

Exhibit A

FILED
4/10/2023 12:31 PM
IRIS Y. MARTINEZ
CIRCUIT CLERK
COOK COUNTY, IL
2023CH03446
Calendar, 9
22218884

CIRCUIT COURT OF COOK COUNTY, ILLINOIS
CHANCERY DIVISION

<p>PATRICIA MAYER, <i>on behalf of herself and all others similarly situated,</i></p> <p>Plaintiff,</p> <p>v.</p> <p>MIDWEST PHYSICIAN ADMINISTRATIVE SERVICES, LLC d/b/a DULY HEALTH AND CARE,</p> <p>Defendant.</p>	<p>Case No. 2023CH03446</p> <p><u>JURY TRIAL DEMANDED</u></p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------

CLASS ACTION COMPLAINT

Plaintiff PATRICIA MAYER (“Plaintiff”) brings this class action lawsuit in her 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 alleges, upon personal knowledge as to her own actions, her counsel’s investigation and upon information and good faith belief as to all other matters, as follows:

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

¹ See <https://www.dulyhealthandcare.com/hipaa-privacy-policy> (last visited March 18, 2023) (emphasis added).

2. As detailed herein, those statements are certainly suspect given Defendant's illegal and widespread practice of disclosing Plaintiff's 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 ("Facebook").

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.

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

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 March 8, 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 March 18, 2023).

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

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

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

10. Plaintiff and Class Members who visited and used (collectively, the “Users”) Defendant’s Web Properties understandably thought they were communicating *only* with their

³ HHS.gov, 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 March 18, 2023).

⁴ <https://mychart.dupagemd.com/MyChart/Authentication/Login?> (last visited March 18, 2023).

trusted healthcare provider.

11. Unbeknownst to Plaintiff and Class Members, however, Defendant had embedded the Facebook Tracking Pixel (the “Pixel” or “Facebook Pixel”) on its Web Properties which automatically transmits to Facebook 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 Plaintiff and Class Members provide to Defendant to be unlawfully disclosed to Facebook 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 feature or text box), among other things.

14. The user’s web browser executes the Pixel via instructions within the webpage to

⁵ Plaintiff’s research shows that the Facebook Pixel is currently embedded in Defendant’s Website (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 Facebook Pixel as well.

⁶ The Pixel forces the website user to share the FID for easy tracking via the “cookie” Facebook stores every time someone accesses their Facebook account from the same web browser. “Cookies are small files of information that a web server generates and sends to a web browser”; “[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 March 18, 2023).

⁷ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited March 8, 2023).

communicate certain information based on parameters selected by the website's owner. The Facebook 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 Facebook.

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

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

17. Unlike the Facebook 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 Facebook. 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 Facebook from the website owner's servers.^{9,10}

18. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and

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 March 18, 2023).

⁹ <https://revealbot.com/blog/facebook-conversions-api/> (last visited March 18, 2023).

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 March 18, 2023).

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 Facebook directly.

20. 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.

21. The Facebook 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. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical conditions and other Private Information disclosed to Defendant.

22. The information that Defendant's Tracking Pixel and CAPI sent to Facebook included the Private Information that Plaintiff and Class Members submitted to Defendant's Website, including, for example, patient status, the type of medical treatment sought, the individual's particular health condition and the fact that the individual attempted to or did book a medical appointment.

¹¹ <https://www.facebook.com/business/help/2041148702652965?id=818859032317965> (last visited March 18, 2023).

¹² See <https://www.dulyhealthandcare.com/hipaa-privacy-policy> (last visited March 18, 2023).

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

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

25. 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 Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue – without the patients' informed and express consent.

26. Neither Plaintiff nor any other Class Member were provided, much less signed, a written authorization permitting Defendant to disclose their Private Information to Facebook.

27. Despite willfully and intentionally incorporating the Facebook Pixel and CAPI into its Website and servers, Defendant has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook.¹³

¹³ In contrast to Defendant, in recent months several medical providers which have installed the Facebook 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*, available at https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited March 28, 2023); *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022), available at <https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3> (last visited March 28, 2023); *Novant Health notifies patients of potential data privacy incident* (Aug. 12, 2022), available at <https://www.novanthealth.org/home/about-us/newsroom/press->

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

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

30. The disclosure of Plaintiff's 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.

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

32. 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

[releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident.aspx](https://www.hhs.gov/oc/foia/releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident.aspx) ((last visited March 28, 2023)).

