Exhibit A1

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS

PATRICIA MAYER, CATHERINE MASSARELLI and MARY MURPHY, *individually and on behalf of all others similarly situated*, Plaintiffs, v. MIDWEST PHYSICIAN ADMINISTRATIVE SERVICES, LLC d/b/a DULY HEALTH AND CARE, Defendant.	Case No. 1:23-cv-3132 **Judge Mary M. Rowland**

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs PATRICIA MAYER, CATHERINE MASSARELLI and MARY MURPHY ("Plaintiffs") bring this class action lawsuit in their individual capacity and on behalf of all others similarly situated against MIDWEST PHYSICIAN ADMINISTRATIVE SERVICES, LLC d/b/a DULY HEALTH AND CARE ("Duly" or "Defendant") and allege, upon personal knowledge as to their own actions, their counsel's investigation and upon information and good faith belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Duly boldly proclaims on its "Notice of Privacy Practices" the lengths it will *supposedly* go to protect its patients' personal and protected health information:

> Nothing is more important than [] ensuring your privacy. At Duly Health and Care, ***we understand that your privacy is vitally important***. As your medical provider, we take proactive measures to safeguard your information. We understand that with each office visit, you are placing your trust in us. ***We will make every effort to ensure this trust is not breached, and that your privacy is***

protected.[1]

2. As detailed herein, those statements are certainly suspect given Defendant's illegal and widespread practice of disclosing Plaintiffs' and putative Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to herein as "Private Information") to third parties, including, but not necessarily limited to, Meta Platforms, Inc. d/b/a Meta ("Meta").

3. Information about a person's physical and mental health is among the most confidential and sensitive information in our society and the mishandling of such information can have serious consequences, including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.[2]

4. Simply put, if people do not trust that their sensitive Private Information will be kept private they may be less likely to seek medical treatment which can lead to much more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical providers is vitally necessary to maintain public trust in the healthcare system as a whole.

---

[1] *See* https://www.dulyhealthandcare.com/hipaa-privacy-policy (last visited February 28, 2024) (emphasis added).

[2] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), available at https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited February 28, 2023) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized."); *see also* Tood Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *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 (last visited February 28, 2024).

5. Protected and highly sensitive medical information collected by healthcare entities includes many categories, from intimate details of an individual's treatment to any unique identifying code which can connect the individual to the collecting entity.

6. Even IP addresses – which in theory could be connected to several members of the same household – are considered PHI *even when the individual does not have an existing relationship with the regulated healthcare entity* since when the medical provider collects this information through its website or mobile app, it is indicative that the individual has received or will receive health care services or benefits from the medical provider.[3]

Duly Collects a Significant Amount of Private Information.

7. Defendant owns, controls and maintains a website, https://www.dulyhealthandcare.com/ (the "Website"), which it encourages patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, signing up for events and classes and more.

8. Defendant also maintains a web-based portal called MyChart (the "Portal") and an application (the "App") whereby registered users can access their account to: (i) communicate with their doctors; (ii) access lab and test results; (iii) manage prescriptions and request refills and (iv) manage appointments, among other things.[4]

---

[3] USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaaonline-tracking/index.html (last visited February 28, 2024).

[4] https://mychart.dupagemd.com/MyChart/Authentication/Login? (last visited February 28, 2024).

9. The Website, the Portal and the App are referred to herein as the "Web Properties."

10. Plaintiffs and Class Members who visited and used (collectively, the "Users") Defendant's Web Properties understandably thought they were communicating *only* with their trusted healthcare provider.

11. Unbeknownst to Plaintiffs and Class Members, however, Defendant had embedded the Meta Tracking Pixel (the "Pixel" or "Meta Pixel") on its Web Properties which automatically transmits to Meta every click, keystroke and detail about their medical treatment.[5]

12. Operating as designed and as implemented by Duly, the Pixel allows the Private Information that Plaintiffs and Class Members provide to Defendant to be unlawfully disclosed to Meta alongside the individual's unique and persistent Facebook ID ("FID").[6]

13. A pixel is a piece of code that "tracks the people and [the] type of actions they take".[7] as they interact with a website (or other digital property), including how long a person spends on a particular web page, which buttons the person clicks, which pages they view and the text or phrases they type into various portions of the website (such as a general search bar, chat

---

[5] Plaintiffs' research shows that the Meta Pixel was embedded in Defendant's Website at the time of the filing of the original complaint (see discussion *infra*). While there is no way to confirm with certainty that Defendant has installed the Pixel in its other Web Properties without access to the host server, upon information and good faith belief, Defendant's Portal and the App are tracking Users' activities through the Meta Pixel as well.

[6] The Pixel forces the website user to share the FID for easy tracking via the "cookie" Meta stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser"; "[c]ookies help inform websites about the user, enabling the websites to personalize the user experience." *See* https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited February 28, 2024).

[7] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited February 28, 2024).

feature or text box), among other things.

14. The User's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Meta Pixel is thus customizable and programmable, meaning that the website owner controls which of its web pages contain the Pixel and which events are tracked and transmitted to Meta.

15. By installing the Meta Pixel, Defendant effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled them to unknowingly disclose their private, sensitive and confidential health-related communications with Defendant to Meta.

16. In addition to the Meta Pixel, Defendant, upon information and good faith belief, also installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its Web Properties' servers.[8]

17. Unlike the Meta Pixel, which coopts a website user's browser and forces it to disclose information to third parties in addition to the website owner, CAPI does not cause the User's browser to transmit information directly to Meta. Rather, CAPI tracks the User's website interaction, including Private Information, records and stores that information on the website owner's servers and then transmits the data to Meta from the website owner's servers.[9,10]

---

[8] CAPI "works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited February 28, 2024).

[9] https://revealbot.com/blog/facebook-conversions-api/ (last visited February 28, 2024).

[10] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." https://developers.facebook.com/docs/marketing-api/conversions-api (last visited February 28, 2024).

18. Indeed, Meta markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[11]

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

20. The decision to use the Pixel and CAPI was made by Defendant.

21. Defendant utilized the Pixel and CAPI data for marketing purposes in an effort to bolster its profits; that is, despite professing that "[n]othing is more important than[] ensuring your privacy,"[12] Duly put its own desires for profit over its patients' privacy rights.

22. The Meta Pixel and CAPI are routinely used to target specific customers by utilizing data to build incredibly fulsome and robust profiles for the purposes of retargeting and future marketing. Meta also uses Plaintiffs' and Class Members' Private Information to create targeted advertisements based on the medical conditions and other Private Information disclosed to Defendant.

23. The information that Defendant's Tracking Pixel and CAPI sent to Meta included the Private Information that Plaintiffs and Class Members submitted to Defendant's Web Properties, including, for example, patient status, the type of medical treatment sought, the

---

[11] https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited February 28, 2024).

[12] *See* https://www.dulyhealthandcare.com/hipaa-privacy-policy (last visited February 28, 2024).

individual's particular health condition and the fact that the individual attempted to or did book a medical appointment.

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

25. Meta and any third-party purchasers of Plaintiffs' and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia or HIV.

Duly's Disclosure of Users' Private Information Without Consent Violates the Law.

26. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its web pages to an undisclosed third party – let alone Meta, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue – without the patients' informed and express consent.

27. Neither Plaintiffs nor any other Class Member were provided, much less signed, a written authorization permitting Defendant to disclose their Private Information to Meta.

28. Despite willfully and intentionally incorporating the Meta Pixel and CAPI into its Web Properties and servers, Defendant has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Meta.[13]

[13] In contrast to Defendant, several medical providers which have installed the Meta Pixel on their web properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*,

29. Defendant's overall intent and purpose in acquiring Users' personal health data was to increase its ability to market and retarget its Users, thereby increasing its profit while violating HIPAA, state and federal statutes and common law.

30. Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted to Meta as they communicated with their healthcare providers via Defendant's Web Properties or that their information was stored on Defendant's servers to be later transmitted to Meta so it could be used for targeted advertising and marketing purposes.

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

32. The disclosure of Plaintiffs' and Class Members' Private Information via the Pixel contravenes the letter and spirit of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). As part of HIPAA, the United States Department of Health and Human Services ("HHS") established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") which governs how health care providers must safeguard and protect Private Information.

33. Simply put, further to the HIPAA Privacy Rule, covered entities such as Duly are ***not*** permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private

---

https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited February 28, 2024); *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3 (last visited February 28, 2024); *Novant Health Notifies 1.3M Patients of Unauthorized PHI Disclosure Caused By Meta Pixel* (Aug. 17, 2022), https://healthitsecurity.com/news/novant-health-notifies-patients-of-unauthorizd-phi-disclosure-caused-by-meta-pixel ((last visited February 28, 2024).

Information to any third-party without express and informed consent from each patient.

34. Lest there be any doubt of the illegal nature of Defendant's practice, the Office for Civil Rights (OCR) at HHS has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[14]

35. The HHS Bulletin does not change any existing rule or impose any new obligation on HIPAA-covered entities. Instead, it reminds these entities of their long-standing obligations by referring to guidance and rules that have been in place for decades. *Id.* ("[I]t has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors").

36. Defendant further made express and implied promises to protect Plaintiffs' and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendant. Furthermore, by obtaining, collecting, using and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and to safeguard that information from unauthorized disclosure.

37. Duly breached its statutory and common law obligations to Plaintiffs and Class

---

[14] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited February 28 2024) (emphasis added).

Members by, *inter alia*: (i) failing to adequately review its marketing programs and web based technologies to ensure the Website and its other Web Properties were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Users' Private Information; (iii) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Meta or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Meta Pixels; (v) failing to warn Plaintiffs and Class Members of sharing their Private Information with third parties and (vi) otherwise failing to design and monitor its Website and other Web Properties to maintain the confidentiality, security and integrity of patient Private Information.

38. As a result, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Pixel, (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 their Private Information.

39. Plaintiffs therefore seek, on behalf of themselves and a class of similarly situated persons, to remedy these harms and asserts the following statutory and common law claims against Duly: (i) violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(1), *et seq.*; (ii) violations of Illinois Eavesdropping Statute, 720 ILCS 5/14-1, *et seq.*; (iii) violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* ("ICFA"); (iv) violations of the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS §§ 510/2, *et seq.* ("IUDTPA"); (v) breach of confidence; (vi) invasion of privacy; (vii) common law invasion of privacy – intrusion upon seclusion; (viii) breach of implied contract and (ix) negligence.

PARTIES

40. Plaintiff Patricia Mayer is a natural person and citizen of Illinois, residing in Cook County, Illinois, where she intends to remain.

41. Plaintiff Catherine Massarelli is a natural person and citizen of Illinois, residing in Cook County, Illinois, where she intends to remain.

42. Plaintiff Mary Murphy is a natural person and citizen of Illinois, residing in DuPage County, Illinois, where she intends to remain.

43. Defendant Midwest Physician Administrative Services, LLC, doing business as Duly Health and Care, is an Illinois Limited Liability Company based in Downers Grove, Illinois.[15]

44. Duly provides all manner of primary, specialty and multi-disciplinary care at over 150 locations throughout Illinois.[16] Defendant is a covered entity under HIPAA.

JURISDICTION & VENUE

45. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under federal law, specifically the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq*. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

46. This Court also has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(d), which expressly provides federal courts with jurisdiction over any class action in which: the proposed class includes at least 100 members; any

[15] As of September 2021, DuPage Medical Group was renamed Duly Health and Care.

[16] https://www.dulyhealthandcare.com/ (last visited February 28, 2024).

member of the class is a citizen of a state and any defendant is a citizen or subject of a foreign state; and the amount in controversy exceeds $5,000,000.00, exclusive of interest and costs.

47. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in this District. Further, Duly is authorized to and regularly conducts business in this District and makes decisions regarding corporate governance and management of its Web Properties in this District, including decisions regarding the privacy of Users' Private Information and the incorporation of the Meta Pixel and other tracking technologies.

48. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant does business in, and is subject to, personal jurisdiction in this District. Venue is also proper in this District, because a substantial part of the events or omissions giving rise to the claim occurred in, and emanated from, this District.

COMMON FACTUAL ALLEGATIONS

A. Background: The Use of Tracking Technologies in the Healthcare Industry

49. Tracking tools installed on many hospitals', telehealth companies' and other healthcare providers' websites (and other digital properties) are collecting patients' and other visitors' confidential and private health information—including details about their medical conditions, prescriptions and appointments, among *many* other things—and sending that information to third party vendors without prior, informed consent.

50. These pixels are snippets of code that tracks users as they navigate through a website, logging which pages they visit, which buttons they click and certain information they enter into forms. In exchange for installing the pixels, the third-party platforms (*e.g.,* Meta and Google) provide website owners analytics about the advertisements they have placed as well as tools to target people who have visited their web properties.

51. While the information captured and disclosed without permission may vary depending on the pixel(s) embedded, these "data packets" can be extensive, sending, for example, not just the name of the physician and her field of medicine, but also the first name, the last name, email address, phone number and zip code and city of residence entered into the booking form.

52. That data is linked to a specific internet protocol ("IP") address. The Meta Pixel, for example, sends information to Meta via scripts running in a person's internet browser so each data packet comes labeled with an IP address that can be used in combination with other data to identify an individual or household.

53. In addition, if the person is (or recently has) logged into Facebook when they visit a particular website when a Meta Pixel is installed, some browsers will attach third-party cookies—another tracking mechanism—that allow Meta to link pixel data to specific Facebook accounts.

54. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to surreptitiously capture and to disclose their Users' personal health information.

55. Specifically, and for example, The Markup reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Meta a packet of data whenever a person clicked a button to schedule a doctor's appointment.[17]

B. Duly Utilized Tracking Technology for the Purpose of Disclosing Plaintiffs' and Class Members' Private Information to Meta.

[17] *See, e.g.*, Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *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 (last visited February 28, 2024).

56. Defendant purposely installed the Pixel and CAPI tools on its Web Properties and programmed the Web Properties to surreptitiously share its patients' private and protected communications with Meta, including communications that contain Plaintiffs' and Class Members' Private Information.

57. On numerous occasions during the relevant Class Period, Plaintiffs accessed Defendant's Website and Portal on their digital devices and used the Website and the Portal to look for providers, to arrange care and treatment, to make appointments, to check payment history and for other billing matters.

58. Plaintiffs have used and continue to use the same devices to maintain and to access active Facebook accounts throughout the relevant period in this case.

59. Further to the systematic process described herein, Duly assisted Meta with intercepting Plaintiffs' communications including those that contained personally identifiable information, protected health information and related confidential information.

60. Defendant assisted these interceptions without Plaintiffs' knowledge, consent or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiffs' personally identifiable information and protected health information.

61. Defendant uses its Website to connect Plaintiffs and Class Members to Defendant's digital healthcare Web Properties with the goal of increasing profitability.

62. In order to understand Defendant's unlawful data sharing practices, it is important to first understand basic web design and tracking tools.

C. Meta's Business Tools & the Pixel

63. Meta operates the world's largest social media company and generated $117 billion

in revenue in 2021, roughly 97% of which was derived from selling advertising space.[18]

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

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

66. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[19]

67. Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[20]

---

[18] 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 February 28, 2024).

[19] SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited February 28, 2024); *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 February 28, 2024).

[20] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited February 28, 2024).

68. One such Business Tool is the Pixel which "tracks the people and type of actions they take."[21]

69. When a user accesses a web page that is hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Meta's servers—traveling from the user's browser to Meta's server.

70. Notably, this transmission only occurs on webpages that contain the Pixel. Thus, Plaintiffs' and Class Members' Private Information would not have been disclosed to Meta but for Defendant's decisions to install the Pixel on its Website.

71. Similarly, Plaintiffs' and Class Members' Private Information would not have been disclosed to Meta via CAPI but for Defendant's decision to install and implement that tool.

72. By installing and implementing both tools, Defendant caused Plaintiffs' and Class Members' communications to be intercepted and transmitted to Meta via the Pixel, and it caused a second improper disclosure of that information via CAPI.

73. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via the Website.

D. Conversions API.

74. Facebook Conversions API ("CAPI") and similar tracking technologies allow businesses to send web events, such as clicks, form submissions, keystroke events and other user actions performed by the user on the Website, from their own servers to Meta and other third parties.[22]

---

[21] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited February 28, 2024).

[22] *See* https://revealbot.com/blog/facebook-conversions-api/ (last visited Feb. 28, 2024).

75. CAPI creates a direct and reliable connection between marketing data (such as website events and offline conversations) from Duly's server to Meta.[23] In doing so, Duly stores Plaintiffs' and Class Members' Private Information on its own server and then transmits it to unauthorized third parties, *i.e.*, Meta.

76. CAPI is an alternative method of tracking versus the Meta Pixel because no privacy protections on the user's end can defeat it. This is because it is "server-side" implementation of tracking technology, whereas the Pixels are "client-side"—executed on users' computers in their web browsers.

77. Because CAPI is server-side, it cannot access the Facebook c_user cookie to retrieve the Facebook ID.[24] Therefore, other roundabout methods of linking the user to their Facebook account are employed.[25]

78. Facebook has an entire page within its developers' website about how to de-duplicate data received when both the Meta Pixel and CAPI are executed.[26]

---

[23] *See* https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Feb. 28, 2024).

[24] "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses and phone numbers, that we use for matching purposes only." *See* https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/ (last visited Feb. 28, 2024).

[25] "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req- rec-params (last visited Feb. 28, 2024).

[26] *See* https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel- and-server-events (last visited Feb. 28, 2024).

79. CAPI tracks the user's website interactions, including Private Information being shared, and then transmits this data to Meta and other third parties. Meta markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[27]

80. Duly installed the Meta Pixels and, upon information and good faith belief, CAPI, as well as other tracking technologies, on many (if not all) of the webpages within its Web Properties (including the member-only patient portal) and programmed or permitted those webpages to surreptitiously share patients' private and protected communications with the Meta—communications that included Plaintiffs' and Class Members' Private Information.

81. Plaintiffs' and Class Members' Private Information would not have been disclosed to Meta via CAPI but for Defendant's decision to install and implement that tool.

82. By installing and implementing both tools, Defendant caused Plaintiffs' and Class Members' communications to be intercepted and transmitted to Meta via the Pixel, and it caused a second improper disclosure of that information via CAPI.

