’s servers at certain times during interaction with the webpage. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser’s attempt to load and read Defendant’s Websites—Defendant’s own code, and Facebook’s embedded code.

170. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients’ Facebook IDs, IP addresses, and/or device IDs and the other information they input into Defendant’s Website, including not only their medical searches, treatment requests, and the webpages they view, but also their home address, zip code, or phone

---

<sup>24</sup> See FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, <https://developers.facebook.com/docs/facebook-pixel/advanced/>; see also FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>; FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Nov. 14, 2022).

<sup>25</sup> FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142> (last visited Nov. 14, 2022).

<sup>26</sup> FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; see also FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Nov. 14, 2022).

<sup>27</sup> FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited May 5, 2023).

number. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.<sup>28</sup> Plaintiffs' and Class Members identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

171. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the website visitor is also a Facebook user, the information collected via the Facebook pixel is associated with the user's Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity.

172. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile. To find the Facebook account associated with a c\_user cookie, one simply needs to type [www.facebook.com/](http://www.facebook.com/) followed by the c\_user ID.

***Plaintiffs Have Specific Evidence of Defendant's Tracking Pixel Communicating with Facebook on dates they submitted Private Information.***

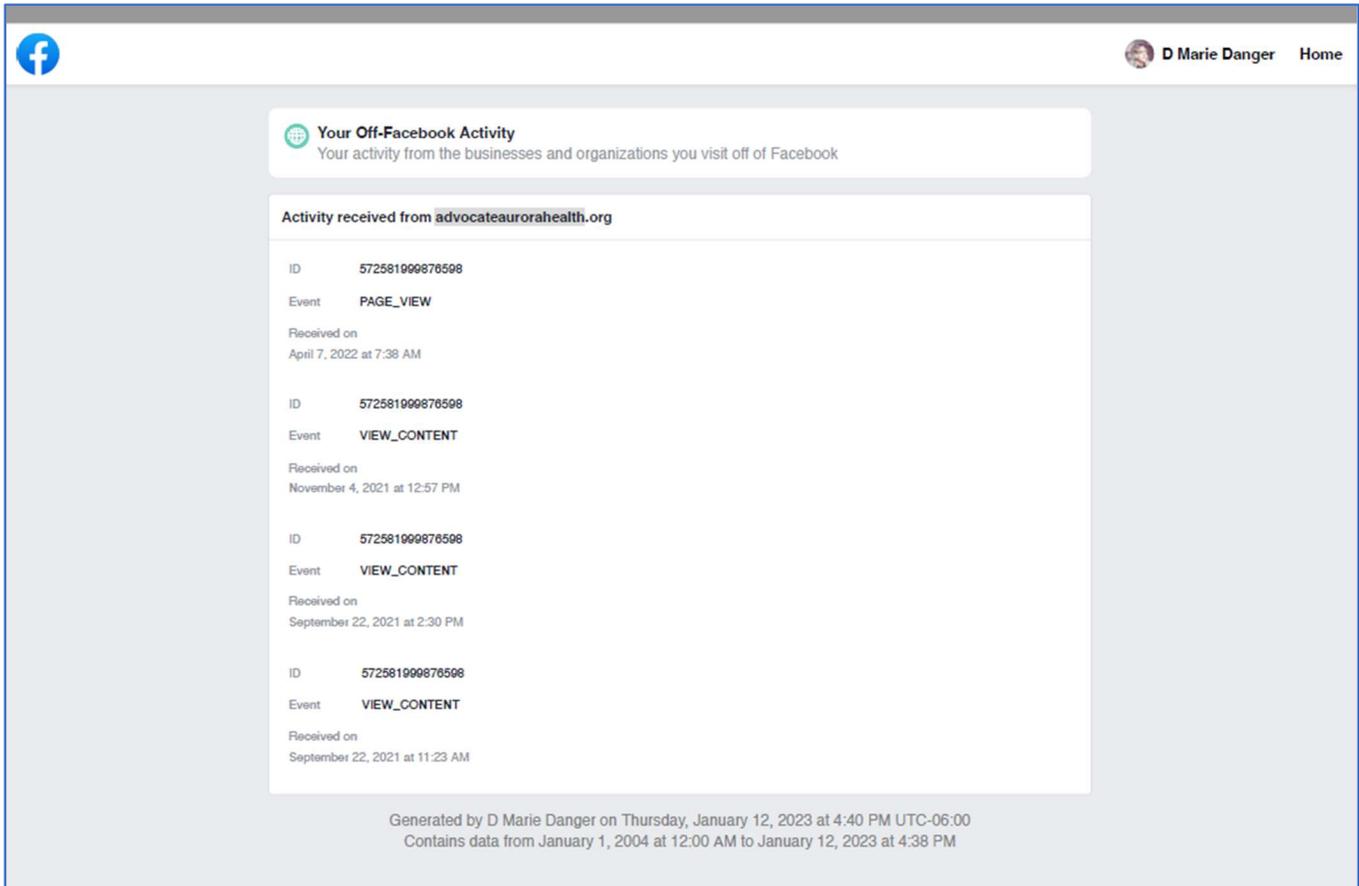
173. For example, in this case, Plaintiff Danger's Facebook offsite activity download ("Off-Facebook activity Download")<sup>29</sup> shows the dates and times that Defendant's Tracking Pixel communicated with Plaintiff's Facebook on different pages within Defendant's Website:

Pixel from [www.advocateaurorahealth.org](http://www.advocateaurorahealth.org)

---

<sup>28</sup> <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Nov. 14, 2022).

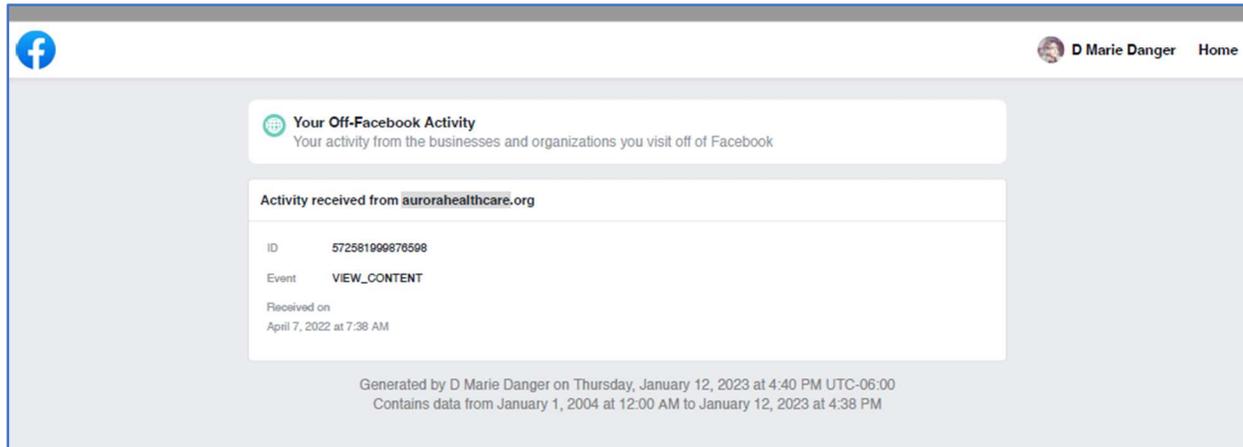
<sup>29</sup> The "Off-Facebook activity is a summary of activity that business and organizations share with [Facebook] about [individuals'] interactions, such as visiting [businesses' and organization's] apps or websites." See <https://www.facebook.com/help/2207256696182627> (last visited Jan. 20, 2023).