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

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

34. Duly breached its statutory and common law obligations to Plaintiff and Class Members by, *inter alia*: (i) failing to adequately review its marketing programs and web based 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 Plaintiff and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Facebook Pixels; (v) failing to warn Plaintiff 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.

35. As a result, Plaintiff and Class Members have suffered numerous injuries,

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 March 8, 2023) (emphasis added).

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.

36. Plaintiff therefore seeks, on behalf of herself 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 Illinois Eavesdropping Statute, 720 ILCS 5/14-1, *et seq.*; (ii) violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* (“ICFA”); (iii) violations of the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS §§ 510/2, *et seq.* (“IUDTPA”); (iv) breach of confidence; (v) invasion of privacy; (vi) common law invasion of privacy – intrusion upon seclusion and (vi) breach of implied contract.

PARTIES

37. Plaintiff Patricia Mayer is a natural person and citizen of Illinois, residing in Arlington Heights, Illinois, where she intends to remain.

38. 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

39. 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

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

¹⁶ <https://www.dulyhealthandcare.com/> (last visited March 18, 2023).

40. This Court has personal jurisdiction over Defendant because its principal place of business is in this judicial district and a substantial portion of the acts and omissions giving rise to the claims asserted herein occurred in and emanated from this judicial district.

41. Venue is proper under 750 ILCS 5/104 because Defendant's principal place of business is in Downers Grove, Illinois, which is in this judicial district.

COMMON FACTUAL ALLEGATIONS

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

42. 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.

43. 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.*, Facebook 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.

44. 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.

45. That data is linked to a specific internet protocol (“IP”) address. The Meta Pixel, for example, sends information to Facebook 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.

46. 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.

47. 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.

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

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 March 18, 2023).

B. Duly Utilized Tracking Technology for the Purpose of Disclosing Plaintiff's and Class Members' Private Information to Facebook.

49. 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 Facebook, including communications that contain Plaintiff's and Class Members' Private Information.

50. On numerous occasions, with the most recent being in February 2023, Plaintiff Mayer accessed Defendant's Website and Portal on her mobile device and computer 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.

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

52. Further to the systematic process described herein, Duly assisted Facebook with intercepting Plaintiff's communications including those that contained personally identifiable information, protected health information and related confidential information.

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

54. Defendant uses the Website to connect Plaintiff and Class Members to Defendant's digital healthcare Properties with the goal of increasing profitability.

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

C. Facebook's Business Tools & the Pixel

56. Facebook operates the world's largest social media company and generated \$117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.¹⁸

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

58. Facebook'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.

59. 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

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

¹⁸ FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited March 18, 2023).

¹⁹ FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142> (last visited March 28, 2023); *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 March 18, 2023).

²⁰ FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; *see also* FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/>

61. One such Business Tool is the Pixel which “tracks the people and type of actions they take.”²¹

62. 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 Facebook’s servers—traveling from the user’s browser to Facebook’s server.

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

64. Similarly, Plaintiff’s and Class Members’ Private Information would not have been disclosed to Facebook via CAPI but for Defendant’s decision to install and implement that tool.

65. By installing and implementing both tools, Defendant caused Plaintiff’s and Class Members’ communications to be intercepted and transmitted to Facebook via the Pixel, and it caused a second improper disclosure of that information via CAPI.

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

D. Defendant’s method of transmitting Plaintiff’s 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)

67. 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

(last visited March 18, 2023).

²¹ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited March 28, 2023).

(e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

68. 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.

69. 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.²²

63. 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).

²² One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

64. Every website consists of Markup and “Source Code.”

65. 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.

66. 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.

67. 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.

68. 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 Facebook.

69. Third parties, like Facebook, 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.

70. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that cannot be evaded by savvy users.

71. Facebook’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].”

72. Thus, the communications between patients and Defendant, which are necessary to use Defendant’s Website, are actually received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook.

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

74. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct 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.”²³

75. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user’s communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (i.e., to bolster profits).

76. 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

²³ See <https://www.facebook.com/business/help/308855623839366?id=818859032317965> (last visited March 18, 2023).

device to contemporaneously and invisibly redirect the Users' communications to third parties.

77. In this case, Defendant employed the Tracking Pixel and CAPI to intercept, duplicate and re-direct Plaintiff's and Class Members' Private Information to Facebook.