83. While Duly patients navigate Duly's Web Properties, the Web Properties routinely provides Meta with its patients' Facebook IDs, IP addresses and/or device IDs and the other information they input into Duly's Web Properties, including not only their medical searches, treatment requests and the webpages they view, but, upon information and good faith belief, also their name, email address and/or phone number.

[27] *About Conversions API*, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Feb. 28, 2024).

84. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[28] 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.

85. Instead of taking proactive steps to verify that businesses using the Pixel obtain the required consent, Meta uses an "honor system" under which Meta assumes these businesses have "provided robust and sufficient prominent notice to users regarding the Business Tool Data collection, sharing, and usage."[29]

86. After intercepting and collecting this information, Meta processes it, analyzes it and assimilates it into datasets, such as Core Audiences and Custom Audiences. When the website visitor is also a Meta user, the information collected via the Meta Pixel is associated with the user's Facebook ID that identifies their name and Facebook profile—their real-world identity.

87. The pixel collects data regardless of whether the visitor has an account. Meta maintains "shadow profiles" on users without Facebook accounts, and links the information collected via the Meta Pixel to the user's real-world identity using their shadow profile.[30]

88. A user's Facebook ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status and other details. Because the user's Facebook Profile

---

[28] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Feb. 28, 2024).

[29] *See* Facebook Business Tools Terms, https://www.facebook.com/legal/terms/businesstools.

[30] *See* Russell Brandom, *Shadow Profiles Are the Biggest Flaw In Facebook's Privacy Defense*, (Apr 11, 2018), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (last visited Feb. 28, 2024).

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/ followed by the c_user ID.

89. The Private Information disclosed via the Pixel allows Meta to know that a specific patient is seeking confidential medical care and the type of medical care being sought. Meta then uses that information to sell advertising to Duly and other advertisers and/or sells that information to marketers who use it to online target Plaintiffs and Class Members.

90. The third parties that receive information from the Pixel and/or CAPI track user data and communications for their own marketing purposes and for the marketing purposes of the website owner. Ultimately, the purpose of collecting user data is to make money.

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

92. In this case, Duly employed the Pixels and CAPI technology to intercept, duplicate and re-direct Plaintiffs' and Class Members' Private Information to Meta.

93. In sum, the Pixels and other tracking technologies on Defendant's Web Properties transmitted Plaintiffs' and Class Members' highly sensitive communications and Private Information to Meta, which communications contained private and confidential medical information.

94. These transmissions were performed without Plaintiffs' or Class Members' knowledge, consent or express written authorization.

95. As explained below, these unlawful transmissions are initiated by Defendant's

source code concurrent with communications made via the Website.

E. Meta Encourages Healthcare Partners, Including Duly, to Upload Patient Lists for Ad Targeting.

96. Meta operates the world's largest social media company. Meta's revenue is derived almost entirely from selling targeted advertising. Meta's Health division is dedicated to marketing to and servicing Meta's healthcare partners.[31] Meta defines its Partners to include businesses that use Meta's products, including the Meta Pixel or Meta Audience Network tools to advertise, market or support their products and services.

97. Meta works with hundreds of Meta healthcare Partners, using the Meta Pixel to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

98. Meta offers an ad targeting option called "Custom Audiences."

99. When a patient takes an action on a Meta healthcare partner's website embedded with the Pixel, the Pixel will be triggered to send Meta "Event" data that Meta matches to its users.

100. A web developer can then create a "Custom Audience" based on Events to target ads to those patients.

101. The Pixel can then be used to measure the effectiveness of an advertising campaign.[32]

---

[31] *See* https://www.facebook.com/business/industries/consumer-goods/healthcare (last visited Feb. 28, 2024).

[32] Meta Business Help Center, *About Customer List Custom Audiences* (2023), https://www.facebook.com/business/help/341425252616329?id=2469097953376494; *see also,* Meta Blueprint, Connect your data with the Meta Pixel and Conversion API (2023), https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d_fnzRCUAh

102. Meta also allows Meta healthcare partners to create a Custom Audience by uploading a patient list to Meta. As Meta describes it:[33]

> A Custom Audience made from a customer list is a type of audience you can create to connect with people who have already shown an interest in your business or product. It's made of information - called "identifiers" - you've collected about your customers (such as email, phone number and address) and provided to Meta. Prior to use, Meta hashes this information.
>
> Then, we use a process called matching to match the hashed information with Meta technologies profiles so that you can advertise to your customers on Facebook, Instagram and Meta Audience Network. The more information you can provide, the better the match rate (which means our ability to make the matches). Meta doesn't learn any new identifying information about your customers.

103. Meta provides detailed instructions for healthcare partners to send their patients' Private Information to Meta through the customer list upload. For example:[34]

> **Prepare your customer list in advance.** To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Meta profiles. The information on a customer list is known as an "identifier" (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach.
>
> Your customer list can either be a CSV or TXT file that includes these identifiers. To get the best match rates, use as many identifiers as possible while following our formatting guidelines. You can hover over the identifiers to display the formatting rules and the correct column header. For example, **first name** would appear as **fn** as a column header in your list.
>
> Alternatively, we have a file template you can download to help our system map to your identifiers more easily. (You can upload from Mailchimp as well.)

KGYsLqNA-VcLTMr3G_hxxFr3GZC_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9dff7fa.

[33] Meta Business Help Center, *About Customer List Custom Audiences* (2023), https://www.facebook.com/business/help/341425252616329?id=2469097953376494.

[34] Create a customer list custom audience, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited Feb. 28, 2024).

104. Meta healthcare partners can then use the Custom Audiences derived from their patient list with the Pixel and Pixel Events for Meta marketing campaigns and to measure the success of those campaigns.

F. Defendant's method of transmitting Plaintiffs' and Class Members' Private Information via the Tracking Pixel and/or CAPI (i.e., the interplay between HTTP Requests and Responses, Source Code & the Pixel)

105. 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 smartphone) 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).

106. 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.

107. 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.[35]

108. A patient's HTTP Request essentially asks the 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 the Website).

109. Every website consists of Markup and "Source Code."

110. Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

111. 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.

112. When patients visit Defendant's website via an HTTP Request to Duly's server, that server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel.

113. Thus, Defendant is, in essence, handing patients a tapped device 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 Meta.

---

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

112. Third parties, like Meta, 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 Personal Information intercepted.

113. 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 Meta, implement workarounds that cannot be evaded by savvy users.

114. Meta's workaround, for example, is called CAPI, which is an "effective" workaround because it does not intercept data communicated from the user's browser. Instead, CAPI "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."

115. Thus, the communications between patients and Defendant, which are necessary to use Defendant's Web Properties, are actually received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Meta.

116. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

117. Companies like Meta instruct customers like Defendant to "[u]se the CAPI 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."[36]

118. The third parties to whom a website transmits data through pixels and associated

[36] *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Feb. 28, 2024).

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 (i.e., to bolster profits).

119. 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 redirect the Users' communications to third parties.

120. In this case, Defendant employed the Tracking Pixel and CAPI to intercept, duplicate and re-direct Plaintiffs' and Class Members' Private Information to Meta.

121. For example, anyone who visits Duly's Website and clicks on the "Search for Services" tab is directed to a page, *https://www.dulyhealthandcare.com/services*, that presents a search bar and links to pages with information on specific conditions, treatments, and services, ranging from "Allergy, Asthma & Immunology" to "Vascular Surgery". Clicking the "Gynecologic Oncology" link leads to a new page, *https://www.dulyhealthandcare.org/gynecologic-oncology/*, discussing various cancer types, treatments, services, and treatment locations, each with separate links. Clicking on the "Radiation Oncology" link leads to another page, *https://www.dulyhealthandcare.com/services/radiation-oncology*, that describes cancer treatment options offered by Defendant, and has links allowing the user to view members of the "Radiation Oncology Team" and specific treatment options. Clicking the "Integrated Oncology Program" link leads to the page https://www.dulyhealthandcare.com/services/integrated-oncology-program, with more links and information regarding Defendant's cancer treatment options, providers, and locations. Clicking the "Schedule an Appointment" button leads to the page, *https://www.dulyhealthandcare.com/schedule*, which directs users to submit their contact

information, physician preferences, and other personally identifiable health information.

122. Defendant's Pixel intercepts and discloses to Meta both the "characteristics" of individuals' communications on the Duly Website (*i.e.,* their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (*i.e.,* the URLs, buttons, links, pages, and tabs they view and the information entered into the Website's forms), including the information patients submit to Defendant while making an appointment (such as their name, medical condition, treatment sought, provider name, specialty and gender, and any additional information entered into the appointment request form).

123. Thus, Duly reveals to Meta exact links and pages website users click and view and discloses extensive insight into the user's past, present, and/or future health care, which undoubtably qualifies as protected health information under HIPAA. *See* 45 C.F.R. § 160.103.

124. This example highlights just one of the hundreds (if not thousands) of paths available on Defendant's Website and Portal that explains how Defendant's Web Properties surreptitiously collect and transmit protected health information to its third-party vendors.

125. As a further example, when a patient visits https://www.dulyhealthandcare.com/services and selects "Gynecologic Oncology," the patient's browser automatically sends an HTTP Request to Defendant's web server. The Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage as depicted below.

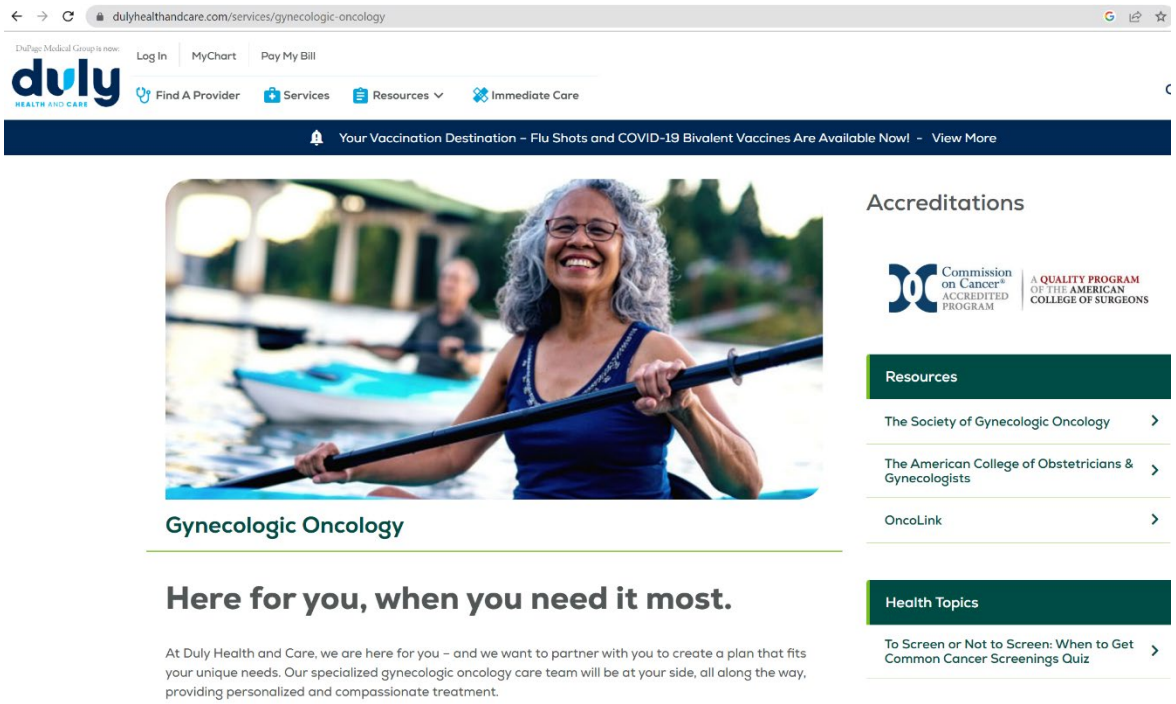


Figure 1. Image taken from https://www.dulyhealthandcare.org/gynecologic-oncology/

126. The patient visiting this particular web page only sees the Markup, not the Defendant's Source Code or underlying HTTP Requests and Responses.

127. In reality, Defendant's Source Code and underlying HTTP Requests and Responses share the patient's personal information with Meta, including the fact that the patient is looking for Gynecologic Oncology treatment – along with the patient's unique Facebook ID.

Figure 2. An HTTP single communication session sent from the device to Meta that reveals the

user's search results and the patient's FID (c_user field).[37]

128. Defendant also notifies Meta of its patients' patient status. For example, when a User accesses Defendant's page to utilize Defendant's patient portal, Defendant notifies Meta of that as well.

129. Such disclosures are taking place without Users' consent.

130. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions and can command a website visitor's browser to send data transmissions to third parties via pixels or web bugs,[38] effectively open a spying window through which the webpage can funnel the visitor's data, actions, and communications to third parties.

131. Looking to the previous example, Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) and send those communications to Meta.

132. This occurs because the Pixel embedded in Defendant's Source Code is programmed to automatically track and transmit a patient's communications, and this occurs contemporaneously, invisibly and without the patient's knowledge.

133. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer patients' computing devices thereby re-directing their Private Information to third parties.

134. The information that Defendant's Pixel sends to Meta may include, among other

---

[37] The user's Facebook ID is represented as the c_user ID highlight in the image above, and Plaintiffs has redacted the corresponding string of numbers to preserve the user's anonymity.

[38] These pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

things, patients' PII, PHI and other confidential information.

135. Consequently, when Plaintiffs and Class Members visit Defendant's website and communicate their Private Information, it is transmitted to Meta, including, but not limited to, appointment type and date, physician selected, specific button/menu selections, content typed into free text boxes, demographic information, email addresses, phone numbers and emergency contact information.

G. Defendant's Pixel and/or CAPI Tracking Practices caused Plaintiffs' & Class Members' PII & PHI to be sent to Meta.

136. Defendant utilizes Meta's Business Tools and intentionally installed the Pixel and CAPI on its Web Properties to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory and regulatory duties and obligations.

137. Defendant's Web Pages contain a unique identifier which indicates that the Pixel is being used on a particular webpage, identified as 486716330266417 on www.dulyhealthandcare.com.

138. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences and decrease advertising and marketing costs.

139. However, Defendant's Web Properties does not rely on the Pixel in order to function.

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

141. Defendant did not disclose to Plaintiffs and Class Members that their Private Information would be shared with Meta as it was communicated to Defendant.

142. Plaintiffs and Class Members never consented, agreed, authorized or otherwise

permitted Defendant to disclose their Private Information to Meta, nor did they intend for Meta to be a party to their communications with Defendant.

143. Defendant's Pixel and CAPI sent non-public Private Information to Meta, including but not limited to Plaintiffs' and Class Members': (i) status as medical patients; (ii) health conditions; (iii) sought treatment or therapies; (iv) appointment requests and appointment booking information; (v) registration or enrollment in medical classes (such as breastfeeding courses); (vi) locations or facilities where treatment is sought; (vii) which web pages were viewed and (viii) phrases and search queries conducted via the general search bar.

144. Importantly, the Private Information Defendant's Pixel sent to Meta was sent alongside Plaintiffs' and Class Members' Facebook ID (c_user cookie or "FID") thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts.[39]

145. 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.

146. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (i) implemented technology *(i.e.*, the Meta Pixel) that surreptitiously tracked, recorded and

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

disclosed Plaintiffs' and other online patients' confidential communications and Private Information; (ii) disclosed patients' protected information to Meta—an unauthorized third-party and (iii) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

H. Defendant's Pixel Disseminates Patient Information via www.dulyhealthandcare.com

147. An example illustrates the point. If a patient uses www.dulyhealthandcare.com to look for a doctor, they may select the "Find a Provider" tab, which takes them to the "Find a Provider" page.

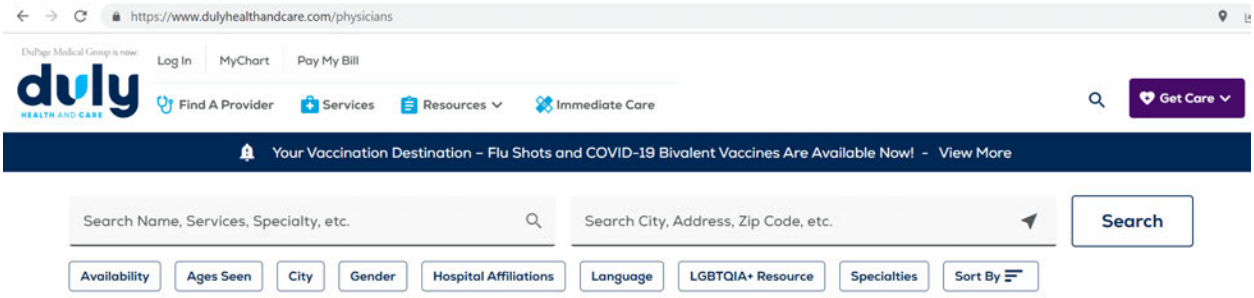


Figure 3. Defendant directs patients to its "Find a Provider" webpage with embedded Pixels – which are invisible to the regular user.

148. On this page Defendant asks to user to narrow their search results by numerous from provider name to provider gender and specialties.

149. If a user selects filters or enters keywords into the search bar on the "Find a Provider" webpage, the filters and search terms are transmitted via the Meta Pixel. Similarly, if a patient uses the Website's general search bar or chat, the terms and phrases the patient types are transmitted to Meta, even if they contain a patient's treatment, procedures, medical conditions, and related queries.

150. This information is automatically sent from the patient's device to Meta, and it

reveals the patient's FID (c_user field) along with each search filter the patient selected.

151. Without alerting the user, Defendant's Pixel sends each and every communication the user made to the Defendant via the Webpage to Meta, and the images below confirm that the communications Defendant sends to Meta contain the user's Private Information.

152. For example, a patient can search for a provider specializing in colonoscopy closest to patient's chosen address, with the option of using additional filters - from provider's gender to their additional specialties.