174. As shown above, Plaintiff Danger's Off-Facebook Download activity shows Defendant's Pixel ID Number 5725819999876598 was contained in Defendant's webpage ([www.advocateaurorahealth.org](http://www.advocateaurorahealth.org)) and communicated with Plaintiff Danger's Facebook on the following dates and times:

- September 22, 2021 at 11:23 am
- September 22, 2021 at 2:30 pm
- November 4, 2021 at 12:57 pm; and
- April 7, 2022 at 7:38 am

Pixel from [www.aurorahealthcare.org](http://www.aurorahealthcare.org) (“Pixel 2”)



175. As shown above, Plaintiff Danger’s Off-Facebook Download activity shows Defendant’s Pixel ID Number 5725819999876598 was contained in Defendant’s webpage [www.aurorahealthcare.org](http://www.aurorahealthcare.org) (a different webpage from [www.advocateaurorahealth.org](http://www.advocateaurorahealth.org)) and communicated with Plaintiff Danger’s Facebook on the following dates and times:

- April 7, 2022 at 7:38 am

  D Marie Danger Home

**Your Off-Facebook Activity**  
Your activity from the businesses and organizations you visit off of Facebook

**Activity received from myadvocateaurora.org**

ID	572581999876598
Event	PAGE_VIEW
Received on	March 19, 2021 at 11:37 AM
ID	572581999876598
Event	PAGE_VIEW
Received on	March 12, 2021 at 8:32 AM
ID	572581999876598
Event	PAGE_VIEW
Received on	March 8, 2021 at 11:14 AM
ID	572581999876598
Event	PAGE_VIEW
Received on	March 4, 2021 at 12:55 PM
ID	572581999876598
Event	PAGE_VIEW
Received on	February 22, 2021 at 9:28 AM

ID	572581999876598
Event	PAGE_VIEW
Received on	February 17, 2021 at 7:26 AM
ID	572581999876598
Event	PAGE_VIEW
Received on	February 10, 2021 at 6:27 AM
ID	572581999876598
Event	PAGE_VIEW
Received on	February 9, 2021 at 1:38 PM
ID	572581999876598
Event	PAGE_VIEW
Received on	January 29, 2021 at 7:26 AM
ID	572581999876598
Event	PAGE_VIEW
Received on	January 28, 2021 at 7:28 AM
ID	572581999876598
Event	PAGE_VIEW
Received on	January 25, 2021 at 11:29 AM

176. As shown above, Plaintiff Danger's Off-Facebook Download activity shows Defendant's Pixel ID Number 5725819999876598 was contained in Defendant's webpage [www.myadvocateaurora.org](http://www.myadvocateaurora.org) and communicated with Plaintiff Danger's Facebook on the following dates and times:

- January 25, 2021 at 11:29 am;
- January 28, 2021 at 7:28 am;
- January 29, 2021 at 7:26 am;
- February 9, 2021 at 1:38 pm;
- February 10, 2021 at 6:27 am;
- February 17, 2021 at 7:26 am;
- February 22, 2021 at 9:28 am;
- March 4, 2021 at 12:56 pm;
- March 8, 2021 at 11:14 am;
- March 12, 2021 at 8:30 am; and
- March 19, 2021 at 11:37 am

177. Notably, [www.myadvocateaurora.org](http://www.myadvocateaurora.org) contains the LiveWell App and access to the MyChart Portal. On the homepage, it provides links to "billing," "message your doctor," "safecheck screening," "get your test results," "manage appointments," "start a video visit," and "classes and events."

178. From January to March 2021, Plaintiff Danger sought and received medical treatment regarding wellness checkups for prescription medication and female wellness checks. During that timeframe, Plaintiff communicated with her treatment providers regarding medical

conditions, medical records, lab results, and used the LiveWell App and MyChart Portal to schedule appointments and procedures.

179. The Off-Facebook Activity Downloads show Defendant's Tracking Pixel communicating with Plaintiff's Facebook account on the days that Plaintiff used Defendant's Website to communicate Private Information.

180. The Off-Facebook Activity Downloads indicate Defendant's Website transmitted and disclosed Plaintiff's Private Information to Facebook because it shows the real-time transmission of Private Information from Defendant's Website to Facebook on dates and times that Plaintiff Danger communicated Private Information to Defendant.

***Defendant's Privacy Policies and Promises***

181. Defendant's Privacy Policies allow for the disclosure of patient information in the following settings: (1) patient treatment; (2) running their organization; (3) billing; and (4) as enabled by law.<sup>30</sup>

182. Defendant's Privacy Policies unequivocally state Defendant will not share Plaintiffs' and Class Members' Private Information for marketing purposes unless patients provide written permission.<sup>31</sup>

183. Plaintiffs and Class Members have not provided Defendant with written permission to share their Private Information for marketing purposes.

184. Despite Defendant's acknowledgement that it will not share Plaintiffs' and Class Members' Private Information, Defendant, in fact, shared Plaintiffs' and Class Members' Private Information via the Tracking Pixel.

---

<sup>30</sup> <https://www.advocateaurorahealth.org/notice-of-privacy-practices/> (last visited Jan. 19, 2023).

<sup>31</sup> *Id.*

185. Specifically, Defendant transmitted and/or disclosed Plaintiffs’ and Class Members’ Private Information to third parties, like Facebook and Google, without Plaintiffs’ and Class Members’ consent or written permission.

186. In doing so, Defendant intended to improve and save costs on its marketing campaign, improve its data analytics, attract new patients, and market new services and/or treatments to its existing patients.

187. In simple terms, Defendant violated its own Privacy Policy—i.e., the Privacy Policy that Plaintiffs and Class Members relied upon—in order to bolster its profits.

***Defendant Violated HIPAA Standards***

188. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients’ express written authorization.<sup>32</sup>

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

190. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, “establishes national standards to protect individuals’ medical records and other individually identifiable health information (collectively defined as ‘protected health information’) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.”<sup>33</sup>

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

---

<sup>32</sup> HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

<sup>33</sup> HHS.gov, HIPAA For Professionals (last visited April 12, 2023), <https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html>.

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

192. IIHI is defined as “a subset of health information, including demographic information collected from an individual” that is: (1) “created or received by a health care provider, health plan, employer, or health care clearinghouse”; (2) “[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual”; and (3) either (a) “identifies the individual” or (b) “[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103.

193. Under the HIPPA de-identification rule, “health information is not individually identifiable only if”: (1) an expert “determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information” and “documents the methods and results of the analysis that justify such determination”; or (2) “the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

a. Names;

\*\*\*

H. Medical record numbers;

\*\*\*

J. Account numbers;

\*\*\*

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; ... and

R. Any other unique identifying number, characteristic, or code...;and”

The covered entity must not “have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”

45 C.F.R. § 160.514.

194. The HIPAA Privacy Rule requires any “covered entity”—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

195. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 (“Part C”): “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.” The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320d-6.

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

197. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall “be fined not more than \$250,000, imprisoned not more than 10 years, or both.”

198. 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 instructed in 2012:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.<sup>34</sup>

199. In its guidance for Marketing, the Department further instructed in 2003:

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).<sup>35</sup>

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

- a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);
- b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002); and
- c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013).

---

<sup>34</sup> *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) at 5, available at [https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs\\_deid\\_guidance.pdf](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf) (last visited Nov. 3, 2022).

<sup>35</sup> <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf> (April 3, 2003) (last visited Nov. 3, 2022).

201. 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 technologies (“tracking technologies”).<sup>36</sup>

202. The Bulletin expressly provides that “[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.”<sup>37</sup>

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

Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (*e.g.* health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual’s IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.<sup>38</sup>

204. The Bulletin further explained that health care providers violate HIPAA when they use tracking technologies that disclose an individual’s identifying information (like an IP address)

---

<sup>36</sup> See HHS.gov, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (Dec. 1, 2022), available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited May 5, 2022).

<sup>37</sup> *Id.* (emphasis in original).

<sup>38</sup> *Id.*

even if no treatment information is included and even if the individual does not have a relationship with the health care provider:

How do the HIPAA Rules apply to regulated entities' use of tracking technologies?

Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually identifiable health information (IIHI) that the individual providers when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. **This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e. it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.**<sup>39</sup>

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

Tracking on unauthenticated webpages

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

---

<sup>39</sup> *Id.* (emphasis added).

entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.<sup>40</sup>

206. HHS explained in the Bulletin that tracking technologies on health care providers' patient portals "generally have access to PHI" and may access diagnoses and treatment information, in addition to other sensitive data:

Tracking on user-authenticated webpages

Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to only use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.<sup>41</sup>

207. The Bulletin is not a pronouncement of new law, but instead reminded covered entities and business associates of their longstanding obligations under existing guidance. The Bulletin notes that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," then explains how online tracking technologies violate the same HIPAA rules that have existed for decades.<sup>42</sup>

---

<sup>40</sup> *Id.* (emphasis added).

<sup>41</sup> *Id.* (emphasis added).

<sup>42</sup> *Id.* (citing, e.g., Modifications of the HIPAA [Rules], Final Rule," 78 FR 5566, 5598, a rulemaking notice from January 25, 2013, which stated: "[P]rotected health information ... may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered entity, then it is protected health information by definition since it is indicative that the individual received health care services or benefits from the covered entity, and therefore it must be protected ... in accordance with the HIPAA rules.").

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

***Defendant Violated Industry Standards***

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

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

211. 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)

212. 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.

213. AMA Code of Medical Ethics Opinion 3.3.2 provides:

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

***Plaintiffs' and Class Members' Expectation of Privacy***

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

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

***IP Addresses are Personally Identifiable Information***

216. On information and belief, through the use of the Tracking Pixels on Defendant's Website, Defendant also disclosed and otherwise assisted Facebook, Google, and/or other third parties with intercepting Plaintiffs' and Class Members' Computer IP addresses.

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

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

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

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

221. Google also tracks IP addresses associated with Internet users.

222. Facebook, Google, and other third-party marketing companies track IP addresses for use in tracking and targeting individual homes and their occupants with advertising by using IP addresses.

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

- a. 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).

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

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

***Defendant was Enriched and Benefitted from the Use of the Pixel and Unauthorized Disclosures and Class Members’ Data Had Financial Value***

225. The sole purpose of the use of the Tracking Pixel on Defendant’s Website was marketing and profits.

226. In exchange for disclosing the Private Information of its patients, Defendant is compensated by third parties, like Facebook and Google, in the form of enhanced advertising services and more cost-efficient marketing on Facebook.

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

228. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients, including Plaintiffs and Class Members.

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

230. Moreover, Plaintiffs’ and Class Members’ Private Information had value and Defendant’s disclosure and interception harmed Plaintiffs and the Class. Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as \$434 per user, for a total of more than \$200 billion industry wide.

231. The value of health data in particular is well-known, and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled “How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry” in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.<sup>43</sup>

232. 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.”<sup>44</sup>

### **PLAINTIFFS’ EXPERIENCES**

#### ***Plaintiff Shyanne John***

233. Plaintiff Shyanne John entrusted her Private Information to Defendant. As a condition of receiving Defendant’s services, Plaintiff John disclosed her Private Information to Defendant.

234. Plaintiff John accessed Defendant’s Website to receive healthcare services from Defendant and at Defendant’s direction.

235. Plaintiff John scheduled doctor’s appointments for herself via Defendant’s Website.

236. Plaintiff John reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

---

<sup>43</sup> See <https://time.com/4588104/medical-data-industry/> (last visited Feb. 16, 2023).

<sup>44</sup> See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited Feb. 16, 2023).

237. Plaintiff John provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

238. As described herein, Defendant worked along with Facebook to intercept Plaintiff John's communications, including those that contained Private Information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

239. Defendant transmitted to third parties Plaintiff John's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff John and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

240. As a "redundant" measure to ensure Plaintiff John's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff John's Private Information from electronic storage on Defendant's server directly to Facebook.

241. By doing so without Plaintiff John's consent, Defendant breached Plaintiff John's right to privacy and unlawfully disclosed Plaintiff John's Private Information to third parties.

242. Defendant did not inform Plaintiff John that it had shared her Private Information with Facebook until on or around October 22, 2022.

243. Plaintiff John suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private

Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

244. Plaintiff John has a continuing interest in ensuring that Plaintiff John's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

***Plaintiff Richard Webster***

245. Plaintiff Richard Webster entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Webster disclosed his Private Information to Defendant.

246. Plaintiff Webster accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

247. Plaintiff Webster scheduled doctor's appointments for himself via Defendant's Website.

248. Plaintiff Webster reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

249. Plaintiff Webster provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

250. As described herein, Defendant worked along with Facebook to intercept Plaintiff Webster's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

251. Defendant transmitted to third parties, like Facebook, Plaintiff Webster's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff Webster and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

252. As a "redundant" measure to ensure Plaintiff Webster's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff Webster's Private Information from electronic storage on Defendant's server directly to Facebook.

253. By doing so without Plaintiff Webster's consent, Defendant breached Plaintiff Webster's right to privacy and unlawfully disclosed Plaintiff Webster's Private Information.

254. Defendant did not inform Plaintiff Webster that it had shared his Private Information with Facebook until on or around October 22, 2022.

255. Plaintiff Webster suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to his Private Information.

256. Plaintiff Webster has a continuing interest in ensuring that Plaintiff Webster's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

***Plaintiff Deanna Danger***

257. Plaintiff Deanna Danger entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Danger disclosed her Private Information to Defendant.

258. Plaintiff Danger accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

259. Plaintiff Danger scheduled doctor's appointments for herself via Defendant's Website.

260. Plaintiff Danger reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

261. Plaintiff Danger provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

262. As described herein, Defendant worked along with Facebook to intercept Plaintiff Danger's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

263. Defendant transmitted to third parties, like Facebook, Plaintiff Danger's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff Danger and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

264. As a “redundant” measure to ensure Plaintiff Danger’s Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff Danger’s Private Information from electronic storage on Defendant’s server directly to Facebook.

265. By doing so without Plaintiff Danger’s consent, Defendant breached Plaintiff Danger’s right to privacy and unlawfully disclosed Plaintiff Danger’s Private Information.

266. Defendant did not inform Plaintiff Danger that it had shared her Private Information with Facebook until on or around October 22, 2022.

267. Plaintiff Danger suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

268. Plaintiff Danger has a continuing interest in ensuring that Plaintiff Danger’s Private Information – which, upon information and belief, remains backed up in Defendant’s possession – is protected and safeguarded from future unauthorized disclosure.

***Plaintiff James Gabriel***

269. Plaintiff James Gabriel entrusted his Private Information to Defendant. As a condition of receiving Defendant’s services, Plaintiff Gabriel disclosed his Private Information to Defendant.

270. Plaintiff Gabriel accessed Defendant’s Website to receive healthcare services from Defendant and at Defendant’s direction.

271. Plaintiff Gabriel scheduled doctor's appointments for himself via Defendant's Website.

272. Plaintiff Gabriel reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

273. Plaintiff Gabriel provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

274. As described herein, Defendant worked along with Facebook to intercept Plaintiff Gabriel's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

275. Defendant transmitted to third parties, like Facebook, Plaintiff Gabriel's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff Gabriel and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

276. As a "redundant" measure to ensure Plaintiff Gabriel's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff Gabriel's Private Information from electronic storage on Defendant's server directly to Facebook.

277. By doing so without Plaintiff Gabriel's consent, Defendant breached Plaintiff Gabriel's right to privacy and unlawfully disclosed Plaintiff Gabriel's Private Information.

278. Defendant did not inform Plaintiff Gabriel that it had shared his Private Information with Facebook until on or around October 22, 2022.

279. Plaintiff Gabriel suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to his Private Information.

280. Plaintiff Gabriel has a continuing interest in ensuring that Plaintiff Gabriel's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

***Plaintiff Katrina Jones***

281. Plaintiff Katrina Jones entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Jones disclosed her Private Information to Defendant.