78. For 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.

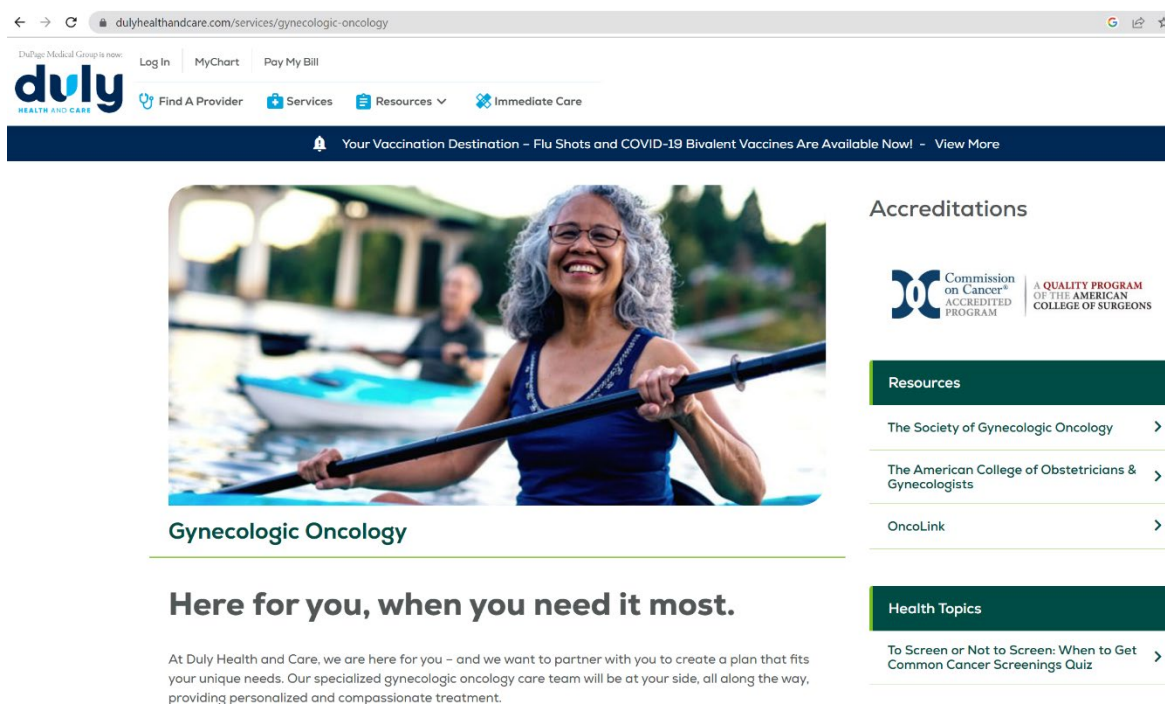


Figure 1. Image taken from <https://www.dulyhealthandcare.org/gynecologic-oncology/>

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

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

▼ Request Headers

```

:authority: www.facebook.com
:method: GET
:path: /tr/?id=486716330266417&ev=PageView&dl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fservices%2Fgynecologic-oncology%3Frl=&if=false&ts=1678677876451&sw=1664&sh=1110&v=2.9.98&r=stable&ec=0&o=30&cs_est=true&fbp=fb.1.1678147503296.14170958&it=1678677876385&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
cookie: sb=ViICZCGTcjdC7v_ZtK5iZyWa; datr=WCICZAI-BhJl4L8rjTo_BPP8; c_user=5 ; xs=56%3A4p0nMzdkaaHr2w%3A2%3A1677861466%3A-1%3A3037%3A%3AAcWmrsV2BCfEmMoq9ZVRGKCBFvXaUSQVksLq8R1VfBo; fr=0kd8Yi8NRIRkz3mve.AWUJbydmlcXaICX-nLzNnLWjjT0.BkDfMo.gk.AAA.0.0.BkDfMo.AwV9aXL3qLI
referer: https://www.dulyhealthandcare.com/

```

Figure 2. An HTTP single communication session sent from the device to Facebook that reveals the user's search results and the patient's FID (c_user field).²⁴

81. 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,²⁵ effectively open a spying window through which the webpage can funnel the visitor's data, actions, and communications to third parties.

82. 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 Facebook.

83. 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.

84. 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.

²⁴ The user's Facebook ID is represented as the c_user ID highlight in the image above, and Plaintiff has redacted the corresponding string of numbers to preserve the user's anonymity.