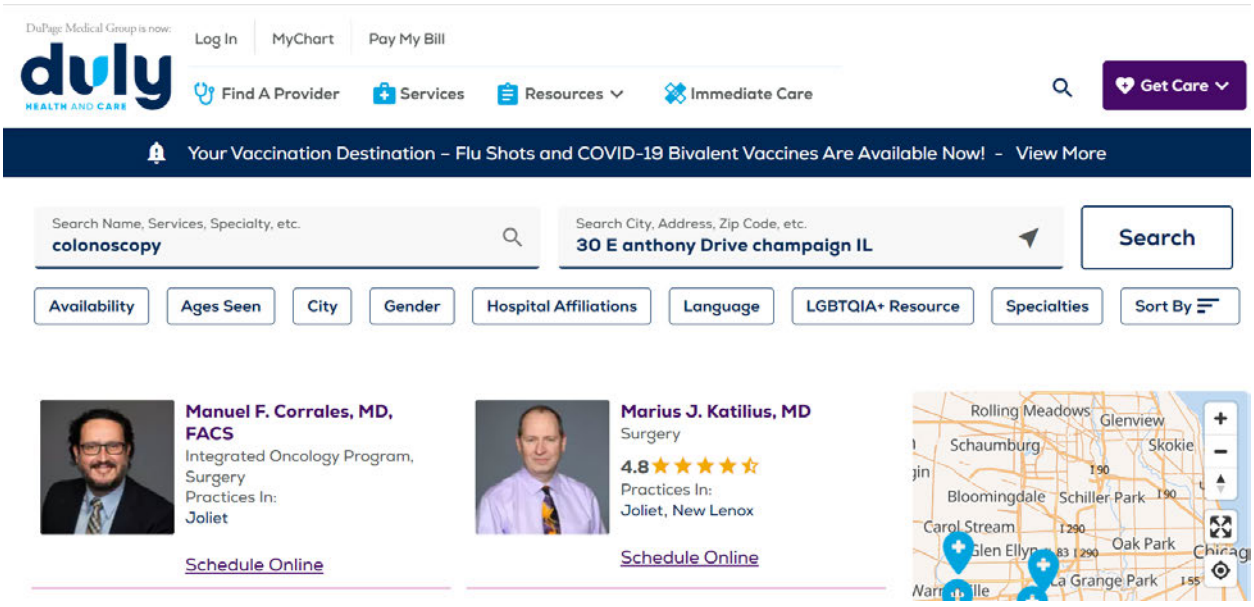


Figure 4. Search results for a provider specializing in "colonoscopy" near "30 E Anthony Drive Champaign IL" as they appear to the user on Defendant's Find a Provider Search results webpage.

153. After taking any of these actions on the 'Find a Provider' page, patients are subsequently directed to the Provider Search Results page (see image above), and their selections or search parameters are automatically transmitted by the Pixel to Meta along with the user's unique Facebook ID, as evidenced by the images below.

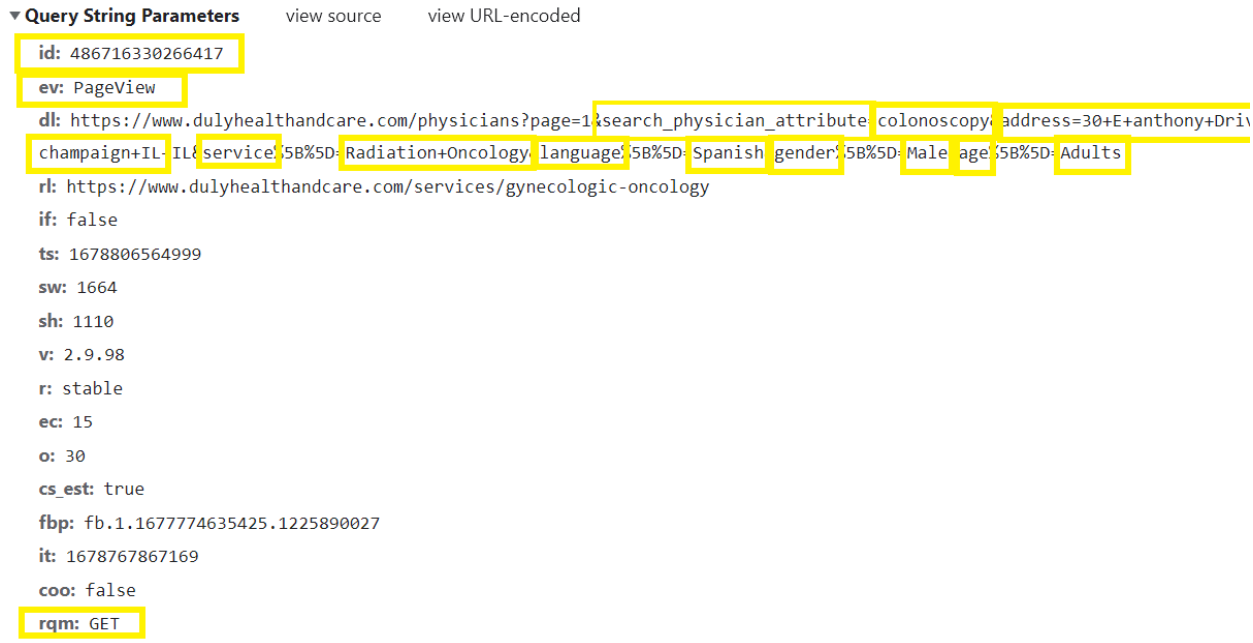


Figure 5. Defendant's transmission to Meta of patient's search parameters showing search terms ("colonoscopy" and "30 E Anthony Drive Champaign IL") and filters used ("Male" provider who speaks "Spanish," specializes in "Radiation Oncology" and services "Adults").

154. The first line of highlighted text, "id: 486716330266417," refers to the Defendant's Pixel ID for this particular Webpage and confirms that the Defendant has downloaded the Pixel into its Source Code on this particular Webpage.

155. The second line of text, "ev: PageView," identifies and categorizes which actions the user took on the Webpage ("ev:" is an abbreviation for event, and "Pageview" is the type of event). Thus, this identifies the user as having viewed the particular Webpage.

156. The remaining lines of text identify: (i) the user as a patient seeking medical care from Defendant via www.dulyhealthandcare.com; (ii) who is in the process of searching for a male provider for adult patients; (iii) who specializes in colonoscopy and Radiation Oncology; (iv) speaks Spanish and (v) is located near the address entered into Defendant's Search bar.

157. Finally, the last line of highlighted text ("GET"), demonstrates that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the

user's Facebook ID (c_user ID). This is further evidenced by the image below, which was collected during the same browsing session as the previous image.[40]

Figure 6. Defendant's transmission to Meta of patient's search parameters showing search terms and the patient's c_user information from Defendant's "Find a Provider" webpage.

158. After searching for a colonoscopy specialist Defendant's Website brings the user to a page listing Defendant's colonoscopy providers, including Dr. Manuel F. Corrales.

159. Once a patient chooses a doctor, all of the information that patient has submitted is automatically sent directly to Meta. The information transmitted to Meta includes: (i) the patient's unique and persistent Facebook ID (c_user ID), (ii) the fact that the patient clicked on a specific provider's profile page (Dr. Corrales in the example above and below), (iii) the patient's search

[40] This image shows yet another "event" recorded and shared by the Pixel, called "SubscribedButtonClick" – which reveals that the user clicked a button on Defendant's webpage to submit search parameters.

parameters (demonstrating they specifically searched for a male doctor who speaks Spanish and treats adult patients, and their specialty) and (iv) the patient's location filter.

Figure 7. An HTTP single communication session sent from the device to Meta that reveals the user's search parameters, results and the patient's FID (c_user field).

160. Defendant's website also includes a feature that allows patients to book appointments through a particular doctor's profile page.

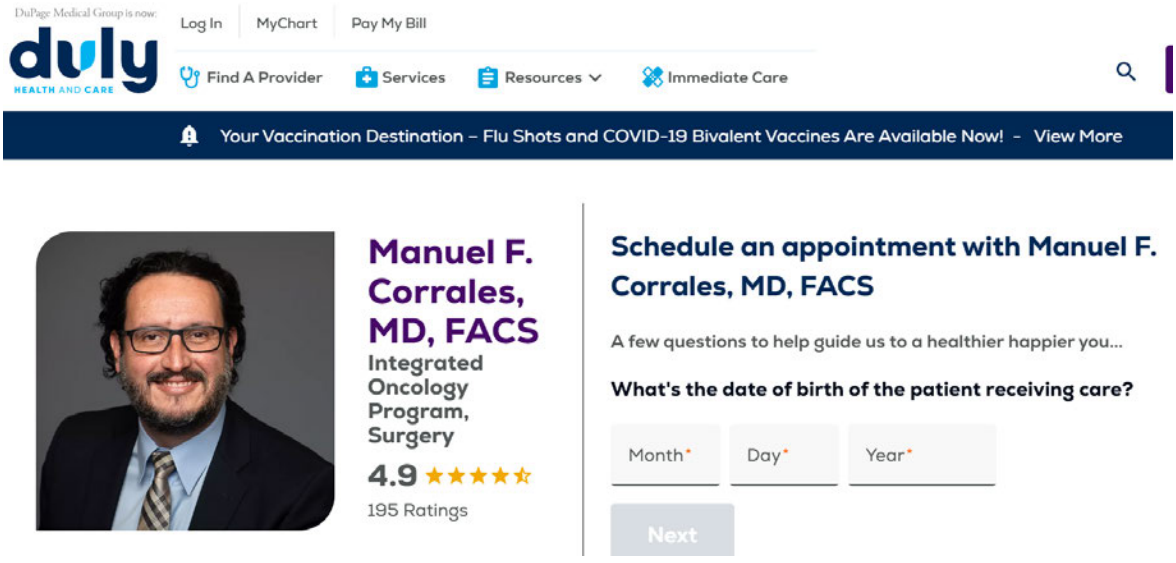


Figure 8. Image from https://www.dulyhealthandcare.com/physicians/manuel-f-corrales-md-facs.

161. If the user decides to schedule an appointment, Defendant communicates every step of the process to Meta.

162. For example, if a patient enters their date of birth in the form shown in the image above and clicks "Next," Defendant shares this action with Meta – along with the provider's name and patient's search parameters which were already shared with Meta in previous interactions.

▼ **Request Headers**

:authority: www.facebook.com

:method: GET

:path: /tr/?id=486716330266417&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%2Fma
nuel-f-corrales-md-facs&rl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%3Fpage%3D1%26search_physician_attri
bute%3Dcolonoscopy%26address%3D30%2BE%2Banthony%2BDrive%2Bchampaign%2BIL%2BIL%26language%255B%255D%3DSpanish%26gend
er%255B%255D%3DMale%26age%255B%255D%3DAdults&if=false&ts=1678826852181&cd[buttonFeatures]=%7B%22classList%22%3A%22d
mgButton%20primary1%22%2C%22destination%22%3A%22https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%2Fmanuel-f-cor
rales-md-facs%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Next%22%2C%22numChildButtons%
22%3A0%2C%22tag%22%3A%22button%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%2C%22value%22%3A%22%22%7D&cd[buttonTex
t]=Next&cd[formFeatures]=%5B%7B%22id%22%3A%22date_of_birth_month%22%2C%22name%22%3A%22date_of_birth_month%22%2C%22t
ag%22%3A%22input%22%2C%22placeholder%22%3A%22MM%22%2C%22inputType%22%3A%22text%22%7D%2C%7B%22id%22%3A%22date_of_bir
th_day%22%2C%22name%22%3A%22date_of_birth_day%22%2C%22tag%22%3A%22input%22%2C%22placeholder%22%3A%22DD%22%2C%22inpu
tType%22%3A%22text%22%7D%2C%7B%22id%22%3A%22date_of_birth_year%22%2C%22name%22%3A%22date_of_birth_year%22%2C%22tag%
22%3A%22input%22%2C%22placeholder%22%3A%22YYYY%22%2C%22inputType%22%3A%22text%22%7D%5D&cd[pageFeatures]=%7B%22titl
e%22%3A%22Manuel%20F.%20Corrales%2C%20MD%2C%20FACS%20%7C%20Duly%20Health%20and%20Care%20-%20DuPage%20Medical%20Grou
p%22%7D&sw=1664&sh=1110&v=2.9.98&r=stable&ec=2&o=30&cs_est=true&fbp=fb.1.1677774635425.1225890027&it=1678825890406&
coo=false&es=automatic&tm=3&rqm=GET

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

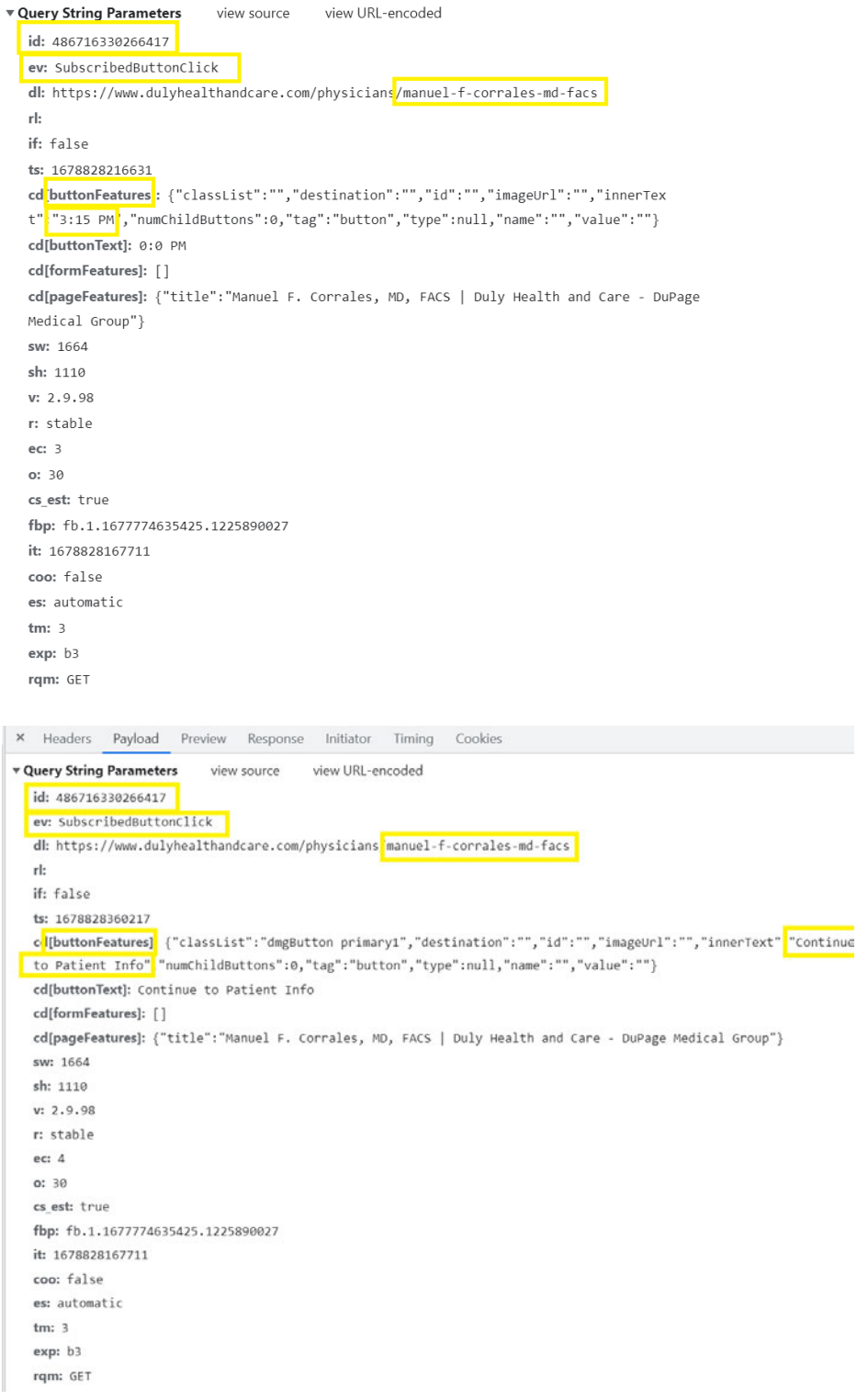
accept-language: en-US,en;q=0.9,ru;q=0.8

cookie: datr=QtI1Y1lVd2UWOuuBmn2Mb8vC; sb=GrxtY1jj9lKWnpCg7UAhiJMv; c_user=5[redacted]; dpr=1.5; usida=eyJ2ZXIiOjEsIml
kIjoiQXJyaG8yMTFocXNlZ3UiLCJ0aW1lIjoxNjc4NzYwNzEzfQ%3D%3D; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3A
AcVddgJMpRq79qEYuBZ7R4ajfU2rdran5L587wTJVqc; fr=0pyQTLs0lx68y5snn.AWU4YHXCuAMCpRNhJznkPTx9OeY.BkEKoB.-f.AAA.0.0.BkE
KoB.AWXpsCnX30c

referer: https://www.dulyhealthandcare.com/

Figure 9. An HTTP single communication session sent from the device to Meta that reveals the user's search parameters, results, the patient's FID (c_user field), and the fact that the "inner Text" of the button patient clicked ("Next").

163. Defendant's Pixel shares what time a patient is choosing for an appointment (in the example below, "3:15 PM") and the fact that the patient clicked on "Proceed to Patient Info" button:



Figures 10 & 11. HTTP communication sessions sent by the Pixel to Meta that reveal the "inner text" of the buttons patient clicked in the process of making an appointment.

164. When the user proceeds to the Patient Information form, Defendant's Pixel communicates and shares this information with Meta as well.

Figure 12. HTTP communication sessions sent by the Pixel to Meta that reveal that the patient is using the "Patient Information" intake form.