282. Plaintiff Jones accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

283. Plaintiff Jones scheduled doctor's appointments for herself via Defendant's Website.

284. Plaintiff Jones reasonably expected that his communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

285. Plaintiff Jones provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

286. As described herein, Defendant worked along with Facebook to intercept Plaintiff Jones' communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

287. Defendant transmitted to third parties, like Facebook, Plaintiff Jones' Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff Jones and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

288. As a "redundant" measure to ensure Plaintiff Jones' Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's Private Information from electronic storage on Defendant's server directly to Facebook.

289. By doing so without Plaintiff Jones' consent, Defendant breached Plaintiff Jones' right to privacy and unlawfully disclosed Plaintiff Jones' Private Information.

290. Defendant did not inform Plaintiff Jones that it had shared her Private Information with Facebook until on or around October 22, 2022.

291. Plaintiff Jones suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

292. Plaintiff Jones has a continuing interest in ensuring that Plaintiff Jones' Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

***Plaintiff Derrick Harris***

293. Plaintiff Derrick Harris entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Harris disclosed his Private Information to Defendant.

294. Plaintiff Harris accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

295. Plaintiff Harris scheduled doctor's appointments for himself via Defendant's Website.

296. Plaintiff Harris reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

297. Plaintiff Harris provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

298. As described herein, Defendant worked along with Facebook to intercept Plaintiff Harris' communications, including those that contained Private Information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

299. Defendant transmitted to third parties, like Facebook, Plaintiff Harris' Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location;

information about providers; types of appointments or procedures; communications between Plaintiff Harris and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

300. As a “redundant” measure to ensure Plaintiff’s Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff’s Private Information from electronic storage on Defendant’s server directly to Facebook.

301. By doing so without Plaintiff Harris’ consent, Defendant breached Plaintiff Harris’ right to privacy and unlawfully disclosed Plaintiff Harris’ Private Information.

302. Defendant did not inform Plaintiff Harris that it had shared his Private Information with Facebook until on or around October 22, 2022.

303. Plaintiff Harris suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to his Private Information.

304. Plaintiff Harris has a continuing interest in ensuring that Plaintiff Harris’ Private Information – which, upon information and belief, remains backed up in Defendant’s possession – is protected and safeguarded from future unauthorized disclosure.

***Plaintiff Amber Smith***

305. Plaintiff Amber Smith entrusted her Private Information to Defendant. As a condition of receiving Defendant’s services, Plaintiff Smith disclosed her Private Information to Defendant.

306. Plaintiff Smith accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

307. Plaintiff Smith scheduled doctor's appointments for herself via Defendant's Website.

308. Plaintiff Smith reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

309. Plaintiff Smith provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

310. As described herein, Defendant worked along with Facebook to intercept Plaintiff Smith's communications, including those that contained Private Information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

311. Defendant transmitted to third parties, like Facebook, Plaintiff Smith's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff Smith and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

312. As a "redundant" measure to ensure Plaintiff's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's Private Information from electronic storage on Defendant's server directly to Facebook.

313. By doing so without Plaintiff Smith's consent, Defendant breached Plaintiff Smith's right to privacy and unlawfully disclosed Plaintiff Smith's Private Information.

314. Defendant did not inform Plaintiff Smith that it had shared her Private Information with Facebook until on or around October 22, 2022.

315. Plaintiff Smith suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

316. Plaintiff Smith has a continuing interest in ensuring that Plaintiff Smith's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

***Plaintiff Bonnie LaPorta***

317. Plaintiff Bonnie LaPorta entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff LaPorta disclosed her Private Information to Defendant.

318. Plaintiff LaPorta accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

319. Plaintiff LaPorta scheduled doctor's appointments for herself via Defendant's Website.

320. Plaintiff LaPorta reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

321. Plaintiff LaPorta provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

322. As described herein, Defendant worked along with Facebook to intercept Plaintiff LaPorta's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

323. Defendant transmitted to third parties, like Facebook, Plaintiff LaPorta's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff John and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

324. As a "redundant" measure to ensure Plaintiff Laporte's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff Laporte's Private Information from electronic storage on Defendant's server directly to Facebook.

325. By doing so without Plaintiff LaPorta's consent, Defendant breached Plaintiff LaPorta's right to privacy and unlawfully disclosed Plaintiff LaPorta's Private Information.

326. Defendant did not inform Plaintiff LaPorta that it had shared her Private Information with Facebook until on or around October 22, 2022.

327. Plaintiff LaPorta is diagnosed with medical conditions that she disclosed on Defendant's Website. After submitting this information, Plaintiff LaPorta noticed Facebook

advertisements targeted towards the medical information that she disclosed via Defendant's Website.

328. Plaintiff LaPorta suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

329. Plaintiff LaPorta has a continuing interest in ensuring that Plaintiff LaPorta's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

***Plaintiff Alistair Stewart***

330. Plaintiff Alistair Stewart entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Stewart disclosed his Private Information to Defendant.

331. Plaintiff Stewart accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

332. Plaintiff Stewart scheduled doctor's appointments for himself via Defendant's Website.

333. Plaintiff Stewart reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

334. Plaintiff Stewart provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

335. As described herein, Defendant worked along with Facebook to intercept Plaintiff Stewart's communications, including those that contained Private Information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

336. Defendant transmitted to third parties, like Facebook, Plaintiff Stewart's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff Stewart and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

337. As a "redundant" measure to ensure Plaintiff Stewart's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff Stewart's Private Information from electronic storage on Defendant's server directly to Facebook.

338. By doing so without Plaintiff Stewart's consent, Defendant breached Plaintiff Stewart's right to privacy and unlawfully disclosed Plaintiff Stewart's Private Information.

339. Defendant did not inform Plaintiff Stewart that it had shared his Private Information with Facebook until on or around October 22, 2022.

340. Plaintiff Stewart suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to his Private Information.

341. Plaintiff Stewart has a continuing interest in ensuring that Plaintiff Stewart's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

***Plaintiff Angel Ajani***

342. Plaintiff Angel Ajani entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Ajani disclosed her Private Information to Defendant.

343. Plaintiff Ajani accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

344. Plaintiff Ajani scheduled doctor's appointments for herself via Defendant's Website.

345. Plaintiff Ajani reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

346. Plaintiff Ajani provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

347. As described herein, Defendant worked along with Facebook to intercept Plaintiff Ajani's communications, including those that contained Private Information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

348. Defendant transmitted to third parties, like Facebook, Plaintiff Ajani's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location;

information about providers; types of appointments or procedures; communications between Plaintiff Ajani and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

349. As a “redundant” measure to ensure Plaintiff Ajani’s Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff Ajani’s Private Information from electronic storage on Defendant’s server directly to Facebook.

350. By doing so without Plaintiff Ajani’s consent, Defendant breached Plaintiff Ajani’s right to privacy and unlawfully disclosed Plaintiff Ajani’s Private Information.

351. Defendant did not inform Plaintiff Ajani that it had shared her Private Information with Facebook until on or around October 22, 2022.

352. Plaintiff Ajani suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

353. Plaintiff Ajani has a continuing interest in ensuring that Plaintiff Ajani’s Private Information – which, upon information and belief, remains backed up in Defendant’s possession – is protected and safeguarded from future unauthorized disclosure.

### **TOLLING**

354. Any applicable statute of limitations has been tolled by the “delayed discovery” rule. Plaintiffs did not know (and had no way of knowing) that Plaintiffs’ Private Information was

intercepted and unlawfully disclosed because Defendant kept this information secret until Defendant's disclosure in October 2022.