²⁵ 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.

85. The information that Defendant's Pixel sends to Facebook may include, among other things, patients' PII, PHI and other confidential information.

86. Consequently, when Plaintiff and Class Members visit Defendant's website and communicate their Private Information, it is transmitted to Facebook, 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.

E. Defendant's Pixel and/or CAPI Tracking Practices caused Plaintiff's & Class Members' PII & PHI to be sent to Facebook.

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

86. 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.

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

88. However, Defendant's Website does not rely on the Pixel in order to function.

89. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

90. Defendant did not disclose to Plaintiff and Class Members that their Private Information would be shared with Facebook as it was communicated to Defendant.

91. Plaintiff and Class Members never consented, agreed, authorized or otherwise

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

92. Defendant's Pixel and CAPI sent non-public Private Information to Facebook, including but not limited to Plaintiff's 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.

93. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside Plaintiff's 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.²⁶

94. 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.

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

²⁶ Defendant's Website tracks and transmits 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 Plaintiff's and other online patients' confidential communications and Private Information; (ii) disclosed patients' protected information to Facebook—an unauthorized third-party and (iii) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

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

96. 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.

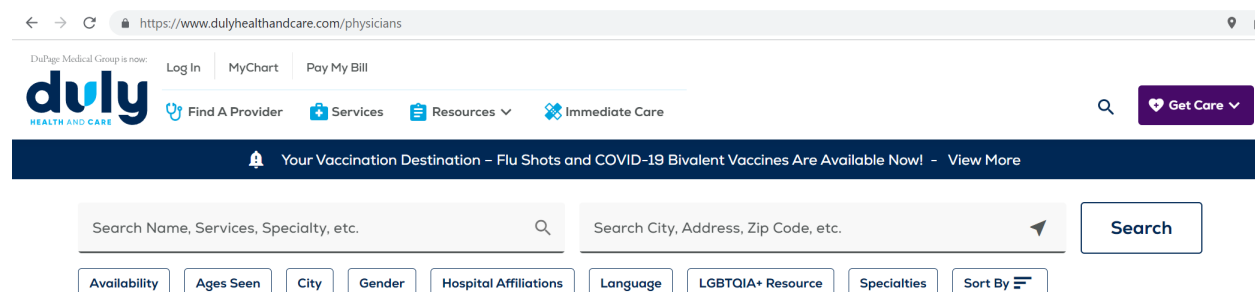


Figure 3. Defendant directs patients to its “Find a Provider” webpage with embedded Pixels – which are invisible to the regular user.

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

98. 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 Facebook Pixel. Similarly, if a patient uses the Website’s general search bar or chat, the terms and phrases the patient types are transmitted to Facebook, even if they contain a patient’s treatment, procedures, medical conditions, and related queries.

99. This information is automatically sent from the patient’s device to Facebook, and

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

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

101. 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.