165. If, after following these steps, a patient clicks on the "Schedule an Appointment" button, Defendant communicates and shares this action with Meta via at least three "events," classified by Meta as "Pageview" – which indicates the patient viewed the page confirming the appointment, "Microdata" – which sends certain information from the page viewed by the patient (in this case, the fact that patient scheduled an appointment), and "Schedule" – which, as its name reveals, also indicates that the patient scheduled an appointment with Defendant:

▼ **Request Headers**

:authority: www.facebook.com

:method: GET

:path: /tr/?id=486716330266417&ev=PageView&dl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fschedule%2Fbook%2Fshare&rl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fschedule%2Fbook&if=false&ts=1678831529931&sw=1664&sh=1110&v=2.9.98&r=stable&ec=0&o=30&cs_est=true&fbp=fb.1.1677774635425.1225890027&it=1678831529802&coo=false&rqm=GET

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

accept-language: en-US,en;q=0.9,ru;q=0.8

cookie: datr=QtI1Y1lVd2UWOuuBmn2Mb8vC; sb=GrxtY1jj9lKWnpCg7UAhiJMv; c_user=54 ; dpr=1.5; usida=eyJ2ZXIiOjEsImlkIjoiQXJyaG8yMTFocXNlZ3UiLCJ0aW1lIjoxNjc4NzYwNzEzfQ%3D%3D; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AAcV7JjHXsLHCcRciOYtWKOtxoPr6F4ltNzzvzpJCtiA; fr=0yIH3VuDHxaXUDL0r.AWU89wEnKjpn-E1Fgn2j_J_GM1k.BkEOo2.-f.AAA.0.0.BkEOo2.AWW9bWS7KhM

referer: https://www.dulyhealthandcare.com/

▼ **Request Headers**

:authority: www.facebook.com

:method: GET

:path: /tr/?id=486716330266417&ev=Microdata&dl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fschedule%2Fbook%2Fshare&rl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fschedule%2Fbook&if=false&ts=1678831531457&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Appointment%20Confirmation%20%7C%20Duly%20Health%20and%20Care%20-%20DuPage%20Medical%20Group%22%7D&cd[OpenGraph]=%7B%7D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=1664&sh=1110&v=2.9.98&r=stable&ec=2&o=30&fbp=fb.1.1677774635425.1225890027&it=1678831529802&coo=false&es=automatic&tm=3&rqm=GET

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

accept-language: en-US,en;q=0.9,ru;q=0.8

cookie: datr=QtI1Y1lVd2UWOuuBmn2Mb8vC; sb=GrxtY1jj9lKWnpCg7UAhiJMv; c_user=5 ; dpr=1.5; usida=eyJ2ZXIiOjEsImlkIjoiQXJyaG8yMTFocXNlZ3UiLCJ0aW1lIjoxNjc4NzYwNzEzfQ%3D%3D; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AAcV7JjHXsLHCcRciOYtWKOtxoPr6F4ltNzzvzpJCtiA; fr=0yIH3VuDHxaXUDL0r.AWU89wEnKjpn-E1Fgn2j_J_GM1k.BkEOo2.-f.AAA.0.0.BkEOo2.AWW9bWS7KhM

referer: https://www.dulyhealthandcare.com/

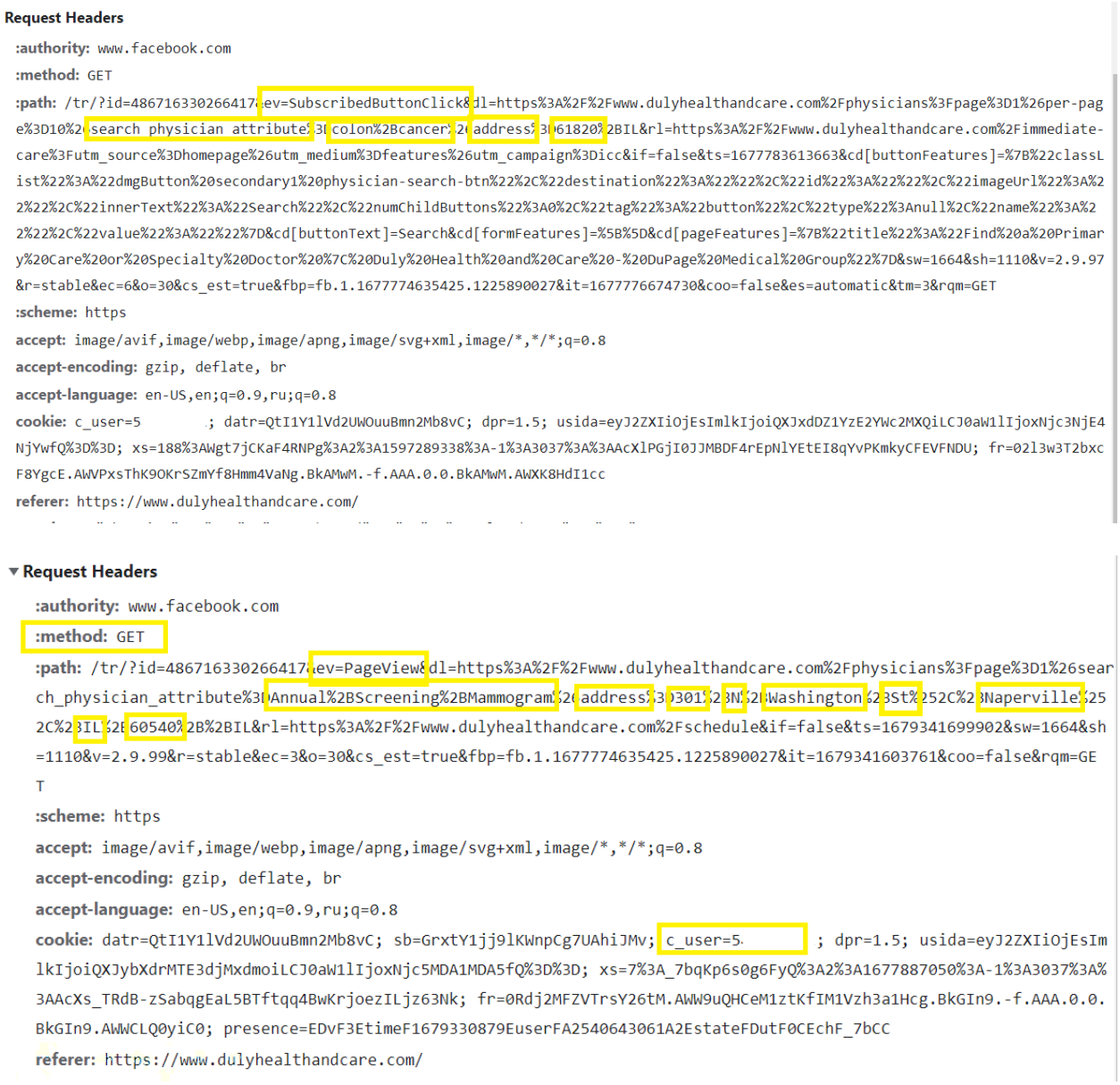
Figures 13-15. This information is automatically sent from the patient's device to Meta, and it reveals the patient's FID (c_user field) along with the fact that the patient made an appointment.

85. Similarly, if a patient searches for a provider who specializes in "Papillotomy" near zip code 61820, selects Dr. Alan Wang from the search results provided by Defendant, and clicks the telephone button to make an appointment with that provider, Defendant shares all of that information with Meta (including the phone number being called) as a "SubscribedButtonClick" event.

Figure 16. The information automatically sent to Meta reveals the patient's FID (c_user field) along with the fact that the patient clicked a button with Defendant's telephone number to make an appointment with a specific provider for a specific procedure.

86. If a user searches for treatment or a particular condition, Defendant's Pixel sends that information to Meta as well.

87. The examples below demonstrate that, if a user searches for "colon cancer" or "annual screening mammogram" near the patient's address, Defendant's Pixel shares that information with Meta as well:

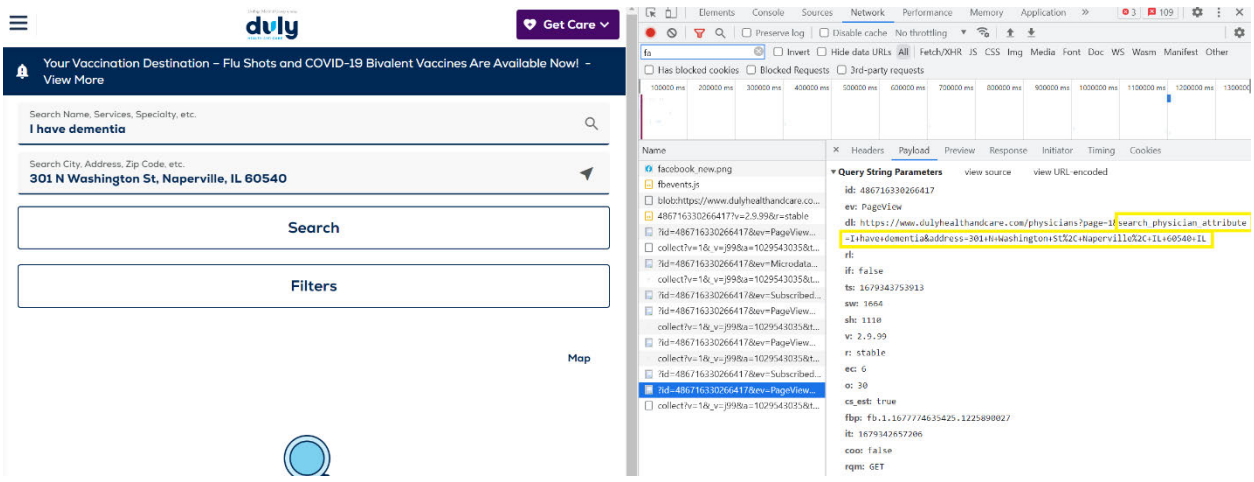


Figures 17 & 18. Examples of data from search results being shared with Meta.

88. To make matters worse, the text and phrases that patients type into the search bar are also sent to Meta.

89. The images below demonstrate that when a user types the phrase "I have dementia" into the general search bar, that exact phrase is sent to Meta alongside the user's Facebook ID (and address), thereby allowing the phrase and medical condition contained therein to be attributed and

associated with their individual Facebook account.



Request Headers

:authority: www.facebook.com

:method: GET

:path: /tr/?id=486716330266417&ev=PageView&dl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%3Fpage%3D1%26search_physician_attribute%3DI%2Bhave%2Bdementia%2Baddress%3D301%2BN%2BWashington%2BSt%252C%2BNaperville%252C%2BIL%2B60540%2BIL&rl=&if=false&ts=1679343753913&sw=1664&sh=1110&v=2.9.99&r=stable&ec=6&o=30&cs_est=true&fbp=fb.1.1677774635425.1225890027&it=1679342657206&coo=false&rqm=GET

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

accept-language: en-US,en;q=0.9,ru;q=0.8

cookie: datr=QtI1Y1lVd2UWOuuBmn2Mb8vC; sb=GrxtY1jj9lKWnpCg7UAhiJMv; c_user=5 ; dpr=1.5; usida=eyJ2ZXIiOjEsImlkIjoiQXJybXdrMTE3djMxdmoiLCJ0aW1lIjoxNjc5MDA1MDA5fQ%3D%3D; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AAcXs_TRdB-zSabqgEaL5BTftqq4BwKrjoezILjz63Nk; fr=0Rdj2MFZVTrsY26tM.AWW9uQHCeM1ztKfIM1Vzh3a1Hcg.BkGIn9.-f.AAA.0.0.BkGIn9.AWWCLQ0yiC0; presence=EDvF3EtimeF1679330879EuserFA2540643061A2EstateFDutF0CEchF_7bCC

referer: https://www.dulyhealthandcare.com/

Figures 19 & 20. Example of exact text and phrases being shared with Meta.

112. Each time Defendant sends this activity data, it also discloses a patient's personally identifiable information alongside the contents of their communications.

113. A user who accesses Defendant's Web Properties while logged into Facebook will transmit the c_user cookie to Meta, which contains that user's unencrypted Facebook ID.

114. When accessing dulyhealthandcare.com, for example, Meta receives as many as eight cookies:

Name	V...	Domain	P.	Expires ...	S
datr	Q...	.facebook.com	/	2024-0...	2
sb	G...	.facebook.com	/	2024-0...	2
c_user	5...	.facebook.com	/	2024-0...	1
dpr	1.5	.facebook.com	/	2023-0...	(
usida	e...	.facebook.com	/	Session	7
xs	7...	.facebook.com	/	2024-0...	9
fr	0...	.facebook.com	/	2023-0...	8
presence	E...	.facebook.com	/	2023-0...	7

Figure 21.

115. When a visitor's browser has recently logged out of an account, Meta compels the visitor's browser to send a smaller set of cookies[41]:

fr	00Zp...	.facebook.com
wd	1156...	.facebook.com
sb	qqAz...	.facebook.com
datr	Malz...	.facebook.com

Figure 22.

116. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.[42] Meta, at a minimum, uses the fr cookie to identify users.[43]

117. At each stage, Defendant also utilized the _fbp cookie, which attaches to a browser

---

[41] The screenshot below serves as an example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

[42] Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited February 28, 2024).

[43] *Cookies & other storage technologies*, FACEBOOK.COM, https://www.facebook.com/policy/cookies/ (last visited February 28, 2024).

as a first-party cookie, and which Meta uses to identify a browser and a user:[44]

Name	Value	Domain
_fbp	fb.1.1677774635425.1225890027	.dulyhealthandcare.com

Figure 22.

118. The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.[45] If that happens, the time resets, and another 90 days begins to accrue.

119. The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website.[46] If that happens, the time resets, and another 90 days begins to accrue.

120. The Meta Tracking Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—*i.e.*, Defendant.[47]

121. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Meta.[48]

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

---

[44] *Id.*

[45] *Id.*

[46] *Cookies & other storage technologies*, FACEBOOK.COM, https://www.facebook.com/policy/cookies/ (last visited February 28, 2024).

[47] *First-Party Cookie*, PCMAG.COM, https://www.pcmag.com/encyclopedia/term/first-party-cookie (last visited February 28, 2024). This is confirmable by using developer tools to inspect a website's cookies and track network activity.

[48] *Third-Party Cookie*, PCMAG.COM, https://www.pcmag.com/encyclopedia/term/third-party-cookie (last visited February 28, 2024). This is also confirmable by tracking network activity.

123. Meta, at a minimum, uses the fr, _fbp, and c_user cookies to link to FIDs and corresponding Facebook profiles.

124. As shown in the above figures, Defendant sent these identifiers with the event data.

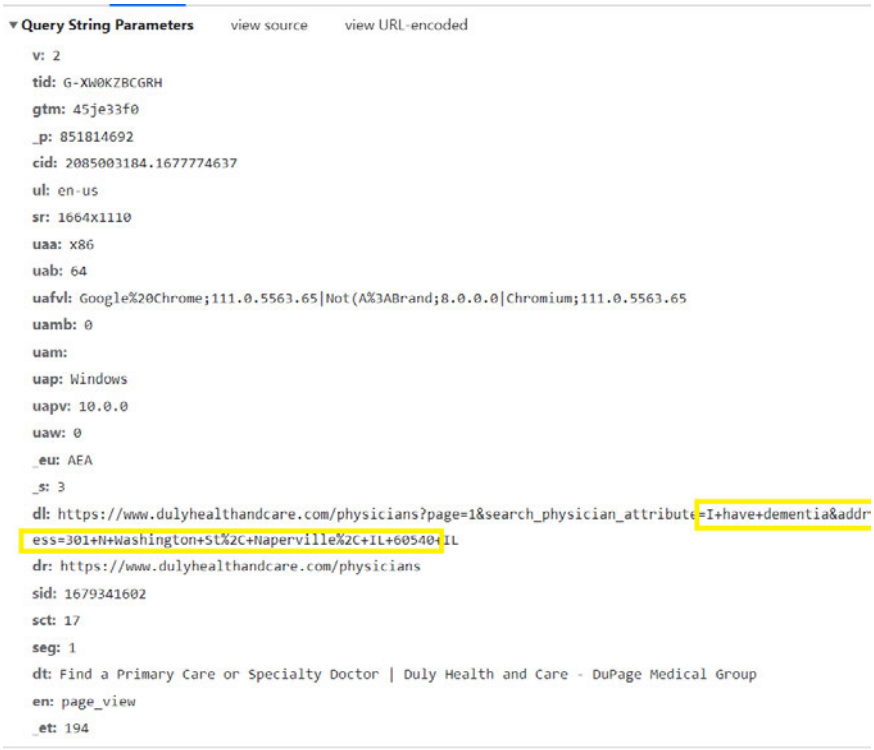
125. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant to disclose their personally identifiable information and protected health information nor did they authorize any assistance with intercepting their communications.

126. Plaintiffs were never provided with any written notice that Defendant disclosed its Web Properties users' PHI nor were they provided any means of opting out of such disclosures.

127. Despite this, Defendant knowingly and intentionally disclosed Plaintiffs' PHI to Meta.

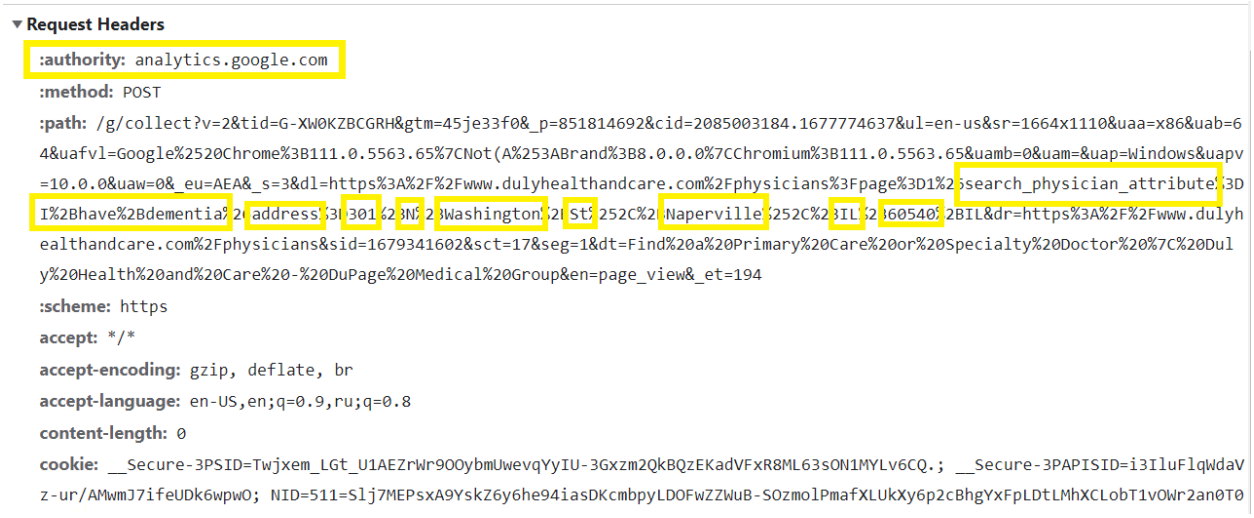
128. Although the full scope of Defendant's illegal data sharing practices is presently unknown, additional evidence demonstrates that Defendant is also sharing its patients' Private Information with Google via the Google Analytics tools, and the image below indicates that Defendant has failed to enable the "anonymize IP" feature.