### CLASS ACTION ALLEGATIONS

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

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

**All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Tracking Pixel on Defendant's Website, LiveWell App, and MyChart patient portal.**

357. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiffs John, Webster, Danger, and Gabriel (the "Wisconsin Plaintiffs") assert claims on behalf of a separate subclass, defined as follows:

**All individuals residing in Wisconsin whose Private Information was disclosed to a third party without authorization or consent through the Tracking Pixel on Defendant's Website, LiveWell App, and MyChart patient portal (the "Wisconsin Class").**

358. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiffs Jones, Harris, Smith, LaPorta, and Stewart (the "Illinois Plaintiffs") assert claims on behalf of a separate subclass, defined as follows:

**All individuals residing in Illinois whose Private Information was disclosed to a third party without authorization or consent through the Tracking Pixel on Defendant's Website, LiveWell App, and MyChart patient portal (the "Illinois Class").**

359. Excluded from the Class and Subclasses are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant

officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

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

361. Numerosity, Fed R. Civ. P. 23(a)(1). The Class Members for each proposed Class are so numerous that joinder of all members is impracticable. Upon information and belief, there are over 3,000,000 individuals whose Private Information may have been improperly accessed by Facebook and/or Google, and the Class is identifiable within Defendant's records.

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

- a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiffs and Class Members;
- b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;
- c. Whether Defendant violated its Privacy Policies by disclosing the PII and PHI of Plaintiffs and Class Members to Facebook, Google, and/or additional third parties.
- d. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI would be disclosed to third parties;
- e. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;

- f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PHI and PII;
- g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;
- h. Whether Defendant violated the consumer protection statutes invoked herein;
- i. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- j. Whether Defendant knowingly made false representations as to its data security and/or Privacy Policies practices;
- k. Whether Defendant knowingly omitted material representations with respect to its data security and/or Privacy Policies practices;
- l. Whether Defendant's knowing disclosure its patients' individually identifiable health information to Facebook and Google is "criminal or tortious" under 18 U.S.C § 2511(2)(d); and
- m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their PII and PHI.

363. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

364. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that Plaintiffs has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that

is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs has suffered are typical of other Class Members. Plaintiffs has also retained counsel experienced in complex class action litigation, and Plaintiffs intends to prosecute this action vigorously.

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

366. 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 Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

367. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure

to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

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

371. Further, Defendant has acted or refused to act on grounds generally applicable to each Class and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

- a. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information;
- b. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information with respect to Defendant's Privacy Policies;
- c. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- e. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;
- f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties; and
- g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

373. Plaintiffs reserve the right to amend or modify the Class definition as this case progresses.

**COUNT I**  
**INVASION OF PRIVACY – INTRUSION UPON SECLUSION**  
**(On Behalf of Plaintiffs, the Illinois Class, and the Wisconsin Class)**

374. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

375. The Private Information of Plaintiffs and Class Members consists of private and confidential facts and information that were never intended to be shared beyond private communications.

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

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

378. The unauthorized disclosure and/or acquisition by a third party of Plaintiffs' and Class Members' Private Information via the use of the Tracking Pixel by Defendant is highly offensive to a reasonable person.

379. Defendant's willful and intentional disclosure of Plaintiffs' and Class Members' Private Information constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

380. In June 2022, a publication called The Markup reported that "Facebook is Receiving Sensitive Medical Information from Hospital Websites."<sup>45</sup> The article quoted numerous

---

<sup>45</sup> Feathers, T., Pixel Hunt: Facebook Is Receiving Sensitive Medical Information from Hospital Websites, The Markup (June 16, 2022) (available at <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>).

experts, none of which defended the practice of hospitals incorporating such tools onto their properties.

- a. David Holtzman, described as a “health privacy consultant who previously served as a senior privacy advisor in the U.S. Department of Health and Human Services’ Office of Civil Rights” and whose LinkedIn profile states that he served as a consultant for “healthcare organizations in defense of claims or regulatory actions alleging inadequate information privacy and security standards,” stated: (1) “I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it. I cannot say [sharing this data] is for certain a HIPAA violation. It is quite likely a HIPAA violation.”; and (2) “When an individual has sought out a provider and indicated that they want to make an appointment, at that point, any individually identifiable health information that they’ve provided in this session, in the past, or certainly in the future, is protected under HIPAA and could not be shared with a third party like Facebook.”
- b. Iliana Peters, described as “a privacy lawyer with the firm Polsinelli who previously headed HIPAA enforcement for the Office for Civil Rights,” stated, “Generally, HIPAA covered entities and business associates should not be sharing identifiable information with social media companies unless they have HIPAA authorization [from the individual] and consent under state law.”
- c. Glenn Cohen, described as the “faculty director of Harvard Law School’s Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics,” stated, “Almost any patient would be shocked to find out that Facebook is being

provided an easy way to associate their prescriptions with their name. Even if perhaps there's something in the legal architecture that permits this to be lawful, it's totally outside the expectations of what patients think the health privacy laws are doing for them.”

381. State and federal judges have expressed similar sentiments, finding similar allegations stated privacy claims that require conduct that would be considered “highly offensive” to a reasonable person. *See, e.g., In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218 (N.D. Cal. Dec. 22, 2022); *Doe v. Bon Secours Mercy Health*, No. A 2002633, 2021 WL 9939010, at \*4-5 (Ohio C.P. Nov. 22, 2021) (declining to dismiss invasion of privacy claim against hospital that implemented Facebook Pixel on website); *Doe v. Virginia Mason*, 2020 WL 1983046, at \*2 (Wash. Super. Feb. 12, 2020); *Doe v. Medstar*, Case No. 24-C-20-000591 (Baltimore City, Maryland); and *Doe v. Partners*, Case No. 1984-CV-01651 (Suffolk County, Massachusetts).

382. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiffs' and Class Members' privacy because Defendant facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

383. Defendant failed to protect Plaintiffs' and Class Members' Private Information and acted knowingly when it incorporated the Tracking Pixel into its Website because it knew the functionality and purpose of the Tracking Pixel.

384. Because Defendant intentionally and willfully incorporated the Tracking Pixel into its Website and encouraged patients to use that Website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiffs and Class Members. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of

Plaintiffs and Class Members was disclosed to a third party without authorization, causing Plaintiffs and the Class to suffer damages.

385. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

- a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their individually-identifiable patient health information (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiff and Class Members to suffer emotional distress;
- b. Defendant received substantial financial benefits from its use of Plaintiffs' and Class members' individually-identifiable patient health information without providing any value or benefit to Plaintiff or Class Members;
- c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and Class members' individually-identifiable patient health information, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiffs or Class Members; and
- d. Defendant has failed to provide Plaintiff and Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information.

386. Plaintiffs, on behalf of themselves and Class Members, seek nominal, compensatory, and punitive damages for Defendant's invasions of privacy.

387. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class because their Private Information is still maintained by Defendant and still in the possession of Facebook, Google, and/or other third parties, and the wrongful disclosure of the information cannot be undone.

388. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook, who on information and belief continues to possess and utilize that information.

389. Plaintiffs, on behalf of themselves and Class Members, further seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

**COUNT II**  
**INVASION OF PRIVACY – PUBLICATION OF PRIVATE FACTS**  
**(On Behalf of Plaintiffs, the Illinois Class, and the Wisconsin Class)**

390. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

391. Plaintiffs' and Class Members' communications with Defendant constitute private conversations, matters, facts, and data.

392. Plaintiffs and Class Members have a reasonable expectation that Defendant would not disclose personally identifiable patient data and communications to third parties for marketing purposes without Plaintiffs' and other Class Members' authorization, consent, knowledge, or any further action on the patient's part.

393. In addition, Plaintiffs and Class Members have a reasonable expectation that Defendant will not place tracking devices on its own patients' communications devices without their knowledge or consent.

394. Defendant, a health care provider, has a duty to keep personally identifiable patient data and communications confidential.

395. Defendant expressly promised to maintain the confidentiality of personally identifiable patient data and communications in its HIPAA Notice of Privacy Practices.

396. Defendant unlawfully published Plaintiffs' and class Members' private facts by deploying source code that caused the transmission of Plaintiffs' Class Members' PII, PHI, and the contents of communications Plaintiffs and Class Members exchanged with their health care providers to third parties, including Facebook and Google.

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

398. Plaintiffs' and Class Members' Private Information and communications are the type of sensitive, personal information that one normally expects will be protected from disclosure to unauthorized parties by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and Class Members' Private Information and communications, and such information is otherwise protected from exposure to the public by the statutes, regulations, and laws described herein.