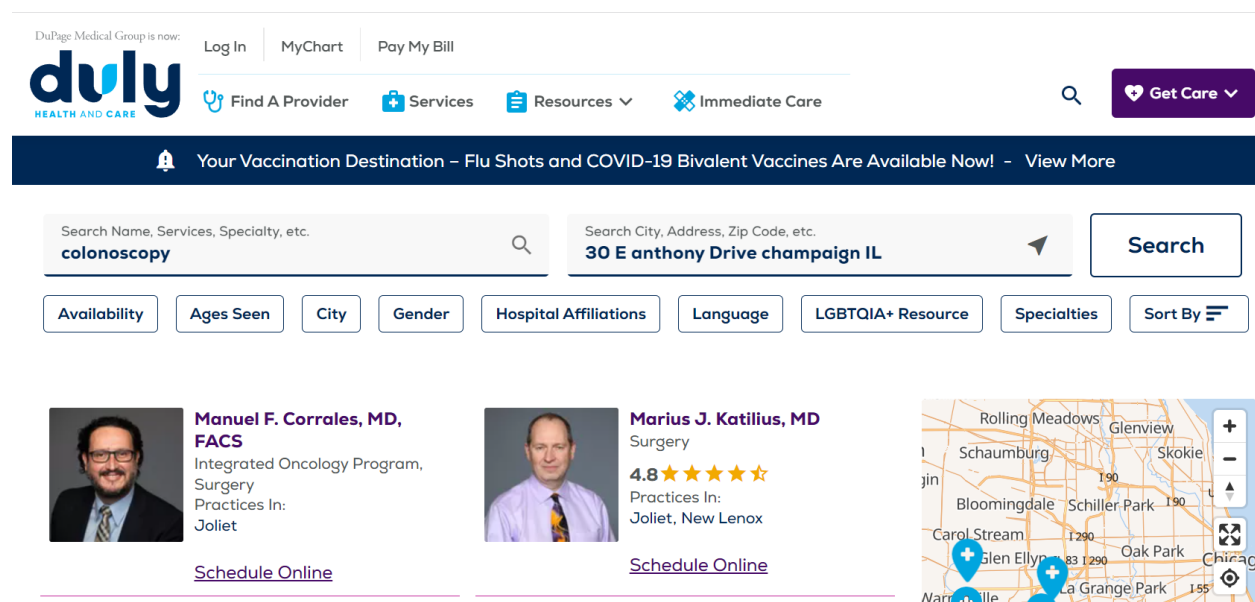


Figure 4. Search results for a provider specializing in “colonoscopy” near “30 E Anthony Drive Champaign IL” as they appear to the user on Defendant’s Find a Provider Search results webpage.

102. 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 Facebook along with the user’s unique Facebook ID, as evidenced by the images below.

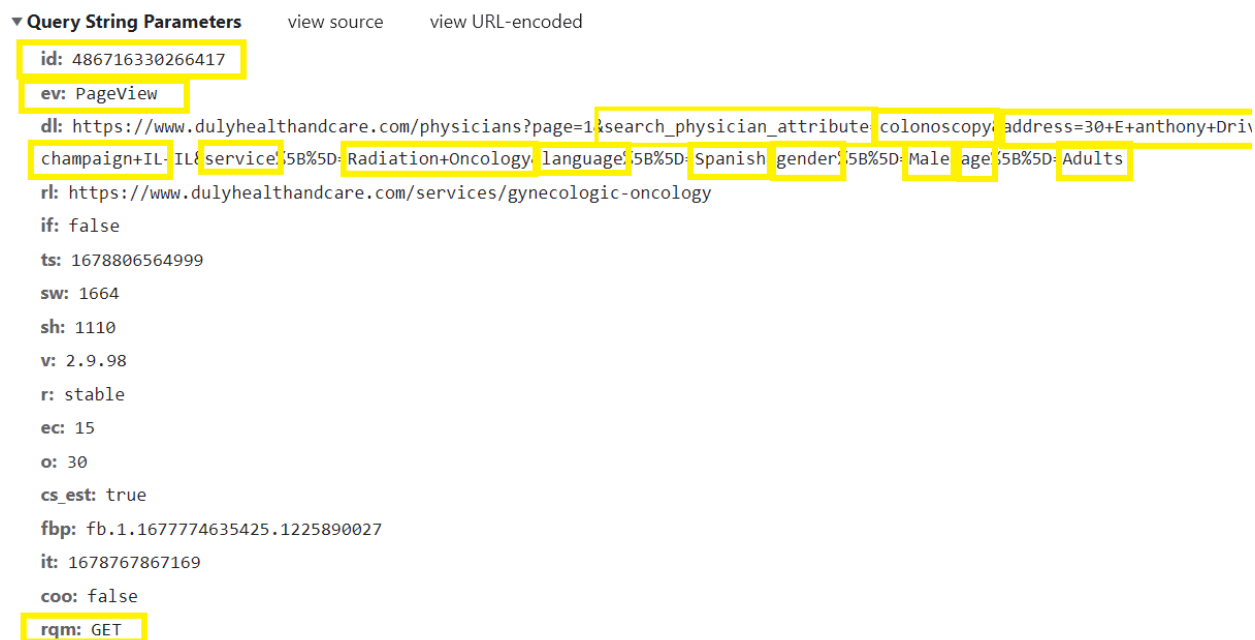


Figure 5. Defendant’s transmission to Facebook of patient’s search parameters showing search terms (“colonoscopy” and “30 E Anthony Drive Champaign IL”) and filters used (“Male” provider who speaks “Spanish,” specializes in “Radiation Oncology” and services “Adults”).

103. 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.

104. 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.

105. 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.