129. Resultantly, Google receives a patient's communications and data alongside their unique IP address, thereby creating an additional and distinct HIPAA violation and breach of confidentiality.



▼ **Query String Parameters** view source view URL-encoded

v: 2
tid: G-XW0KZBCGRH
gtm: 45je33f0
_p: 851814692
cid: 2085003184.1677774637
ul: en-us
sr: 1664x1110
uaa: x86
uab: 64
uafvl: Google%20Chrome;111.0.5563.65|Not(A%3ABrand;8.0.0.0|Chromium;111.0.5563.65
uamb: 0
uam:
uap: Windows
uapv: 10.0.0
uaw: 0
_eu: AEA
_s: 3
dl: https://www.dulyhealthandcare.com/physicians?page=1&search_physician_attribute=I+have+dementia&address=301+N+Washington+St%2C+Naperville%2C+IL+60540+IL
dr: https://www.dulyhealthandcare.com/physicians
sid: 1679341602
sct: 17
seg: 1
dt: Find a Primary Care or Specialty Doctor | Duly Health and Care - DuPage Medical Group
en: page_view
_et: 194



▼ **Request Headers**

:authority: analytics.google.com
:method: POST
:path: /g/collect?v=2&tid=G-XW0KZBCGRH&gtm=45je33f0&_p=851814692&cid=2085003184.1677774637&ul=en-us&sr=1664x1110&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B111.0.5563.65%7CNot(A%253ABrand%3B8.0.0.0%7CChromium%3B111.0.5563.65&uamb=0&uam=&uap=Windows&uapv=10.0.0&uaw=0&_eu=AEA&_s=3&dl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%3Fpage%3D1%26search_physician_attribute%3DI%2Bhave%2Bdementia%26address%3D301%2BN%2BWashington%2BSt%252C%2BNaperville%252C%2BIL%2B60540%2BIL&dr=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians&sid=1679341602&sct=17&seg=1&dt=Find%20a%20Primary%20Care%20or%20Specialty%20Doctor%20%7C%20Duly%20Health%20and%20Care%20-%20DuPage%20Medical%20Group&en=page_view&_et=194
:scheme: https
accept: */*
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9,ru;q=0.8
content-length: 0
cookie: __Secure-3PSID=Twjxem_LGt_U1AEZrWr9OOybmUwevqYyIU-3Gxzm2QkBQzEKadVFxR8ML63sON1MYLv6CQ.; __Secure-3PAPISID=i3IluFlqWdaVz-ur/AMwmJ7ifeUDk6wpwO; NID=511=Slj7MEPsxA9YskZ6y6he94iasDKcmbpyLDOFwZZWuB-SOzmolPmafXLUkXy6p2cBhgYxFpLDtLMhXCLobT1vOWr2an0T0

Figures 23 and 24. Images of the data that is sent to Google, which contains the exact phrase and medical condition the user communicated via Defendant's Website, along with their address.

130. By law, Plaintiffs are entitled to privacy in their protected health information and confidential communications.

131. Defendant deprived Plaintiffs and Class Members of their privacy rights when it:

(i) implemented a system that surreptitiously tracked, recorded and disclosed Plaintiffs' and Class Members' confidential communications, personally identifiable information and protected health information to a third party; (ii) disclosed patients' protected information to Meta – an unauthorized third-party eavesdropper and (iii) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent.

132. Plaintiffs Mayer and Murphy did not discover that Defendant disclosed their personally identifiable information and protected health information to Meta and assisted Meta with intercepting their communications until March 2023 the earliest. Plaintiff Massarelli did not discover that Defendant disclosed her personally identifiable information and protected health information to Meta and assisted Meta with intercepting her communications until February 2024.

G. Defendant's Privacy Policy & Promises

133. Defendant's Privacy Policy provides that it does not apply to any Protected Health Information and that Users of the Web Properties should visit a separate page for its HIPAA Notice of Privacy Practices:

> PLEASE NOTE THAT THIS PRIVACY POLICY DOES NOT APPLY TO YOUR PROTECTED HEALTH INFORMATION.
>
> We may receive your Protected Health Information when you, for example, schedule an appointment, provide your Protected Health Information through the Epic MyChart portal, the online bill pay portal, or while you are receiving treatment from us. Protected Health Information is treated in accordance with our Notice of Privacy Practices, which are available here. If you have any questions about DMG's use or disclosure of your Protected Health Information, please review the Notice of Privacy Practices. Alternatively, you may contact us using the information below. We may link Usage Information and/or Personal Information to your Protected Health Information. In such circumstances, we will treat such linked

> information as Protected Health Information on a going-forward basis.[49]

134. On a web page titled HIPAA Privacy Practices & Forms, Duly sets forth its Notice of Privacy Practices, which begins by stating that:

> **Your Information. Your Rights. Our Responsibilities.**
>
> Nothing is more important than[] ensuring your privacy. At Duly Health and Care, we understand that your privacy is vitally important. As your medical provider, we take proactive measures to safeguard your information. We understand that with each office visit, you are placing your trust in us. We will make every effort to ensure this trust is not breached, and that your privacy is protected.
>
> This Notice was developed to provide you with information regarding your rights to privacy and confidentiality. It contains our policies regarding privacy according to the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations. We encourage you to read this information thoroughly so that you are fully informed about our policies and procedures. We welcome any questions you may have regarding this information.[50]

135. That web page includes a hyperlink to a document titled Notice of Privacy Practices (the "HIPAA Notice"), which purports to describe for patients and Users how Duly will handle PHI.[51]

136. Defendant represents to patients and visitors to its Website that it will keep PHI information confidential and that it will only use and disclose PHI provided to it under certain circumstances, ***none of which apply here***:

> OUR USES & DISCLOSURES We typically use or share your health information in the following ways: Treatment, Payment, and Operations (TPO).

---

49 *See* https://www.dulyhealthandcare.com/privacy-policy (last visited February 28, 2024).

50 https://www.dulyhealthandcare.com/hipaa-privacy-policy (last visited February 28, 2024).

51 On information and belief, the current version of the Notice (as of January 2023) is attached as **Exhibit A** hereto.

> To treat you · We can use your health information and share it with other professionals that have a treatment relationship with you. · Example: A doctor treating you for an injury may ask another doctor who treated you about your overall health condition. · We may use and disclose medical information about you to contact you about health-related benefits and services that may be of interest to you, including: - To describe a health-related product or service that is provided by us. - For case management or your care coordination. - To direct or recommend alternative treatments, therapies, health care providers or settings of care. · We may communicate with you about our products and services through face-to-face communication. We may also communicate about products or services in the form of a promotional gift of nominal value.
>
> Operate our organization · We can use or share your health information to operate our practice, improve your care, and contact you when necessary. · Example: We use your health information to manage your treatment and services, such as appointment reminders, and to train our staff. · We can share your health information with "business associates" – individuals or companies that provide services to Duly. This may include a survey vendor, a software vendor, a billing vendor, or a collection agency. We require our business associates to protect your information.
>
> To bill for our services · We can use and share your health information to bill and receive payment from health plans and other entities responsible for the payment of your care. · Example: we provide information about you to your health insurance plan so it will pay for services provided to you.

135. Defendant's Notice does ***not*** permit it to use and to disclose Plaintiffs' and Class Members' Private Information for marketing purposes without prior express consent:

> In these cases, we never share your information unless you give us written permission · We must obtain your authorization for the following purposes (and for all other uses and disclosures) not described in this Notice: - ***Marketing*** - Sale of your information - Most sharing of psychotherapy notes, alcohol treatment and drug dependence treatment, unless otherwise required by law.[52]

136. Defendant violated their own HIPAA Notice by unlawfully intercepting and

[52] *See* Ex. A (emphasis added).

disclosing Plaintiffs' and Class Members' Private Information to Meta and third parties without adequately disclosing that Defendant shared Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

H. Federal Warning on Tracking Codes on Healthcare Websites.

137. Beyond Defendant's own policies, the U.S. government has issued guidance warning that tracking code like Meta Pixel may come up against federal privacy law when installed on healthcare websites.

138. The statement, titled *Use of Online Tracking Technologies By HIPAA Covered Entities And Business Associates* (the "Bulletin"), was recently issued by the Department of Health and Human Services' Office for Civil Rights ("OCR").[53]

139. Healthcare organizations regulated under the Health Insurance Portability and Accountability Act (HIPAA) may use third-party tracking tools, such as Google Analytics or Meta Pixel, in a limited way, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' protected health information to these vendors.

140. The Bulletin explains:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[54]

---

[53] USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaaonline-tracking/index.html (last visited February 28, 2024).

[54] *Id.* (Emphasis added).

141. The bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.*** Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.*** While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***[55]

142. Plaintiffs and Class Members face just the risks about which the government expresses concern. Defendant has passed along Plaintiffs' and Class Members' search terms about health conditions for which they seek doctors; their contacting of doctors to make appointments; the names of their doctors; the frequency with which they take steps relating to obtaining healthcare for certain conditions; and where they seek medical treatment.

143. This information is, as described by the OCR in its bulletin, "highly sensitive." The Bulletin goes on to make clear how broad the government's view of protected information is as it explains:

> 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.***[56]

---

55 *Id.* (emphasis added).

56 *Id.* (emphasis added).

144. Crucially, that paragraph in the government's Bulletin continues:

> ***All such [individually identifiable health information ("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.***[57]

145. The OCR Bulletin reminds healthcare organizations regulated under the HIPAA that they may use third-party tracking tools, such as Google Analytics or Pixels only in a limited way, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[58]

146. The federal government is taking these violations of health data privacy and security seriously as recent high-profile FTC settlements against several telehealth companies evidence.

147. For example, earlier this year, the FTC imposed a $1.5 million penalty on GoodRx for violating the FTC Act by sharing its customers' sensitive PHI with advertising companies and platforms, including Meta and Google. The FTC also reached a $7.8 million settlement with the online counseling service BetterHelp, resolving allegations that the company shared customer health data with Meta and Snapchat for advertising purposes. Likewise, the FTC reached a

---

57 *Id.* (emphasis added).

58 *See Id.*

settlement with Flo Health, Inc. related to information about fertility and pregnancy that Flo fertility-tracking app was improperly sharing with Meta, Google and other third parties. And Easy Healthcare was ordered to pay a $100,000 civil penalty for violating the Health Breach Notification Rule when its ovulation tracking app Premon shared health data for advertising purposes.[59]

148. Even more recently, in July 2023, federal regulators sent a letter to approximately 130 healthcare providers warning them about using online tracking technologies that could result in unauthorized disclosures of Private Information to third parties. The letter highlighted the "risks and concerns about the use of technologies, such as the Meta Pixel and Google Analytics, that can track a user's online activities," and warned about "[i]mpermissible disclosures of an individual's personal health information to third parties" that could "result in a wide range of harms to an individual or others." According to the letter, "[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."[60]

---

[59] *See* How FTC Enforcement Actions Will Impact Telehealth Data Privacy, https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy (last visited Feb. 29, 2024); *see also* Allison Grande, *FTC Targets GoodRx In 1st Action Under Health Breach Rule*, Law360 (Feb. 1, 2023), available at www.law360.com/articles/1571369/ftc-targets-goodrx-in1st-action-under-health-breach-rule?copied=1 ("The Federal Trade Commission signaled it won't hesitate to wield its full range of enforcement powers when it dinged GoodRx for allegedly sharing sensitive health data with advertisers, teeing up a big year for the agency and boosting efforts to regulate data privacy on a larger scale."); https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising; https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc (last visited Feb. 29, 2024); https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google (last visited Feb. 29, 2024).

[60] *See* OCR Bulletin, *supra* note 53.

149. This is further evidence that the data that Defendant chose to disclose is protected Private Information, and the disclosure of that information was a violation of Plaintiffs' and Class Members' rights.

I. Duly's Use of Tracking Technologies such as the Pixel Violation of HIPAA.

150. Defendant's disclosure of Plaintiffs' and Class Members' Private Information to entities like Meta also violated HIPAA, which provided Plaintiffs and Class Members with another reason to believe that the information they communicated to Defendant through its Website would be protected rather than shared with third-parties for marketing purposes.

151. Under federal law, a healthcare provider may not disclose PII, non-public medical information about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[61]

152. Guidance from HHS instructs healthcare providers that patient status alone is protected by HIPAA.

153. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (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 either (i) "identifies the individual;" or (ii) "[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.

154. The Privacy Rule broadly defines protected health information as individually

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

identifiable health information that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

155. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (i) 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 (ii) "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
> P. 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."[62]

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

157. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a

[62] *See* 45 C.F.R. § 160.514.

particular entity, can be PHI.

158. HHS has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, "[i]f 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."[63]

159. Consistent with this restriction, HHS has issued marketing guidance that provides, "With limited exceptions, the [Privacy] 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 or enrollees to third parties without obtaining authorization from each person on the list."[64]

160. Here, as described *supra*, Duly provided patient information to third parties in violation of the Privacy Rule—and its own Privacy Policy. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."

161. The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information … if the information is maintained by a covered entity

---

[63] *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, (last visited Feb. 29, 2024).

[64] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (last visited Feb. 29, 2024).

… and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320(d)(6).

162. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties 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. § 1320(d)(6)(b). In such cases, an 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." 42 U.S.C. § 1320(d)(6)(b)(1).

163. HIPAA also requires Duly to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(c), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights," 45 C.F.R. § 164.312(a)(1)—which Duly failed to do.

164. Under HIPAA, Duly may not disclose PII about a patient, potential patient or household member of a patient for marketing purposes without the patient's express written authorization. *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

165. Duly further failed to comply with other HIPAA safeguard regulations as follows:

a) Failing to ensure the confidentiality and integrity of electronic PHI that Duly created, received, maintained and transmitted in violation of 45 C.F.R. section 164.306(a)(1);

b) Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);

c) Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Duly in violation of 45 C.F.R. section 164.308(a)(6)(ii);

d) Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. section 164.306(a)(2);

e) Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3), and

f) Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

166. In disclosing the content of Plaintiffs and the Class Members' communications, Duly had a purpose that was tortious, criminal and designed to violate state constitutional and statutory provisions.

167. Commenting on a June 2022 report discussing the use of Meta Pixels by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it … It is quite likely a HIPAA violation."[65]

168. Duly's placing third-party tracking codes on its Web Properties is a violation of Plaintiffs' and Class Members' privacy rights under federal law. While Plaintiff do not bring a

[65] ADVISORY BOARD, '*Deeply Troubled*': *Security experts worry about Facebook trackers on hospital sites*, https://www.advisory.com/daily-briefing/2022/06/17/data-trackers (last visited Feb. 29, 2024).

claim under HIPAA itself, this violation demonstrates Duly's wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

J. Plaintiffs' & Class Members' Private Information Has Substantial Financial Value.

169. Plaintiffs and Class Members' Private Information had value, and Duly's disclosure and interception harmed Plaintiffs and the Class by not compensating them for the value of their Private Information and in turn decreasing the value of their Private Information.

170. Meta "generate[s] substantially all of [its] revenue from advertising."[66]

171. In addition to its own independent marketing programs, Meta also receives billions of dollars of unearned advertising sales revenue from Meta healthcare partners, including Duly, who are targeting Facebook users based on their health information.

172. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the technology economy.

173. Courts recognize the value of personal information and the harm when it is disclosed without consent. *See, e.g., In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that Plaintiffs'allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing "the value that personal identifying information has in our increasingly digital economy").

174. Healthcare data is particularly valuable on the black market because it often

[66] Meta 2022 Annual Report at 17.

contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

175. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

176. The value of health data is well-known and various reports have been conducted to identify its value.

177. Specifically, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[67]

178. Trustwave Global Security published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[68]

179. The value of health data has also been reported 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

---

[67] *See* https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Feb. 29, 2024).

[68] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (last visited Feb. 29, 2024) (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

and observed that the market for information was both lucrative and a significant risk to privacy.[69]

180. 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."[70]

181. The dramatic difference in the price of healthcare data compared to other forms of private information commonly sold is evidence of the value of PHI.

182. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

183. Meta's, Google's and others' practices of using such information to package groups of people as "Lookalike Audiences" and similar groups and selling those packages to advertising clients demonstrates the financial worth of that data. Data harvesting is the fastest growing industry in the nation.

184. As software, data mining and targeting technologies have advanced, the revenue from digital ads and the consequent value of the data used to target them have risen rapidly.

185. Consumer data is so valuable that some have proclaimed that data is the new oil.

186. Between 2016 and 2018, the value of information mined from Americans increased by 85% for Meta and 40% for Google.

187. Overall, the value internet companies derive from Americans' personal data increased almost 54%.

---

69 *See* https://time.com/4588104/medical-data-industry/ (last visited Feb. 29, 2024).

70 *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Feb. 28, 2024).

188. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user. By 2020, that value had jumped to approximately $420 per adult American user each year, making personal data sales a nearly $140 million industry.[71] In 2025, that value is expected to exceed $225 billion industry wide.[72]

189. As to health data specifically, as detailed in an article in Canada's National Post:

> As part of the multibillion-dollar worldwide data brokerage industry, health data is one of the most sought-after commodities. De-identified data can be re identified (citing https://www.nature.com/articles/s41467-019-10933-3/) and brazen decisions to release records with identifiable information (citing https://www.wsj.com/articles/hospitals-give-tech-giants-access-todetailed-medical-records-11579516200?mod=hp_lista_pos3) are becoming commonplace).[73]

190. Further demonstrating the financial value of Class Members' medical data, CNBC has reported that hospital executives have received a growing number of bids for user data:

> Hospitals, many of which are increasingly in dire financial straits, are weighing a lucrative new opportunity: selling patient health information to tech companies. Aaron Miri is chief information officer at Dell Medical School and University of Texas Health in Austin, so he gets plenty of tech start-ups approaching him to pitch deals and partnerships. Five years ago, he'd get about one pitch per

---

[71] Medium, HOW MUCH IS USER DATA WORTH?, March 16, 2020, https://pawtocol.medium.com/how-much-is-user-data-worth-f2b1b0432136 (last visited February 28, 2024); Invisibly, HOW MUCH IS YOUR DATA WORTH? THE COMPLETE BREAKDOWN FOR 2024, July 13, 2021, https://www.invisibly.com/learn-blog/how-much-is-data-worth/#:~:text=Together%2C%20internet%20advertising%20turned%20%24139.8,back%20of%20your%20personal%20data (last visited February 29, 2024).