399. Defendant's conduct was knowing and intentional as shown by its decision to install the Pixel onto its Website.

400. Defendant's conduct in disclosing Plaintiffs' and Class Members' Private Information and communications to third parties was and is highly offensive to a reasonable person.

401. Defendant's willful and reckless conduct in disclosing Plaintiffs' and Class Members' Private Information and communications to unauthorized third parties is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

402. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

- a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their individually-identifiable patient health information (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiff and the Class Members to suffer emotional distress;
- b. Defendant received substantial financial benefits from its use of Plaintiffs' and the Class Members' individually-identifiable patient health information without providing any value or benefit to Plaintiff or the Class Members;
- c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and the Class Members' individually-identifiable patient health information, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiffs or the Class Members; and

d. Defendant has failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information.

403. Plaintiffs, on behalf of themselves and Class Members, seek nominal, compensatory, and punitive damages for Defendant's invasions of privacy.

404. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class because their Private Information is still maintained by Defendant and still in the possession of Facebook, Google, and/or other third parties, and the wrongful disclosure of the information cannot be undone.

405. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook, who on information and belief continues to possess and utilize that information.

406. Plaintiffs, on behalf of themselves and Class Members, further seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

**COUNT III**  
**UNJUST ENRICHMENT**  
**(On behalf of Plaintiffs, the Illinois Class, and the Wisconsin Class)**

407. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

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

409. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiffs and Class Members and then disclosed to third parties without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

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

411. The benefits that Defendant derived from Plaintiffs and Class Members were not offered by Plaintiffs and Class Members gratuitously and rightly belong to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles in Illinois, Wisconsin, and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

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

**COUNT IV**  
**BREACH OF IMPLIED CONTRACT**  
**(On behalf of Plaintiffs, the Illinois Class, and the Wisconsin Class)**

413. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

414. When Plaintiffs and Class Members provided their user data to Defendant in exchange for services, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

415. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

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

417. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information to third parties, *i.e.*, Facebook and/or Google.

418. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members would not have used Defendant's services, or would have paid substantially less for these services, had they known their Private Information would be disclosed.

419. Plaintiffs and Class Members are entitled to nominal, compensatory, and consequential damages as a result of Defendant's breaches of implied contract.

**COUNT V**  
**BREACH OF CONFIDENCE/PROFESSIONAL NEGLIGENCE**  
**(On behalf of Plaintiffs, the Illinois Class, and the Wisconsin Class)**

420. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

421. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

422. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website and on Defendant's MyChart portal.

423. Plaintiffs' and Class Members' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Privacy Policies.

424. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Tracking Pixel to disclose and transmit Plaintiffs' Private Information and the contents of their communications exchanged with Defendant to third parties.

425. The third-party recipients included, but were not limited to, Facebook and Google.

426. Defendant's disclosures of Plaintiffs' and Class Members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

427. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

428. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiffs and Class Members were damaged by Defendant's breach in that:

- 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 provider-patient relationship;

- c. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensating Plaintiffs for the data;
- d. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- e. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information; and
- f. Defendant's actions violated the property rights Plaintiffs and Class Members have in their Private Information.

429. Plaintiffs, on behalf of themselves and Class Members, seek nominal, compensatory, and punitive damages for Defendant's breaches of confidence.

**COUNT VI**  
**VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")**  
**18 U.S.C. § 2511(1) *et seq.***  
**UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE**  
**(On Behalf of Plaintiffs and the Nationwide Class)**

430. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

431. The ECPA protects both sending and receipt of communications.

432. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

433. The transmissions of Plaintiffs' PII and PHI to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

434. **Electronic Communications.** The transmission of PII and PHI between Plaintiffs and Class Members and Defendant’s Website with which they chose to exchange communications are “transfer[s] of signs, signals, writing, ... data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce” and are therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(2).

435. **Content.** The ECPA defines content, when used with respect to electronic communications, to “include[] *any* information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8) (emphasis added).

436. **Interception.** The ECPA defines the interception as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device” and “contents ... include any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

437. **Electronic, Mechanical, or Other Device.** The ECPA defines “electronic, mechanical, or other device” as “any device ... which can be used to intercept a[n] ... electronic communication[.]” 18 U.S.C. § 2510(5). The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- a. Plaintiffs’ and Class Members’ browsers;
- b. Plaintiffs’ and Class Members’ computing devices;
- c. Defendant’s web-servers; and
- d. The Pixel Code deployed by Defendant to effectuate the sending and acquisition of patient communications

438. By utilizing and embedding the Pixel on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

439. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Pixel imbedded and ran on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiffs' and Class Members' electronic communications to third parties, including Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

440. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Pixel imbedded and ran on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiffs' and Class Members' electronic communications, for purposes other than providing health care services to Plaintiff and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

441. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally redirected the contents of Plaintiffs' and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

442. Defendant's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiffs' and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

443. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

444. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

445. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

446. Defendant was not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communication.

447. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' privacy via the Pixel tracking code.

448. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

449. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

450. The ECPA provides that a “party to the communication” may liable where a “communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C § 2511(2)(d).

451. Defendant is a “party to the communication” with respect to patient communications. However, Defendant’s simultaneous, unknown duplication, forwarding, and interception of Plaintiffs’ and Class Members’ Private Information does not qualify for the party exemption.

452. Defendant’s acquisition of patient communications that were used and disclosed to Facebook and Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States, Wisconsin, and Illinois, including.

- a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;
- b. Violation of the Illinois Computer Fraud Act, 720 ILCS 5/17-50;
- c. Violation of the Illinois Computer Crime Prevention Law, 720 ILCS 5/17-51;
- d. Violation of the Illinois Deceptive Trade Practices Act, 815 ILCS §§ 510/2, et seq.
- e. Violation of Illinois Stat. § 410 ILCS 50;
- f. Violation of 815 Ill. Comp. Stat. §§ 505/1 et seq.;
- g. Violation of Wis. Stat. §§ 100.18, et seq.;
- h. Violation of Wis. Stat. §§ 146.81, et seq.;
- i. Violation of Wis. Stat. §§100.18, et seq.;
- j. Violation of Wis. Stat. §§ 905.04, et seq.;
- k. Violation of Wis. Stat. §§ 995.50, et seq.; and
- l. Invasion of Privacy.

453. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to “use[] or cause[] to be used a unique health identifier” or to “disclose[] individually identifiable health information to another person ... without authorization” from the patient.

454. The penalty for violation is enhanced where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320d-6.

455. Defendant’s conduct violated 42 U.S.C. § 1320d-6 in that it:

- a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and
- b. Disclosed individually identifiable health information to Facebook and Google without patient authorization.

456. Defendant’s conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant’s use of the Facebook and Google source code was for Defendant’s commercial advantage to increase revenue from existing patients and gain new patients.

457. Under 720 ILCS, 17-50, “[a] person commits computer fraud when he or she knowingly:

- a. Accesses or causes to be accessed a computer or any part therefor, or a program or data, with the intent of devising or executing any scheme or artifice to defraud, or as part of a deception;
- b. Obtains use of, damages, or destroys a computer or any part thereof, or alters, deletes, or removes any program or data contained therein, in connection with any scheme or artifice to defraud, or as part of a deception; or

- c. Access or causes to be accessed a computer or any part thereof, or a program or data, and obtains money or control over any such money, property, or services of another in connection with any scheme or artifice to defraud, or as part of a deception.