106. 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.²⁷

▼ Request Headers

```
:authority: www.facebook.com
:method: GET
:path: /tr/?id=486716330266417&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%3Fpage%
3D1%25search_physician_attribute%3Fcolonoscopy%2Faddress%3B%3B%2F%2Fanthony%2BDrive%2Fchampaign%2F%2BIL%2Fservice%25
5B%255D%3FRadiation%2BOnco%2Flanguage%255B%255D%3FSpanish%2Fgender%255B%255D%3FMale%2Fage%255B%255D%3FAdults&url=ht
tps%3A%2F%2Fwww.dulyhealthandcare.com%2Fservices%2Fgynecologic-oncology&if=false&ts=1678806612362&cd[buttonFeatures]=%
7B%22classList%22%3A%22dmgButton%20secondary%20filter-btn-mobile%22%2C%22destination%22%3A%22%22%2C%22id%22%3A%22%22%
2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Filters%22%2C%22numChildButtons%22%3A%22%22%2C%22tag%22%3A%22button%22%2C%
22type%22%3A%22%22%2C%22name%22%3A%22%22%2C%22value%22%3A%22%22%2C%22cd[buttonText]=Filters&cd[formFeatures]=%5B%5D&cd[pag
eFeatures]=%7B%22title%22%3A%22Find%20a%20Primary%20Care%20or%20Specialty%20Doctor%20%7C%20Duly%20Health%20and%20Care%
20-%20DuPage%20Medical%20Group%22%7D&sw=1664&sh=1110&v=2.9.98&r=stable&ec=17&o=30&cs_est=true&fbp=fb.1.1677774635425.1
225890027&it=1678767867169&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=QtI1Y1lVd2UW0uuBmn2Mb8vC; sb=GrxtY1jj9lKwnpCg7UAhiJMv; c_user=5. , dpr=1.5; xs=7%3A_7bqKp6s0g6FyQ%3A
2%3A1677887050%3A-1%3A3037%3A%3AAcuJUPuF7a0Pg1uFoZkdEJA2-sXIcPnXEqtqwb7C0M; fr=0n0nya2GPw4JH1CM3.AwVLt8cYVqieGwqfTwTn
pCS0g0k.BkD9C8.-f.AAA.0.0.BkD9jB.AWU3d_krcxo; usida=eyJ2ZXIiOiJEsIm1kiJoiQXJyaG8yMTFocXNlZ3U1LCJ0aW11IjoxNjc4NzYwNzEzEz
Q%3D%3D
:referer: https://www.dulyhealthandcare.com/
```

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

107. 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.

108. Once a patient chooses a doctor, all of the information that patient has submitted is automatically sent directly to Facebook. The information transmitted to Facebook 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

²⁷ 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.

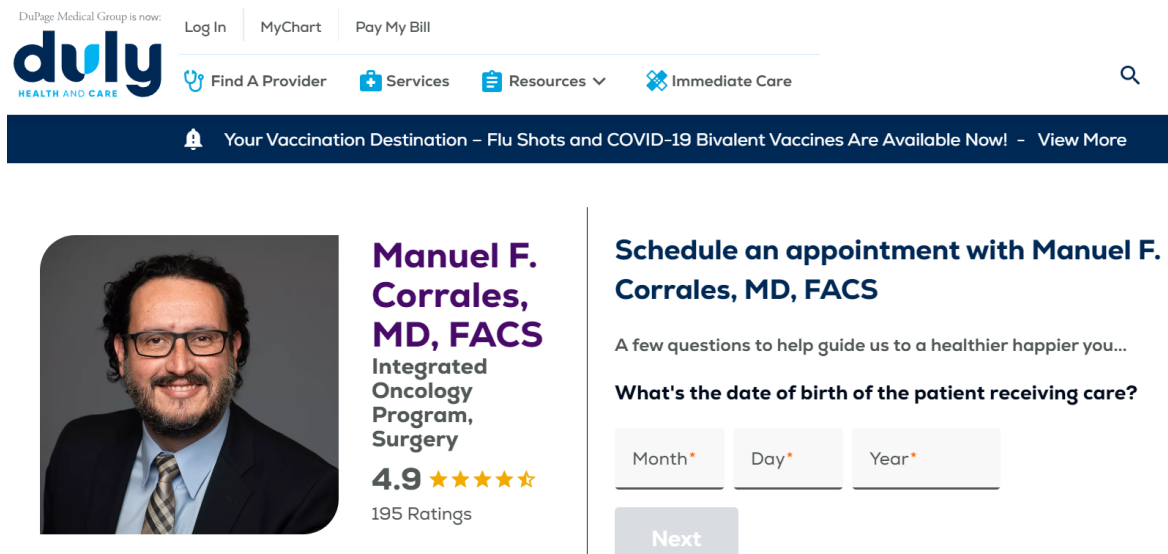
search parameters (demonstrating they specifically searched for a male doctor who speaks Spanish and treats adult patients, and their specialty) and (iv) the patient's location filter.