[72] Invisibly, TOP INDUSTRIES AND COMPANIES THAT YOU'RE YOUR DATA, Aug. 20, 2021, https://www.invisibly.com/learn-blog/companies-selling-your-personal-data/ (last visited February 29, 2024).

[73] *See* National Post, IRIS KULBATSKI: THE DANGERS OF ELECTRONIC HEALTH RECORDS, February 26, 2020, https://nationalpost.com/opinion/iris-kulbatski-the-dangers-of-electronichealth-records (last visited February 29, 2024).

> quarter. But these days, with huge data-driven players like Amazon and Google making incursions into the health space, and venture money flooding into Silicon Valley start-ups aiming to bring machine learning to health care, the cadence is far more frequent. "It's all the time," he said via phone. "Often, once a day or more."
>
> * * *
>
> [H]ealth systems administrators say [the data] could also be used in unintended or harmful ways, like being cross-referenced with other data to identify individuals at higher risk of diseases and then raise their health premiums, or to target advertising to individuals.[74]

191. The CNBC article also explained:

> De-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. Just one company alone, IQVIA, said on its website that it has access to more than 600 million patient records globally that are nonidentified, much of which it accesses through provider organizations. The buyers, which include pharma marketers, will often use it for things like clinical trial recruiting But hospital execs worry that this data may be used in unintended ways, and not always in the patient's best interest.
>
> * * *

192. Tech companies are also under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own needs. For instance, the health data Google collects could eventually help it micro-target advertisements to people with particular health conditions. Policymakers are proactively calling for a revision and potential upgrade of the health privacy rules known as HIPAA, out of concern for what might

[74] CNBC, HOSPITAL EXECS SAY THEY ARE GETTING FLOODED WITH REQUESTS FOR YOUR HEALTH DATA, https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited February 29, 2024).

happen as tech companies continue to march into the medical sector.[75]

193. Time Magazine similarly, in an article titled, *How your Medical Data Fuels A Hidden Multi-Billion Dollar Industry*, referenced the "growth of the big health data bazaar," in which patients' health information is sold. It reported that:

> [T]he secondary market in information unrelated to a patient's direct treatment poses growing risks, privacy experts say. That's because clues in anonymized patient dossiers make it possible for outsiders to determine your identity, especially as computing power advances in the future.[76]

194. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[77]

195. These There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

196. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

197. Duly gave away Plaintiffs' and Class Members' communications and transactions on its Website without permission.

---

75 *Id.*

76 Time, HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY, https://time.com/4588104/medical-data-industry/ (last visited Feb. 29, 2024).

77 *See 10 Apps for Seling Your Data for* Cash, https://wallethacks.com/apps-for-selling-your-data/ (last visited Feb. 29, 2024).

198. The unauthorized to Plaintiffs' and Class Members' personal and Private Information has diminished the value of that information, resulting in harm to Web Properties Users, including Plaintiffs and Class Members.

199. Plaintiff has a continuing interest in ensuring that their future communications with Duly are protected and safeguarded from future unauthorized disclosure.

K. Defendant Violated Industry Standards

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

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

202. AMA Code of Ethics Opinion 3.1.1 provides that "[p]rotecting 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)[.]

203. 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.

204. 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.[78]

L. Plaintiffs' & Class Members' Expectation of Privacy

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

206. Indeed, at all times when Plaintiffs and Class Members provided their PII and PHI to Defendant, they each 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.

207. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

208. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[79]

209. Personal data privacy and obtaining consent to share Private Information are material to Plaintiffs and Class Members.

---

[78] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (last visited February 29, 2024).

[79] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/ (last visited February 29, 2024).

210. Plaintiffs' and Class Members' reasonable expectations of privacy in their PII/PHI are grounded in, among other things, Defendant's status as a healthcare provider, Defendant's common law obligation to maintain the confidentiality of patients' PII/PHI, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Defendant's express and implied promises of confidentiality.

M. Unique Personal Identifiers, including IP Addresses, are Protected Health Information.

211. While not all health data is covered under HIPAA, the law specifically applies to healthcare providers, health insurance providers and healthcare data clearinghouses.[80]

212. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered PII. This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual.

213. These HIPAA Identifiers, as relevant here, include names, dates related to an individual, email addresses, device identifiers, web URLs and IP addresses.[81]

214. Duly improperly disclosed Plaintiffs' and Class Members' HIPAA identifiers,

---

[80] *See* Alfred Ng &_Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids' Information to Facebook* (June 21, 2022), https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook (stating that "[w]hen you are going to a covered entity's website, and you're entering information related to scheduling an appointment, including your actual name, and potentially other identifying characteristics related to your medical condition, there's a strong possibility that HIPAA is going to apply in those situations") (last visited February 29, 2024).

[81] *Guidance regarding Methods for De-identification of Protected Health Information, supra*, n. 63.

including their names, emails, dates they sought treatments, computer IP addresses, device identifiers and web URLs visited to third parties through their use of the Pixels *in addition to* services selected, patient statuses, medical conditions, treatments, provider information and appointment information.

215. HIPAA further declares information as personally identifiable where the covered entity has "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. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

216. In addition to patient status, medical conditions, treatment, specific providers, appointment information and patient's unique and persistent Facebook ID, Defendant improperly disclosed patients' computer IP addresses to Meta through the use of the Pixel.

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

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

222. Meta, 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.

224. 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).

225. Consequently, Defendant's disclosure of patients' IP addresses violated HIPAA and industry-wide privacy standards

N. Defendant was Enriched & Benefitted from the Use of The Pixel & Unauthorized Disclosures.

226. The sole purpose of the use of the Meta Pixel on Defendant's Web Properties was marketing and profits.

227. In exchange for disclosing the Personal Information of its patients, Defendant is compensated by Meta in the form of enhanced advertising services and more cost-efficient marketing on Meta.

228. After receiving individually identifiable patient health information communicated on Duly's Web Properties, Meta forwards this data, and its analysis of this data, to Duly.

229. Duly then uses this data and analysis for its own commercial purposes that include understanding how Users utilize its Web Properties.

230. Duly also receives an additional commercial benefit from using Meta's tracking tools, such as the Meta Pixel and CAPI, namely being able to serve more targeted advertisements to existing and prospective patients on their Meta accounts such as Facebook and Instagram.

231. Meta advertises its Pixel as a piece of code "that can help you better understand the ***effectiveness of your advertising*** and the actions people take on your site."[82]

232. Upon information and belief, Defendant was advertising its services on Facebook,

---

[82] *What is the Meta Pixel,* https://www.facebook.com/business/tools/meta-pixel (emphasis added) (last visited Feb. 29, 2024).

and the Pixel was used to "help [Defendant] understand the success of [its] advertisement efforts on Facebook."[83]

233. Retargeting is a form of online marketing that targets users with ads based on previous internet communications and interactions. In particular, retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.[84]

234. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Meta via the tracking technologies and the Pixel embedded on, in this case, Duly's Web Properties. For example, when a User searches for doctors or medical conditions or treatment on Duly's Web Properties, that information is sent to Meta. Meta can then use its data on the User to find more users to click on am Duly ad and ensure that those users targeted are more likely to convert.[85]

235. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures, "includes URL names of pages visited, and actions taken—all of which could be potential examples of health information."[86]

---

83 HEALTHCARE PROVIDER ISSUES WARNING AFTER TRACKING PIXELS LEAK PATIENT DATA, https://www.infosecurity-magazine.com/news/novant-leak-meta-tracking-pixel/ (last visited Feb. 29, 2024).

84 *The complex world of healthcare retargeting,* https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/ (last visited February 29, 2024).

85 *See, e.g.*, *How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023), https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking (last visited February 29, 2024).

86 *Id*.

236. Plaintiffs' and Class Members' Private Information has considerable value as highly monetizable data especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

237. In exchange for disclosing the Private Information of their account holders and patients, Duly is compensated by Meta in the form of enhanced advertising services and more cost-efficient marketing on their platform(s).

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

Plaintiff Patricia Mayer

238. Plaintiff Mayer has been a patient of Defendant and has been accessing the Web Properties since at least 2019.

239. As a condition of receiving Defendant's services, Plaintiff Mayer disclosed her Private Information to Defendant on numerous occasions, and most recently in February 2023.

240. Plaintiff Mayer accessed Defendant's Website and Patient Portal on her phone, computer and tablet to receive healthcare services from Defendant and at Defendant's direction.

241. Plaintiff Mayer has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

242. During the relevant time period, when the Defendant's Pixels were present, Plaintiff Mayer used Defendant's Website, *https://www.dulyhealthandcare.com/,* to research providers including [redacted]; specific health conditions (including but not limited to, [redacted]) and treatments (including but not limited to, [redacted]); look for Defendant's locations close to her address; and schedule doctor's appointments for herself including appointments with [redacted] The full scope of Duly's interceptions and disclosures of Plaintiffs' communications to

Meta can only be determined through formal discovery. However, Duly intercepted at least the following communications about Plaintiffs' prospective healthcare. The following long-URLs or substantially similar URLs were sent to Meta via the Pixel:

[redacted]

243. Contemporaneously with the interception and transmission of Plaintiff's communications on *https://www.dulyhealthandcare.com*, Defendant also disclosed to Meta Plaintiff's personal identifiers, including but not limited to her IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers.

244. During the relevant time period, when Defendant's Pixels were present, Plaintiff used Duly's MyChart Patient Portal to research providers [redacted]; schedule doctor's appointments for herself [redacted]; look at her bills and payments and to see her test results. The full scope of Duly's interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, Duly intercepted at least the following communications about Plaintiff's prospective healthcare. The following long-URLs or substantially similar URLs were sent to Meta via the Pixel:

245. Contemporaneously with the interception and transmission of Plaintiff's communications on Duly's Portal, Defendant also disclosed to Meta Plaintiff's personal identifiers, including but not limited to her IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers.

246. When Plaintiff Mayer engaged in these communications with Defendant's Web Properties, Defendant's Pixels intercepted individually identifiable health information that included: her status as a Duly patient, the dates and times she logged-in to the MyChart Patient Portal, and the webpages she clicked and viewed related to her medical providers, conditions, and treatments. Because Defendant and Meta's conduct was surreptitious and conducted through back-end electronic systems and processes, Plaintiff will seek specific information about these intercepted and transmitted communications in discovery. However, when Plaintiff used her digital devices to visit Defendant's Website or log-in to the Duly MyChart Patient Portal, which she did many times during the relevant period in connection with communications about her medical providers, appointments, test results, treatments, and prescriptions, Defendant's Pixels Duly's Web Properties sent at least the following personally identifiable patient information and patient health information to Meta[87]:

a. Mayer was communicating with Duly on its https://www.dulyhealthandcare.com/ website and on its MyChart Patient Portal;

[87] Plaintiffs' investigation has revealed that Duly has removed the Pixel from all its Web Properties. Accordingly, the full extent of Defendant's interception and disclosure of individually identifiable health information can only be determined through formal discovery.

b. Mayer engaged in an "ev,"' or event, called "PageView," "MicroData," "SubscribedButtonClick," or something substantially similar;

c. Descriptive URLs that describe the categories of the Website, categories that describe the current section of the Website, and the referrer URL that caused navigation to the current page;

d. Button/menu selections and/or content typed into free text boxes;

e. The content of the button Plaintiff clicked was "Sign In" to MyChart, or something substantially similar;

f. The page on which Plaintiff clicked the button was "Patient Portal," "Home," or something substantially similar;

g. Plaintiff had previously visited a Duly webpage;

h. Plaintiff's Internet Protocol address;

i. Identifiers that Meta uses to identify Plaintiff Mayer and her devices, including but not limited to, the "c-user," "datr," "fr," and "fbp" cookies; and

j. Browser attribute information sufficient to fingerprint Plaintiff Mayer's device.

247. As a result, the Pixels on Defendant's Web Properties intercepted and disclosed to Meta information about Plaintiff Mayer's identity, her log-in to the patient portal, and the content of the communications she made on Duly's Web Properties.

248. Duly never notified Plaintiff Mayer that either it or Meta would put individually identifiable patient health information about her past, present, or future health conditions to their own commercial uses. Plaintiff Mayer never provided informed consent or written permission allowing Duly to send individually identifiable patient health information about her past, present, or future health conditions to Meta. Plaintiff never provided informed consent or written

permission allowing Duly or Meta to put individually identifiable patient health information about her past, present, or future health conditions to their own commercial use.

249. Plaintiff Mayer is diagnosed with specific medical condition [redacted] and submitted information to Defendant's Website and Portal about scheduling medical appointments for her condition and receiving specific tests for it.

250. After submitting her Private Information to Defendant, Plaintiff Mayer began to receive spam and ads on Facebook and other social media related to her medical condition.

251. Meta maintains a history of every ad it has shown to Plaintiffs and the Class Members, both on and off Meta's social media sites, including on Meta properties and the Facebook Audience Network through which Meta serves ads to Facebook users on non-Meta websites. Plaintiff intends to seek this information in discovery to fully inform the scope of her claims and damages.

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

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

254. By doing so without her consent, Defendant breached Plaintiff Mayer's privacy and unlawfully disclosed her Private Information.

255. Plaintiff Mayer suffered damages in the forms of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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.

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

Plaintiff Mary Murphy

257. As a condition of receiving Defendant's services, Plaintiff Murphy disclosed her Private Information to Defendant on numerous occasions, and most recently in February 2024.

258. Plaintiff Murphy accessed Defendant's Website and Patient Portal on her phone, computer and tablets to receive healthcare services from Defendant and at Defendant's direction.

259. Plaintiff Murphy has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

260. During the relevant time period, when the Defendant's Pixels were present, Plaintiff Murphy used Defendant's Website, *https://www.dulyhealthandcare.com/*, to research providers, specific health conditions (including but not limited to, [redacted]) and treatments (including but not limited to, [redacted]), look for Defendant's locations close to her address, and schedule doctor's appointments for herself (including but not limited to, appointments with [redacted]). The full scope of Duly's interceptions and disclosures of Plaintiffs' communications to Meta can only be determined through formal discovery. However, Duly intercepted at least the following communications about Plaintiffs' prospective healthcare. The following long-URLs or substantially similar URLs were sent to Meta via the Pixel:

https://www.dulyhealthandcare.com/physicians?page=1&search_physician_attribute=anxiety&a

ddress=wood+dale++IL

https://www.dulyhealthandcare.com/physicians?page=1&search_physician_attribute=insomnia&address=wood+dale++IL

https://www.dulyhealthandcare.com/physicians?page=1&search_physician_attribute=asthma&address=wood+dale++IL

https://www.dulyhealthandcare.com/physicians?page=1&search_physician_attribute=wrist+pain&address=wood+dale++IL

https://www.dulyhealthandcare.com/physicians?page=1&search_physician_attribute=allergies&address=wood+dale++IL

https://www.dulyhealthandcare.com/physicians?page=1&search_physician_attribute=dermatologist&address=wood+dale++IL

261. Contemporaneously with the interception and transmission of Plaintiffs' communications on *https://www.dulyhealthandcare.com*, Defendant also disclosed to Meta Plaintiffs' personal identifiers, including but not limited to her IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers.

262. During the relevant time period, when Defendant's Pixels were present, Plaintiff used Duly's MyChart Patient Portal to research providers and schedule doctor's appointments for herself including but not limited to, [redacted]; research medications and devices provided for her specific health conditions including but not limited to, [redacted]; look for Defendant's locations close to her address; refill prescriptions [redacted]

[redacted] look at her bills and payments and to see her test results. The full scope of Duly's interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, Duly intercepted at least the following communications about Plaintiff's prospective healthcare. The following long-URLs or substantially similar URLs were sent to Meta via the Pixel:

[redacted]

263. Contemporaneously with the interception and transmission of Plaintiff's communications on Duly's Portal, Defendant also disclosed to Meta Plaintiff's personal identifiers, including but not limited to her IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers.

264. When Plaintiff Murphy engaged in these communications with Defendant's Web Properties, Defendant's Pixels intercepted individually identifiable health information that included: her status as a Duly patient, the dates and times she logged-in to the MyChart Patient Portal, and the webpages she clicked and viewed related to her medical providers, conditions, and treatments. Because Defendant and Meta's conduct was surreptitious and conducted through back-end electronic systems and processes, Plaintiff will seek specific information about these intercepted and transmitted communications in discovery. However, when Plaintiff used her digital devices to visit Defendant's Website or log-in to the Duly MyChart Patient Portal, which she did many times during the relevant period in connection with communications about her medical

providers, appointments, test results, treatments, and prescriptions, Defendant's Pixels Duly's Web Properties sent at least the following personally identifiable patient information and patient health information to Meta.[88]

a. Murphy was communicating with Duly on its https://www.dulyhealthandcare.com/ website and on its MyChart Patient Portal;

b. Murphy engaged in an "ev,"' or event, called "PageView," "MicroData," "SubscribedButtonClick," or something substantially similar;

c. Descriptive URLs that describe the categories of the website, categories that describe the current section of the website, and the referrer URL that caused navigation to the current page;

d. Button/menu selections and/or content typed into free text boxes;

e. The content of the button Plaintiff clicked was "Sign In" to MyChart, or something substantially similar;

f. The page on which Plaintiff clicked the button was "Patient Portal," "Home," or something substantially similar;

g. Plaintiff had previously visited a Duly webpage;

h. Plaintiff's Internet Protocol address;

i. Identifiers that Meta uses to identify Plaintiff Murphy and her devices, including but not limited to, the "c-user," "datr," "fr," and "fbp" cookies; and

j. Browser attribute information sufficient to fingerprint Plaintiff Murphy's device.