458. Defendant violated the Illinois Computer Fraud Act in that:

- a. Defendant accessed Plaintiffs' and Class Members' computing devices and data as part of a deception and without their authorization, including through placement of the fbp, ga, and gid cookies as well as use of source code that commanded Plaintiffs' and Class Members' computing devices to send identifiers and the content of communications with Defendant simultaneously to Defendant and Facebook, Google, and others;
- b. Defendant obtained use of or and removed data from Plaintiffs' and Class Members' computing devices as part of a deception and without their authorization, including through placement, use, and removal of the fbp, ga, and gid cookies as well as use of source code that commanded Plaintiffs' and Class Members' computing devices to send identifiers and the content of communications with Defendant simultaneously to Defendant and Facebook, Google, and others;
- c. Defendant accessed or caused to be accessed the Plaintiffs' and Class Members' computing devices and data, and thereby obtained control over the Plaintiffs' and Class Members' property in the form of their computing devices and right to control access and use of their personal health information as part of a deception and without their authorization, including through placement of the

fbp, ga, and gid cookies as well as the use of source code that commanded Plaintiffs' and Class Members' computing devices to send identifiers and the content of communication with Defendant simultaneously to Facebook, Google, and others.

459. The Illinois Computer Crime Prevention Law (“ICCPL”) prohibits “computer tampering,” and provides a private right of action for whoever “suffers loss by reason of a violation of subdivision (a)(4).” 720 ILCS 5/17-51(c).

460. Subdivision (a)(4) of the ICCPL provides: “a) A person commits computer tampering when he or she knowingly and without the authorization of a computer’s owner or in excess of the authority granted to him or her: ... (4) Inserts or attempts to insert a program into a computer or computer program knowing or having reason to know that such program contains information or commands that will or may...(b) alter, delete, or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer; or (c) cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such program...”

461. Defendant violated the ICCPL when it knowingly and without Plaintiffs' or Class Members' authorization inserted the fbp, ga, and gid cookies on Plaintiffs' and Class Members' computing devices.

462. The fbp, ga, and gid cookies, which constitute programs, commanded Plaintiffs' and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendant to Google, Facebook, and others.

463. Defendant knew or had reason to know that the fbp, ga, and gid cookies would command Plaintiffs' and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendant to Google, Facebook, and others.

464. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class Members' communications about their individually-identifiable patient health information on its Website, because it used its participation in these communications to improperly share Plaintiffs' and Class Members' individually-identifiable patient health information with Facebook and Google, third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know was receiving their individually-identifiable patient health information, and that Plaintiffs and Class Members did not consent to receive this information.

465. As such, Defendants cannot viably claim any exception to ECPA liability.

466. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

- a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their individually-identifiable patient health information (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiff and the Class Members to suffer emotional distress;
- b. Defendant received substantial financial benefits from its use of Plaintiffs' and the Class Members' individually-identifiable patient health information without providing any value or benefit to Plaintiff or the Class Members;

- c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and the Class Members' individually-identifiable patient health information, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiffs or the Class Members;
- d. Defendant has failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and
- e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

467. As a result of Defendant's violation of the ECPA, Plaintiffs are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

**COUNT VII**  
**VIOLATION OF CONFIDENTIALITY OF PATIENT HEALTH CARE RECORDS**  
**Wis. Stat. § 146.81, *et seq.***  
**(On Behalf of Plaintiffs and the Wisconsin Class)**

468. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

469. Under Wisconsin law all patient health care records must remain confidential and patient health care records may only be released to a person upon the informed consent of the patient, or as authorized by the patient.

470. Defendant disclosed the private and protected medical information of Plaintiffs and Class Members to unauthorized third parties without their knowledge, consent, or authorization.

471. Defendant is a healthcare provider as defined by Wis. Stat. § 146.816(1).

472. Plaintiffs and Class Members are patients, and, as a health care provider, Defendant had and has an ongoing obligation not to disclose their Private Information.

473. The Private information disclosed by Defendant is protected health information as defined by Wis. Stat. § 146.816(f).

474. Defendant violated Wis. Stat. § 146.81, *et seq.* through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class. Defendant's conduct with respect to the disclosure of its patients' confidential Private Information was willful and knowing because Defendant configured and implemented the digital platforms and tracking software that gave rise to the disclosure and interception of the Private Information.

475. Plaintiffs and Class Members were injured as a result of Defendant's violation of the confidentiality of patient health care law.

476. As a result of its intentional and willful disclosure of Private Information, Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, punitive damages, restitution, reasonable attorneys' fees and costs, and any other relief that is just and proper.

**COUNT VIII**  
**WISCONSIN DECEPTIVE TRADE PRACTICES ACT**  
**Wis. Stat. §§100.18, *et seq.***  
**(On behalf of Plaintiffs and the Wisconsin Class)**

477. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

478. Defendant's conduct violates Wisconsin's Deceptive Trade Practices Act, Wis. Stat. §100.18 (the "WDTPA"), which provides that no,

"firm, corporation or association ... with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading."

479. Plaintiffs and Class Members "suffer[ed] pecuniary loss because of a violation" of the WDTPA. Wis. Stat. § 100.18(11)(b)(2).

480. Plaintiffs and Class Members relied on and had the reasonable expectation that Defendant (i.e., a healthcare network) would protect their Private Information and comply with all common law, state, and federal privacy laws designed to protect their Private Information.

481. Defendant engaged in deceptive and unfair acts and practices, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the WDPTA, including, but not limited to, the following: (1) promising to protect Plaintiffs' and Class Members' Private Information via its Privacy Policies and then, in fact,

knowingly, transmitting Plaintiffs' and Class Members' Private Information to third parties, such as Facebook and Google; (2) unlawfully disclosing Plaintiffs' and Class Members' Private Information to third parties such as Facebook and Google; (3) failing to disclose or omitting material facts that that Plaintiffs' and Class Members' Private Information would be disclosed to third parties; (4) failing to obtain Plaintiffs' and Class Members' consent in transmitting Plaintiffs' and Class Members' Private Information to third parties, such as Facebook and Google; and (5) knowingly violating industry and legal standards regarding the protection of Plaintiffs' and Class Members' Private Information.

482. These actions also constitute deceptive and unfair acts or practices because Defendant knew its Website contained the Tracking Pixel and also knew the Pixel would be unknown and/or not easily discoverable by Plaintiffs and Class Members.

483. Defendant intended that Plaintiffs and the Wisconsin Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

484. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiffs and Class Members have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

485. As a result of Defendant's wrongful conduct, Plaintiffs and Class Members were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII and PHI from being hacked and taken and misused by others.

486. As a direct and proximate result of Defendant's violations of the WDTPA, Plaintiffs and the Wisconsin Class have suffered harm, including the diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private; financial losses related to the payments made to Defendant that Plaintiffs and the Wisconsin Class would not have made had they known of Defendant's disclosure of their Private Information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

487. Plaintiffs and Class Members are entitled to reasonable attorney fees and costs, and other relief that the Court deems proper.

**COUNT IX**  
**VIOLATION OF STATUTORY DUTY TO MAINTAIN CONFIDENTIALITY OF**  
**PATIENT HEALTHCARE RECORDS**  
**Illinois Stat. § 410 ILCS 50, et seq.**  
**(On Behalf of Illinois Plaintiffs and the Illinois Class)**

488. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

489. Under Illinois law all patient health care records must remain confidential and patient health care records may only be released to a person upon the informed consent of the patient, or as authorized by the patient.

490. Defendant disclosed the private and protected medical information of Plaintiffs and Class Members to unauthorized third parties without their knowledge, consent, or authorization.

491. Defendant is a healthcare services corporation and provider as defined by 410 ILCS 501 2.02 and 2.03.

492. Plaintiffs and Class Members are patients, and, as a health care provider, Defendant had and has an ongoing obligation not to disclose their Private Information.

493. The Private information disclosed by Defendant is protected health information under the Illinois Medical Patient Rights Act.

494. Defendant violated 410 ILCS 50, *et seq.*, through its willful and knowing failure to maintain and preserve the confidentiality of the Private Information of Plaintiffs and the Class. Defendant's conduct with respect to the disclosure of its patients' confidential Private Information was willful and knowing because Defendant configured and implemented the digital platforms and tracking software that gave rise to the disclosure and interception of the Private Information.

495. Plaintiffs and Class Members were injured as a result of Defendant's violation of the confidentiality of the Medical Patients' Rights Act, which imposed a duty of confidentiality on Defendant.

496. As a result of its intentional and willful disclosure of Plaintiffs and Class Members' Private Information, Defendant is liable to Plaintiffs and Class Members for damages, whether nominal or actual and punitive damages.

**COUNT X**  
**VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("CFA")**

**815 Ill. Comp. Stat. §§ 505/1, *et seq.***  
**(On behalf of Illinois Plaintiffs and the Illinois Class)**

497. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

498. Plaintiffs and the Illinois Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiffs, the Illinois Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

499. Defendant engaged in “trade” or “commerce,” including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of “merchandise” (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

500. Defendant engaged in deceptive and unfair acts and practices and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including, but not limited to, the following: (1) promising to protect Plaintiffs’ and Class Members’ Private Information via its Privacy Policies and then, in fact, knowingly, transmitting Plaintiffs’ and Class Members’ Private Information to third parties, such as Facebook and Google; (2) unlawfully disclosing Plaintiffs’ and Class Members’ Private Information to third parties such as Facebook and Google; (3) failing to disclose or omitting material facts that that Plaintiffs’ and Class Members’ Private Information would be disclosed to third parties; (4) failing to obtain Plaintiffs’ and Class Members’ consent in transmitting Plaintiffs’ and Class Members’ Private Information to third parties, such as Facebook and Google; and (5) knowingly violating industry and legal standards regarding the protection of Plaintiffs’ and Class Members’ Private Information.

501. These actions also constitute deceptive and unfair acts or practices because Defendant knew its Website contained the Pixel and also knew the Pixel would be unknown and/or not easily discoverable by Plaintiffs and Class Members.

502. Defendant intended that Plaintiffs and the Illinois Class rely on its unfair acts and practices and the concealment and omission of material facts in connection with Defendant’s offering of goods and services.

503. Defendant’s wrongful practices were and are injurious to the public because those practices were part of Defendant’s generalized course of conduct that applied to the Illinois Class.

Plaintiffs and the Illinois Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

504. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiffs and the Illinois Class of the nature and extent of the disclosure of their Private Information pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.*

505. As a result of Defendant's wrongful conduct, Plaintiffs and the Illinois Class were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII and PHI from being disclosed to and intercepted by others.

506. As a direct and proximate result of Defendant's violations of the CFA, Plaintiffs and the Illinois Class have suffered harm, including the diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private; financial losses related to the payments made to Defendant that Plaintiffs and the Wisconsin Class would not have made had they known of Defendant's disclosure of their Private Information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

507. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Illinois Plaintiffs and the Illinois Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

**COUNT XI**  
**VIOLATIONS OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT**  
**(“DTPA”)**  
**815 ILCS §§ 505/2, *et seq.***  
**(On behalf of Illinois Plaintiffs and the Illinois Class)**

508. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

509. Defendant is a “person” as defined by 815 ILCS § 510/1(5).

510. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of 815 ILCS § 510/2(a), including: a. Representing that goods or services have characteristics that they do not have; b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; c. Advertising goods or services with intent not to sell them as advertised; and d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

511. Defendant’s practice of disclosing Plaintiffs’ and Class Members’ personally identifiable data and re-directing their communications to third parties without authorization, consent, or knowledge is a deceptive trade practice, in violation of 815 ILCS § 510/2(a).

512. Defendant’s practice of disclosing Plaintiffs’ and Class Members’ personally identifiable data and re-directing their communications to third parties without authorization, consent, or knowledge was willful.

513. Defendant’s practice of disclosing Plaintiffs’ and Class Members’ personally identifiable data and re-directing their communications to third parties without authorization, consent, or knowledge was intentional.

514. Defendant's omissions were material because they were likely to deceive reasonable consumers about the privacy, security, and use of their personally identifiable patient data and communications when using Defendant's Website, including the MyChart patient portal.

515. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

516. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive trade practices, Plaintiffs and the Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including (1) overpaying for Defendant's health care services, (2) loss of value of their personally identifiable patient data and communications, and (3) injured privacy interests.

517. Plaintiffs and the Class Members are patients of Defendant and need access to Defendant's Website and the MyChart portal in connection with receiving health care from Defendant. Because Plaintiffs and Class Members need to, and so will continue to use Defendant's web properties in the future, if Defendant's unfair, unlawful, and deceptive trade practices are allowed to continue, Plaintiffs and Class Members are likely to suffer continuing harm in the future.

518. Plaintiffs and the Class Members seek all relief allowed by law, including injunctive relief and reasonable attorney's fees.

#### **PRAYER FOR RELIEF**

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

- A. For an Order certifying the Nationwide Class, Wisconsin Class, and Illinois Class, and appointing Plaintiffs and their Counsel to represent the Classes;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members:
- D. For an award of damages, including, but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

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

Date: May 5, 2023

Respectfully submitted,

/s/ Gary M. Klinger  
Gary M. Klinger  
**MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN, PLLC**  
227 Monroe Street, Suite 2100  
Chicago, IL 60606  
Phone: 866.252.0878  
*gklinger@milberg.com*

Terence R. Coates  
Dylan J. Gould  
**MARKOVITS, STOCK & DEMARCO, LLC**  
119 East Court Street, Suite 530  
Cincinnati, OH 45202  
Telephone: (513) 651-3700  
Fax: (513) 665-0219  
*tcoates@msdlegal.com*  
*dgould@msdlegal.com*

*Interim Co-Lead Class Counsel*

David K. Lietz  
**MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN, PLLC**  
5335 Wisconsin Avenue NW, Suite 440  
Washington, D.C. 20015-2052  
Telephone: (866) 252-0878  
Facsimile: (202) 686-2877  
*dlietz@milberg.com*

Joseph M. Lyon  
**THE LYON LAW FIRM, LLC**  
2754 Erie Ave.  
Cincinnati, OH 45208  
Phone: (513) 381-2333  
Fax: (513) 766-9011  
*jlyon@thelyonfirm.com*

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

Nola J. Hitchcock Cross  
**CROSS LAW FIRM, S.C.**  
WI State Bar No. 1015817  
Mary C. Flanner  
WI State Bar No. 1013095  
845 North 11th St.  
Lawyers' Building  
Milwaukee, Wisconsin 53233  
Tel: (414) 224-0000  
Fax: (414) 273-7055  
*njhcross@crosslawfirm.com*  
*mflanner@crosslawfirm.com*

Stephen R. Basser\*  
**BARRACK RODOS & BACINE**  
Calif. State Bar No. 121950  
E-mail: sbasser@barrack.com  
Samuel M. Ward\*  
Calif. State Bar No. 216562  
E-mail: sward@barrack.com  
One America Plaza  
600 West Broadway, Ste. 900  
San Diego, California 92101

John Emerson\*  
**EMERSON FIRM LLP**  
2500 Wilcrest, Ste. 300  
Dallas, Texas 77042  
*jemerson@emersonfirm.com*  
Phone: (800) 551-8649  
Fax: (501) 286-4659

Ryan F. Stephan  
James B. Zouras  
Teresa M. Becvar  
Mohammed A. Rathur  
**STEPHAN ZOURAS, LLP**  
222 W. Adams Street  
Suite 2020  
Chicago, Illinois 60606  
(312) 233-1550  
(312) 233-1560  
*rstephan@stephanzouras.com*  
*jzouras@stephanzouras.com*  
*tbecvar@stephanzouras.com*  
*mrathur@stephanzouras.com*

Bryan Paul Thompson  
Robert W. Harrer  
**CHICAGO CONSUMER LAW CENTER, P.C.**  
650 Warrenville Road, Suite 100  
Lisle, IL 60532  
Tel. 312-858-3239  
Fax 312-610-5646  
Bryan.thompson@cclc-law.com  
Rob.harrer@cclc-law.com

Michael Kind, Esq.  
**KIND LAW**  
8860 S. Maryland Parkway, Suite 106  
Phone: (702) 337-2322  
FAX: (702) 329-5881  
Email: mk@kindlaw.com

*Counsel for Plaintiffs and Putative Classes*

*\*Bar application forthcoming*