265. As a result, the Pixels on Defendant's Web Properties intercepted and disclosed to

[88] Plaintiffs' investigation has revealed that Duly has removed the Pixel from all its Web Properties. Accordingly, the full extent of Defendant's interception and disclosure of individually identifiable health information can only be determined through formal discovery.

Meta information about Plaintiff Murphy's identity, her log-in to the patient portal, and the content of the communications she made on Duly's Web Properties.

266. Duly never notified Plaintiff Murphy that either it or Meta would put individually identifiable patient health information about her past, present, or future health conditions to their own commercial uses. Plaintiff Murphy never provided informed consent or written permission allowing Duly to send individually identifiable patient health information about her past, present, or future health conditions to Meta. Plaintiff never provided informed consent or written permission allowing Duly or Meta to put individually identifiable patient health information about her past, present, or future health conditions to their own commercial use.

267. Plaintiff Murphy is diagnosed with several specific medical conditions including but not [redacted] and submitted information to Defendant's Website and Portal about scheduling medical appointments for her conditions and receiving specific medications for them.

268. After submitting her Private Information to Defendant, Plaintiff Murphy began to receive spam and ads on Facebook and other social media related to [redacted].

269. Meta maintains a history of every ad it has shown to Plaintiffs and the Class Members, both on and off Meta's social media sites, including on Meta properties and the Facebook Audience Network through which Meta serves ads to Facebook users on non-Meta websites. Plaintiff intends to seek this information in discovery to fully inform the scope of her claims and damages.

270. Plaintiff Murphy provided her Private Information to Defendant and trusted that the

information would be safeguarded according to Defendant's policies and state and federal law.

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

272. By doing so without her consent, Defendant breached Plaintiff Murphy's privacy and unlawfully disclosed her Private Information.

273. Plaintiff Murphy suffered damages in the forms of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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.

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

Plaintiff Catherine Massarelli

275. As a condition of receiving Defendant's services, Plaintiff Massarelli disclosed her Private Information to Defendant on numerous occasions, and most recently in February 2024.

276. Plaintiff Massarelli accessed Defendant's Website and Patient Portal on her computer and tablet to receive healthcare services from Defendant and at Defendant's direction.

277. Plaintiff Massarelli has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

278. During the relevant time period, when the Defendant's Pixels were present, Plaintiff Massarelli used Defendant's Website, *https://www.dulyhealthandcare.com/,* to research providers, specific health conditions (including but not limited to providers specializing in [redacted])

and treatments (including but not limited to, medications for [redacted]); look for Defendant's locations close to her address; and schedule doctor's appointments for herself (including but not limited to, appointments with a [redacted]). The full scope of Duly's interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, Duly intercepted at least the following communications about Plaintiff's prospective healthcare. The following long-URLs or substantially similar URLs were sent to Meta via the Pixel:

279. Contemporaneously with the interception and transmission of Plaintiffs' communications on *https://www.dulyhealthandcare.com*, Defendant also disclosed to Meta Plaintiffs' personal identifiers, including but not limited to her IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers.

280. During the relevant time period, when Defendant's Pixels were present, Plaintiff used Duly's MyChart Patient Portal to research and communicate with her providers [redacted]; review test results and appointment summaries related to diagnosing and treating [redacted]; and look at her bills and payments. The full scope of Duly's interceptions and disclosures of Plaintiff's communications to Meta can

only be determined through formal discovery. However, Duly intercepted at least the following communications about Plaintiff's prospective healthcare. The following long-URLs or substantially similar URLs were sent to Meta via the Pixel:

281. Contemporaneously with the interception and transmission of Plaintiff's communications on Duly's Portal, Defendant also disclosed to Meta Plaintiff's personal identifiers, including but not limited to her IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers.

282. When Plaintiff Massarelli engaged in these communications with Defendant's Web Properties, Defendant's Pixels intercepted individually identifiable health information that included: her status as a Duly patient, the dates and times she logged-in to the MyChart Patient Portal, and the webpages she clicked and viewed related to her medical providers, conditions, and treatments. Because Defendant and Meta's conduct was surreptitious and conducted through back-end electronic systems and processes, Plaintiff will seek specific information about these intercepted and transmitted communications in discovery. However, when Plaintiff used her digital devices to visit Defendant's Website or log-in to the Duly MyChart Patient Portal, which she did many times during the relevant period in connection with communications about her medical providers, appointments, test results, treatments, and prescriptions, Defendant's Pixels Duly's Web Properties sent at least the following personally identifiable patient information and patient

health information to Meta[89]:

a. Massarelli was communicating with Duly on its https://www.dulyhealthandcare.com/ website and on its MyChart Patient Portal;

b. Massarelli engaged in an "ev,"' or event, called "PageView," "MicroData," "SubscribedButtonClick," or something substantially similar;

c. Descriptive URLs that describe the categories of the website, categories that describe the current section of the website, and the referrer URL that caused navigation to the current page;

d. Button/menu selections and/or content typed into free text boxes;

e. The content of the button Plaintiff clicked was "Sign In" to MyChart, or something substantially similar;

f. The page on which Plaintiff clicked the button was "Patient Portal," "Home," or something substantially similar;

g. Plaintiff had previously visited a Duly webpage;

h. Plaintiffs' Internet Protocol address;

i. Identifiers that Meta uses to identify Plaintiff Massarelli and her devices, including but not limited to, the "c-user," "datr," "fr," and "fbp" cookies; and

j. Browser attribute information sufficient to fingerprint Plaintiff Massarelli's device.

283. As a result, the Pixels on Defendant's Web Properties intercepted and disclosed to Meta information about Plaintiff Massarelli's identity, her log-in to the patient portal, and the content of the communications she made on Duly's Web Properties.

[89] Plaintiffs' investigation has revealed that Duly has removed the Pixel from all its Web Properties. Accordingly, the full extent of Defendant's interception and disclosure of individually identifiable health information can only be determined through formal discovery.

284. Duly never notified Plaintiff Massarelli that either it or Meta would put individually identifiable patient health information about her past, present, or future health conditions to their own commercial uses. Plaintiff Massarelli never provided informed consent or written permission allowing Duly to send individually identifiable patient health information about her past, present, or future health conditions to Meta. Plaintiff never provided informed consent or written permission allowing Duly or Meta to put individually identifiable patient health information about her past, present, or future health conditions to their own commercial use.

285. Plaintiff Massarelli is diagnosed with a specific medical condition [redacted] and submitted information to Defendant's Website and Portal about scheduling medical appointments for her conditions and receiving specific medications for them.

286. After submitting her Private Information to Defendant, Plaintiff Massarelli began to receive spam and ads on Facebook and other social media related to [redacted], including ads from companies selling various type of products for [redacted].

287. Meta maintains a history of every ad it has shown to Plaintiffs and the Class Members, both on and off Meta's social media sites, including on Meta properties and the Facebook Audience Network through which Meta serves ads to Facebook users on non-Meta websites. Plaintiff intends to seek this information in discovery to fully inform the scope of her claims and damages.

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

289. Plaintiff Massarelli reasonably expected that her communications with Defendant via the Web Properties were confidential, solely between herself and Defendant, and that such

communications would not be transmitted to or intercepted by a third party.

290. By doing so without her consent, Defendant breached Plaintiff Massarelli's privacy and unlawfully disclosed her Private Information.

291. Plaintiff Massarelli suffered damages in the forms of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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 Massarelli has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

TOLLING

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

CLASS ACTION ALLEGATIONS

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

295. The 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 Pixel on Defendant's Web Properties.

296. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries,

any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

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

298. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(1), because the Class Members are so numerous and geographically dispersed that their joinder would be impracticable. Plaintiffs believe that Defendant's and Meta's business records will permit the identification of thousands of people meeting the Class definition.

299. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(2), because there are many common questions of facts and law concerning and affecting the Class Members, including:

a. Whether Duly had a duty to protect and refrain from disclosing the Class Members' individually identifiable health information;

b. Whether Duly intentionally disclosed the Class Members' individually identifiable health information to Meta;

c. Whether the Class Members consented to Duly's disclosure of their individually identifiable health information to Meta;

d. Whether the Class Members are entitled to damages because of Duly's conduct; and

e. Whether Duly's knowing disclosure of its patients' individually identifiable health information to Meta is "criminal or tortious" under 18 U.S.C. § 2511(2)(d).

300. Plaintiffs also anticipate that Defendant will raise defenses common to the Class.

301. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(3), because Plaintiffs' claims are typical of the claims belonging to the Class Members. Plaintiffs and

the Class Members were harmed by the same wrongful conduct perpetrated by Defendant that caused their individually identifiable health information to be intercepted and disclosed without notice or consent. As a result, Plaintiffs' claims are based on the same facts and legal theories as the Class Members' claims.

302. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(4), because Plaintiffs will fairly and adequately protect the interests of all the Class Members, there are no known conflicts of interest between Plaintiffs and the Class Members, and Plaintiffs have retained counsel experienced in the prosecution of complex litigation.

303. Class certification is appropriate under Fed. R. Civ. P. 23(b)(3), because common questions of law and fact predominate over questions affecting the individual Class Members, because a class action is superior to other available methods for the fair and efficient adjudication of these claims and because important public interests will be served by addressing the matter as a class action. Further, the prosecution of separate actions by the individual Class Members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendant and substantially impair the Class Members' ability to protect their interests.

304. The State of Illinois has a significant interest in regulating the conduct of businesses operating within its borders.

305. The State of Illinois has a significant interest in regulating the conduct of businesses operating within its borders.

306. Illinois, which seeks to protect the rights and interests of Illinois and all residents and citizens of the United States against a company headquartered and doing business in Illinois, has a greater interest in the claims of Plaintiffs and the Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

307. The principal place of business and headquarters of Duly, located in Illinois, is the "nerve center" of its business activities—the place where its high-level officers direct, control and coordinate its activities, including major policy, financial and legal decisions.

308. Upon information and good faith belief, Defendant's actions and corporate decisions surrounding the allegations made in the Amended Complaint were made from and in Illinois.

309. Defendant's breaches of duty to Plaintiffs and Class Members emanated from Illinois.

310. Application of Illinois law to the Classes with respect to Plaintiffs' and the Class' common law claims is neither arbitrary nor fundamentally unfair because, further to choice of law principles applicable to this action, the common law of Illinois applies to the nationwide common law claims of all Class Members. Additionally, given Illinois' significant interest in regulating the conduct of businesses operating within its borders, and that Illinois has the most significant relationship to Defendant, as it is headquartered in Illinois, there is no conflict in applying Illinois law to non-resident consumers such as Plaintiffs and Class Members. Alternatively, and/or in addition to Illinois law, the laws set forth below apply to the conduct described herein.

COUNT I
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. § 2511(1), *et seq.*
(*On Behalf of Plaintiffs & the Class*)

311. Plaintiffs incorporate and re-allege the allegations contained in the foregoing paragraphs as if fully set forth herein.

312. The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

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

314. The ECPA provides a private right of action to any person whose wire or electronic communications are intercepted. 18 U.S.C. § 2520(a).

315. Duly intentionally intercepted electronic communications that Plaintiffs and the Class Members exchanged with Duly through the Meta Pixel installed on Duly's Web Properties.

316. The transmissions of data between Plaintiffs and the Class Members and Duly qualify as communications under the ECPA. 18 U.S.C. § 2510(12).

317. Duly contemporaneously intercepted and transmitted Plaintiffs' and the Class Members' communications to Meta.

318. The intercepted communications include:

a. the content of Plaintiffs' and the Class Members' registrations for patient portals, including clicks on buttons to "Register" or "Signup" for portals;

b. the content Plaintiffs' and the Class Members' log in and log out of patient portals, including clicks to "Sign-in," "Log-in," "Sign-out," or "Log-out";

c. the content of communications that Plaintiffs and the Class Members exchange inside patient portals immediately before logging out of the portals;

d. the content of Plaintiffs' and the Class Members' communications relating to appointments with medical providers;

e. the content of Plaintiffs' and the Class Members' communications relating to specific healthcare providers, conditions, treatments, diagnoses, prognoses, prescription drugs, symptoms, insurance, and payment information;

f. Button/menu selections and/or content typed into free text boxes; and

g. Full-string URLs that contain any information concerning the

substance, purport, or meaning of patient communications with their health entities.

319. For example, Defendant's interception of the fact that a patient views a webpage like *https://www.dulyhealthandcare.com/conditions/cervical-cancer*, involves "content," because it communicates that patient's request for the information on that page.

320. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. the cookies Duly and Meta use to track Plaintiffs' and the Class Members' communications;

b. Plaintiffs' and the Class Members' browsers;

c. Plaintiffs' and the Class Members' computing devices;

d. Duly's web-servers or webpages where the Meta Pixel is present;

e. Meta's web-servers; and

f. the Meta Pixel and CAPI source code Duly deploys on its web properties to acquire Plaintiffs' and the Class Members' communications.

321. Meta is not a party to Plaintiffs' and the Class Members' communications with Duly.

322. Duly transmits the content of Plaintiffs' and the Class Members' communications to Meta through the surreptitious redirection of those communications from Plaintiffs' and the Class Members' computing devices.

323. Plaintiffs and the Class Members did not consent to Meta's acquisition of their patient portal, appointment, and treatment communications with Duly.

324. Meta did not obtain legal authorization to obtain Plaintiffs' and the Class Members' communications with Duly relating to communications with their health entities.

325. Meta did not require Duly to obtain the lawful rights to share the content of

Plaintiffs' and the Class Members' communications relating to patient portals, appointments, and treatments.

326. Any purported consent that Meta received from Duly to obtain the content of Plaintiffs' and the Class Members' communications was not valid.

286. In disclosing the content of Plaintiffs' and the Class Members' communications relating to patient portals, treatments, conditions, and appointments, Duly had a purpose that was tortious, criminal and designed to violate state constitutional and statutory provisions including:

a. the unauthorized disclosure of individually identifiable health information is tortuous in and of itself regardless of whether the means deployed to disclose the information violates the Wiretap Act or any subsequent purpose or use for the acquisition. Duly intentionally committed a tortious act by disclosing individually identifiable health information without authorization to do so.

b. the unauthorized acquisition of individually identifiable health information is a criminal violation of 42 U.S.C. § 1320d-6 regardless of any subsequent purpose or use of the individually identifiable health information. Duly intentionally violated 42 U.S.C. 1320d-6 by intentionally disclosing individually identifiable health information without authorization.

c. a violation of HIPAA, particularly 42 U.S.C. § 1320d-6, which is a criminal offensive punishable by fine or imprisonment with *increased penalties* where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage [or] personal gain." Duly provision of 42 U.S.C. § 1320d-6 by disclosing the individually identifiable health information "with intent to sell transfer or use" it for "commercial advantage [or] personal gain."

d. a knowing intrusion upon Plaintiffs' and the Class Members' seclusion;

e. trespass upon Plaintiffs' and the Class Members' personal and private property via the placement of an _fbp cookie associated with Duly's web properties on Plaintiffs' and the Class Members' personal computing devices;

f. the requirement under 410 ILCS § 5/30 that healthcare providers maintain the confidentiality of patient health records; and

g. violation of the federal wire fraud statutes at 18 U.S.C. §§ 1343 (fraud by wire, radio, or television) and 1349 (attempt and conspiracy), which prohibit a person from "devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate … commerce, any writing, signs, signals, pictures, or sounds for purpose of executing such scheme or artifice."

327. The federal wire fraud statute, 18 U.S.C. § 1343, has four elements: (1) that the defendant voluntarily and intentionally devised a scheme to defraud another out of money or property; (2) that the defendant did so with the intent to defraud; (3) that is was reasonably foreseeable that interstate wire communications would be used; and (4) that interstate wire communications were in fact used. The attempt version of the wire fraud statute provides that "[a]ny person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy." 18 U.S.C. § 1349.

328. Any party exception in 18 U.S.C. § 2511(2)(d) does not apply. The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information to a third party.

329. Plaintiffs' and Class Members' information that Defendant disclosed to third

parties qualifies as IIHI, and Defendant violated Plaintiffs' expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixels and other tracking codes to track and utilize Plaintiffs' and Class Members' Private Information for its own financial benefit.

330. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' and Class Members' privacy via the Pixel. Plaintiffs and Class Members had a reasonable expectation that Defendant would not re-direct their communications content to Meta, Google or others attached to their personal identifiers in the absence of their knowledge or consent.

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

332. Duly's scheme or artifice to defraud in this action further consists of:

a. the false and misleading statements and omissions in its privacy policies set forth above, including the statements and omissions recited in the breach of contract and negligence claims below;

b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie of Duly's web properties rather than a third-party cookie from Meta

333. Duly acted with the intent to defraud in that it willfully invaded and took Plaintiffs' and the Class Members' property:

a. property rights to the confidentiality of their individually identifiable health information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b. property rights to determine who has access to their computing devices.

334. Duly acted with the intent to defraud in that it willfully invaded and took Plaintiffs' and the Class Members' property:

a. with knowledge that (1) Duly did not have the right to share such data without written authorization; (2) courts had determined that a healthcare providers' use of the Meta Pixel gave rise to claims for invasion of privacy and violations of state criminal statutes; (3) a reasonable Facebook user would not understand that Meta was collecting their individually-identifiable health information based on their activities on Duly's web properties; (4) "a reasonable Facebook user would be shocked to realize" the extent of Meta's collection of individually-identifiable health information; (5) a Covered Incident had occurred which required a report to be made to the FTC pursuant to Meta's consent decrees with the FTC; and (6) the subsequent use of health information for advertising was a further invasion of such property rights in making their own exclusive use of their individually-identifiable health information for any purpose not related to the provision of their healthcare; and

b. with the intent to (1) acquire Plaintiffs and the Class Members' individually-identifiable health information without their authorization and without their healthcare providers or covered entities obtaining the right to share such information; (2) use Plaintiffs' and the Class Members' individually-identifiable health information without their authorization; and (3) gain access to the Plaintiffs' and the Class Members' personal computing devices through the 'fbp' cookie disguised as a first-party cookie

335. Plaintiffs and the Class Members have suffered damages because of Duly's violations of the ECPA that include:

a. Duly eroded the essential, confidential nature of the provider-patient relationship;

b. Duly failed to provide Plaintiffs 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;

c. Duly derived valuable benefits from using and sharing the contents of Plaintiffs' and the Class Members' communications on its web properties without their knowledge or informed consent, and without providing any compensation for the information it used or shared;

d. Duly's actions deprived Plaintiffs and the Class Members of the value of their individually identifiable health information;

e. Duly's actions diminished the value of Plaintiffs' and the Class Members' property rights in their individually identifiable health information; and

f. violating Plaintiffs' and the Class Members' privacy rights by sharing their individually identifiable health information for commercial use.

336. For Duly's violations set forth above, Plaintiffs and the Class Members seek appropriate equitable or declaratory relief, including injunctive relief; actual damages and "any profits made by [Duly] as a result" of its violations or the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred pursuant to 18 U.S.C § 2520.

337. Unless enjoined, Duly may continue to commit the violations of law alleged here.

338. Plaintiffs want to continue to communicate with their healthcare providers through online platforms but has no practical way of knowing if their communications are being intercepted and disclosed to Meta, and thus continues to be at risk of harm from Duly's conduct.

339. Pursuant to 18 U.S.C. § 2520, Plaintiffs and the Class Members seek monetary damages for the *greater of* (i) the sum of the actual damages suffered by the plaintiff and any profits made by Duly as a result of the violation or (ii) statutory damages of whichever is greater of $100 a day for each violation or $10,000.

COUNT II
VIOLATION OF ILLINOIS EAVESDROPPING STATUTE
720 ILCS 5/14-1, *et seq.*
(*On Behalf of Plaintiffs & the Class*)

303. Plaintiffs incorporate and re-allege each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

304. Defendant violated 720 ILCS 5/14-2(a)(2), which provides that a person or entity violates the Illinois Eavesdropping Statute "when he or she knowingly and intentionally . . . [u]ses an eavesdropping device, in a surreptitious manner, for the purpose of transmitting or recording all or any part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation." 720 ILCS 5/14-2(a)(2).

305. Defendant also violated 720 ILCS 5/14-2(a)(5) which provides that a person or entity violates the Illinois Eavesdropping Statute when they "[u]se[] or disclose[] any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication in violation of this Article, unless he or she does so with the consent of all of the parties."

306. The Illinois Eavesdropping Statute broadly defines "Private electronic communication," as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation." 720 ILCS 5/14-1(e).[90]

[90] According to the statute, a "reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege,

307. The Pixel, as configured by Defendant and as described herein, constitutes an "eavesdropping device" as that term is defined in the Illinois Eavesdropping Statute, which provides, in pertinent part, that "[a]n eavesdropping device is any device capable of being used to hear or record oral conversation ***or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means."*** 720 ILCS 5/14-1(e) (emphasis added).

308. Defendant used the Pixel in a surreptitious manner as the use of the Pixel, which is not visible to Users, was ***not*** disclosed in any manner to patients and/or visitors to Defendants' web properties.

309. Defendant installed the Pixel on its Web Properties in order to record and/or to transmit all or parts of Plaintiffs' and the putative Class Members' private conversations to third parties for marketing and analytics purposes.

310. The Illinois Eavesdropping Statute defines "private conversation" as "any oral communication between 2 or more persons, whether in person or transmitted between the parties by wire or other means, when one or more of the parties intended the communication to be of a private nature under circumstances reasonably justifying that expectation. A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution." 720 ILCS 5/14-1(d).

311. The private conversations recorded and transmitted by Defendant to undisclosed third-parties included, but were not necessarily limited to, Plaintiffs' and Class Members'

---

immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution."

communications concerning their patient status and past, present or future medical conditions, including requests for information about specific providers and locations, and information about specific health conditions, treatments, appointments and services.

312. Defendant, who maintained the Web Properties, was a party to those private conversations.

313. Defendant did not have the consent of Plaintiffs nor the putative Class Members to transmit or record all or any part of those private conversations.

314. Plaintiffs and the putative Class Members intended and believed that the information they provided to Defendant via its Web Properties would be kept private, confidential and secure.

315. Indeed, those private conversations contained extremely sensitive and personal health information including, but not necessarily limited to, symptoms, treatments, diagnoses and other protected health information.

316. Defendant did not notify or inform Plaintiffs and the putative Class Members that it was recording and transmitting their private electronic communications to third parties.

317. As a result, Plaintiffs and the putative Class Members are entitled to: (i) "an injunction by the circuit court prohibiting further eavesdropping;"; (ii) "all actual damages against the eavesdropper or his principal or both" and (iii) "any punitive damages which may be awarded by the court or by a jury" *See* 720 ILCS 5/14-6(a), (b) & (c).

COUNT III
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/1, *et seq.*
(*On behalf of Plaintiffs & the Class*)

318. Plaintiffs incorporate and re-allege each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

319. Duly is a "person" as defined by ILCS § 505/1(c).

320. Plaintiffs and the other Class Members are "consumers" as defined by 815 ILCS § 505/1(e).

321. Duly's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 ILCS. § 505/1(f).

322. Duly's unfair acts and practices against Plaintiffs and the other Class Members occurred in the course of trade or commerce in Illinois, arose out of transactions that occurred in Illinois and/or harmed individuals in Illinois.

323. Plaintiffs and Class Members received and paid for health care services from Duly.

324. Plaintiffs and Class Members used Duly's Web Properties, including the Website and the MyChart patient portal, in connection with receiving health care services from Duly.

325. Plaintiffs' and other Class Members' payments to Duly for health care services were for household and personal purposes.

326. Duly's practice of disclosing Plaintiffs' and other Class Members' personally identifiable data and re-directing their communications to third parties without authorization, consent or knowledge is a deceptive, unfair and unlawful trade act or practice in violation of 815 ILCS § 505/2.

327. Duly's unfair business practices were targeted at all Duly patients, including

Plaintiffs and other Class Members.

328. Duly's representations and 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 the Duly web property, including the MyChart patient portal.

329. Duly intended to mislead Plaintiffs and other Class Members and induce them to rely on its misrepresentations and omissions.

330. Duly's surreptitious collection and disclosure of Plaintiffs' and other Class Members' personally identifiable data and communications to third parties involves important consumer protection concerns.

331. The relief requested by Plaintiffs and other Class Members would provide redress for the harms Duly caused not just to Plaintiff but to all other Class Members.

332. Plaintiffs and other Class Members were injured and have suffered damages as a direct and proximate result of Duly's unfair acts and practices.

333. Plaintiffs' and other Class Members' injuries were proximately caused by Duly's unfair and deceptive business practices.

334. Duly's acts caused substantial injury that Plaintiffs and other Class Members could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

335. Duly acted intentionally, knowingly and maliciously to violate Illinois's Consumer Fraud and recklessly disregarded Plaintiffs' and Class Members' rights.

336. As a direct and proximate result of Duly's unfair, unlawful and deceptive acts and practices, Plaintiffs and other Class Members have suffered and will continue to suffer injury,

ascertainable losses of money or property and monetary and non-monetary damages including overpaying for Duly's health care services and loss of value of their personally identifiable patient data and communications.

337. As a direct and proximate result of Duly's unfair, unlawful and deceptive acts and practices, Plaintiffs and other Class Members were also damaged by Duly's conduct in that:

a. Duly harmed Plaintiffs' and other Class Members' interest in privacy;

b. Sensitive and confidential information that Plaintiffs and other Class Members intended to remain private is no more;

c. Duly eroded the essential confidential nature of the provider-patient relationship;

d. Duly took something of value from Plaintiffs and other Class Members and derived benefit therefrom without Plaintiffs' and other Class Members' authorization, informed consent or knowledge and without sharing the benefit of such value.

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

f. Duly's actions diminished the value of Plaintiffs and other Class Members' personal information.

338. Plaintiffs, individually and on behalf of the Illinois Class Members, seek all monetary and non-monetary relief allowed by law.

COUNT IV
VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 ILCS §§ 510/2, *et seq.*
(On behalf of Plaintiffs & the Class)

339. Plaintiffs incorporate and re-allege each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

340. Duly is a "person" as defined by 815 ILCS § 510/1(5).

341. Duly engaged in deceptive trade practices in the conduct of its business, in violation of 815 ILCS § 510/2(a), including: (i) representing that goods or services have characteristics that they do not have; (ii) representing that goods or services are of a particular standard, quality or grade if they are of another; (iii) advertising goods or services with intent not to sell them as advertised and (iv) engaging in other conduct that creates a likelihood of confusion or misunderstanding.

342. Duly's practice of disclosing Plaintiffs' and other 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).

343. Duly's practice of disclosing Plaintiffs' and other Class Members' personally identifiable data and re-directing their communications to third parties without authorization, consent or knowledge was willful and/or intentional.

344. Duly's representations and 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 the Duly web property, including the MyChart patient portal.

345. The above unfair and deceptive practices and acts by Duly were immoral, unethical, oppressive and unscrupulous.

346. These acts caused substantial injury to Plaintiffs and other Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

347. As a direct and proximate result of Duly's unfair, unlawful and deceptive trade practices, Plaintiffs and other Class Members have suffered and will continue to suffer injury,

ascertainable losses of money or property and monetary and non-monetary damages, including overpaying for Duly's health care services and loss of value of their personally identifiable patient data and communications.

348. As a direct and proximate result of Duly's unfair, unlawful and deceptive acts and practices, Plaintiffs and other Class Members were also damaged by Duly's conduct in that:

a. Duly harmed Plaintiffs' and other Class Members' interest in privacy;

b. Sensitive and confidential information that Plaintiffs and other Class Members intended to remain private is no more;

c. Duly eroded the essential confidential nature of the provider-patient relationship;

d. Duly took something of value from Plaintiffs and other Class Members and derived benefit therefrom without Plaintiffs' and other Class Members' authorization, informed consent, or knowledge and without sharing the benefit of such value;

e. Plaintiffs and other Class Members did not get the full value of the medical services for which they paid which included Duly's duty to maintain confidentiality and

f. Duly's actions diminished the value of Plaintiffs and other Class Members' personal information.

349. Plaintiffs and other Class Members are patients of Duly and need access to Duly's Web Properties, including the Website and the MyChart Portal, in connection with receiving health care from Duly.

350. Because Plaintiffs and other Class Members need to and so will continue to use Duly's Web Properties in the future, if Duly's unfair, unlawful and deceptive trade practices are allowed to continue, Plaintiffs and other Class Members are likely to suffer continuing harm in the future.

351. Plaintiffs and other Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT V
BREACH OF CONFIDENCE
(On behalf of Plaintiffs & the Class)

352. Plaintiffs incorporate and re-allege the allegations contained in the foregoing paragraphs as if fully set forth herein.

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

354. Plaintiffs and other Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website and the MyChart Portal, which were further buttressed by Defendant's express promises in its privacy policy.

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

356. These disclosures were made without Plaintiffs' or other Class Members' knowledge, consent or authorization.

357. The third-party recipients included, but were not limited to, Meta.

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

359. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiffs and other

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. Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. General damages for invasion of their rights in an amount to be determined by a jury;

e. Nominal damages for each independent violation;

f. 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 compensation for such data;

g. 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;

h. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information; and

i. Defendant's actions violated the property rights Plaintiffs and Class Members have in their Private Information.

COUNT VI
COMMON LAW INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(*On Behalf of Plaintiffs & the Class*)

360. Plaintiffs incorporate and re-allege the allegations contained in the foregoing paragraphs as if fully set forth herein.

361. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Web Properties and the communication platforms and

services therein.

362. Plaintiffs and Class Members communicated sensitive and protected medical information and individually identifiable information that they intended for only Defendant to receive and that they understood Defendant would keep private.

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

364. Plaintiffs and Class Members had a reasonable expectation of privacy because Defendant's Web Properties Notice of Privacy Practices states that they can expect such privacy.

365. Moreover, Plaintiffs and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendant's disclosure of private medical information coupled with individually identifying information is highly offensive to the reasonable person.

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

367. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

368. Plaintiffs and Class Members seek appropriate relief for these injuries, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as a result of the intrusion(s) upon Plaintiffs' and Class Members' privacy.

369. Plaintiffs and Class Members are also entitled to punitive damages resulting from

the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

370. Plaintiffs seek all other relief as the Court may deem just and proper.

COUNT VII
BREACH OF IMPLIED CONTRACT
(*On Behalf of Plaintiffs & the Class*)

371. Plaintiff re-alleges and incorporates by reference all prior paragraphs as if fully set forth herein.

372. When Plaintiffs and Class Members provided their Private Information 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.

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

374. 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.

375. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information to third parties, including Meta.

376. 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 for these services, had they known their Private Information would be disclosed.

377. Plaintiffs and Class Members are entitled to compensatory and consequential

damages as a result of Defendant's breach of implied contract.

COUNT VIII
NEGLIGENCE
(On Behalf of Plaintiffs & the Class)

378. Plaintiffs re-allege and incorporate by reference all prior paragraphs as if fully set forth herein.

379. Defendant owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, safeguarding, and preventing any disclosure of their Private Information. This duty included but was not limited to: (a) preventing Plaintiffs' and Class Members' Private Information from being to be disclosed to unauthorized third parties; and (b) destroying Plaintiffs' and Class Members' Private Information within an appropriate amount of time after it was no longer required by Defendant.

380. Defendant's duties to use reasonable care arose from several sources, including those described below. Defendant had a common law duty to prevent foreseeable harm to others, including Plaintiffs and Class Members, who were the foreseeable and probable victims of any data misuse, such as disclosure of Private Information to unauthorized parties.

381. Defendant had a special relationship with Plaintiffs and Class Members, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members resulting from unauthorized disclosure of their Private Information to third parties such as Meta. Plaintiffs and Class Members were compelled to entrust Defendant with their Private Information. At relevant times, Plaintiffs and Class Members understood that Defendant would take adequate data storage practices to safely store their Private Information. Only Defendant had the ability to protect Plaintiffs' and Class

Members' Private Information collected and stored on Defendant's websites.

382. Defendant's duty to use reasonable measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of [PHI]." 45 C.F.R. § 164.530(c)(1).

383. Defendant's conduct as described above constituted an unlawful breach of their duty to exercise due care in collecting, storing, and safeguarding Plaintiffs' and the Class Members' Private Information by failing to protect this information.

384. Plaintiffs and the Class Members trusted Defendant and in doing so provided Defendant with their Private Information, based upon Defendant's representations that it would "never share your information unless you give us written permission" and it "must obtain [patient] authorization" to disclose their personally identifiable information for sales or marketing purposes.[91] Defendant failed to do so.

385. Defendant breached its duty in this relationship to collect and safely store Plaintiffs' and Class Members' Private Information.

386. Plaintiffs' and the Class Members' Private Information would have remained private and secure had it not been for Defendant's wrongful and negligent breach of their duties. Defendant's negligence was, at least, a substantial factor in causing Plaintiffs' and Class Members' Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing Plaintiffs and the Class Members other injuries because of the unauthorized disclosures.

387. The damages suffered by Plaintiffs and the Class Members were the direct and

[91] *See* Exhibit A.

reasonably foreseeable result of Defendant's negligent breach of their duties to maintain Users' Private Information. Defendant knew or should have known that their unauthorized disclosure of highly sensitive Private Information was a breach of their duty to collect and safely store such information.

388. Defendant's negligence directly caused significant harm to Plaintiffs and the Class. Specifically, Plaintiffs and Class Members are now subject to their sensitive information being accessed by unauthorized parties, which may lead to significant harms.

389. Defendant had a fiduciary duty to protect the confidentiality of its communications with Plaintiffs and Class Members by virtue of the explicit privacy representations Defendant made on their websites to Plaintiffs and members of the Class.

390. Defendant had information relating to Plaintiffs and Class Members that they knew or should have known to be confidential.

391. Plaintiffs' and Class Members' communications with Defendant about sensitive Private Information and their status as patients of Defendant were not matters of general knowledge.

392. Defendant breached its fiduciary duty of confidentiality by designing their data protection systems in a way to allow for a data breach of a massive caliber.

393. At no time did Plaintiff or Class Members give informed consent to Defendant's conduct.

394. As a direct and proximate cause of Defendant's actions, Plaintiffs and Class Members suffered damage in that the information they intended to remain private is no longer so and their Private Information was disclosed to, tracked, and intercepted by third-party Internet tracking companies, including Meta, without their knowledge or consent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs PATRICIA MAYER, CATHERINE MASSARELLI and MARY MURPHY, on behalf of themselves and all those similarly situated, respectfully pray for judgment in their favor and against MIDWEST PHYSICIAN ADMINISTRATIVE SERVICES, LLC d/b/a DULY HEALTH AND CARE as follows:

- For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and Plaintiffs' counsel as Class Counsel;
- For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and other Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and other Class Members;
- For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage and safety, and to disclose with specificity the type of PII and PHI disclosed to third parties;
- For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- For an award of actual damages, compensatory damages, statutory damages and statutory penalties, in an amount to be determined as allowable by law;
- For an award of punitive damages as allowable by law;
- For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- Pre- and post-judgment interest on any amounts awarded and
- All such other and further relief as this court may deem equitable and just.

DEMAND FOR JURY TRIAL

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

Date: March 1, 2024

Respectfully submitted,

/s/ James B. Zouras

ALMEIDA LAW GROUP LLC
Firm ID 100530
David S. Almeida (ARDC 6285557)
Elena A. Belov
Britany A. Kabakov (ARDC 6336126)
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024 (phone)
david@almeidalawgroup.com
elena@almeidalawgroup.com
britany@almeidalawgroup.com

James B. Zouras
Ryan F. Stephan
Teresa M. Becvar
Michael Casas
STEPHAN ZOURAS, LLP
222 W. Adams St, Suite 2020
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
Firm ID: 43734
jzouras@stephanzouras.com
rstephan@stephanzouras.com
tbecvar@stephanzouras.com
mcasas@stephanzouras.com

Attorneys for Plaintiffs & the Putative Class

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on March 1, 2024, I filed the attached with the Clerk of the Court using the Court's electronic filing system, and will send such filing to all attorneys of record.

/s/ James B. Zouras