▼ Request Headers

```
:authority: www.facebook.com
:method: GET
:path: /tr/?id=486716330266417&ev=PageView&dl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%2Fmanuel-f-corrales-md-facs&rl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%3Fpage%3D1%26search_physician_attribute%3Acolonoscopy%26address%3A%30%2BE%2Banthony%2BDrive%2Bchampaign%2BIL%26BIL%26language%255B%255D%3ASpanish%26gender%255B%255D%3AMale%26age%255B%255D%3AAdults&if=false&ts=1678825890538&sw=1664&sh=1110&v=2.9.98&r=stable&ec=0&o=30&cs_est=true&fbp=fb.1.1677774635425.1225890027&it=1678825890406&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=QtI1Y1lVd2U0Uu8mn2Mb8vC; sb=GrxTY1j9lKwPcg7UAhiJMV; c_user=5; dpr=1.5; usida=eyJ2ZXIiOiJEsImkIjoiQXJyaG8yMTFocXNlZ3UiLCJ0aW1lIjoxNjc4NzYwNzEzZDQ3D%3D; xs=%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AAcVddgJMpRq79qEYUz7R4ajfU2rdran5L587wTJVqc; fr=0pyQTLs0lX68y5snn.AWU4YHXCuAMCpRNhJznkPTX90eY.BkEkoB.-f.AAA.0.0.BkEkoB.AWxpsCnX30c
:referer: https://www.dulyhealthandcare.com/
```

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

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



DuPage Medical Group is now: **duly** HEALTH AND CARE

Log In MyChart Pay My Bill

Find A Provider Services Resources Immediate Care

Your Vaccination Destination - Flu Shots and COVID-19 Bivalent Vaccines Are Available Now! - View More

Manuel F. Corrales, MD, FACS
Integrated Oncology Program, Surgery
4.9 ★★★★★
195 Ratings

Schedule an appointment with Manuel F. Corrales, MD, FACS

A few questions to help guide us to a healthier happier you...

What's the date of birth of the patient receiving care?

Month Day Year

Next

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

button:

▼ Query String Parameters view source view URL-encoded

```

id: 486716330266417
ev: SubscribedButtonClick
dl: https://www.dulyhealthandcare.com/physicians/manuel-f-corrales-md-facs
rl:
if: false
ts: 1678828216631
cd[buttonFeatures]: {"classList":"","destination":"","id":"","imageUrl":"","innerTex
t": "3:15 PM","numChildButtons":0,"tag":"button","type":null,"name":"","value":""}
cd[buttonText]: 0:0 PM
cd[formFeatures]: []
cd[pageFeatures]: {"title":"Manuel F. Corrales, MD, FACS | Duly Health and Care - DuPage
Medical Group"}
sw: 1664
sh: 1110
v: 2.9.98
r: stable
ec: 3
o: 30
cs_est: true
fbp: fb.1.1677774635425.1225890027
it: 1678828167711
coo: false
es: automatic
tm: 3
exp: b3
rqm: GET

```

X Headers Payload Preview Response Initiator Timing Cookies

▼ Query String Parameters view source view URL-encoded

```

id: 486716330266417
ev: SubscribedButtonClick
dl: https://www.dulyhealthandcare.com/physicians/manuel-f-corrales-md-facs
rl:
if: false
ts: 1678828360217
cd[buttonFeatures]: {"classList":"dmgButton primary1","destination":"","id":"","imageUrl":"","innerText":"Continue
to Patient Info","numChildButtons":0,"tag":"button","type":null,"name":"","value":""}
cd[buttonText]: Continue to Patient Info
cd[formFeatures]: []
cd[pageFeatures]: {"title":"Manuel F. Corrales, MD, FACS | Duly Health and Care - DuPage Medical Group"}
sw: 1664
sh: 1110
v: 2.9.98
r: stable
ec: 4
o: 30
cs_est: true
fbp: fb.1.1677774635425.1225890027
it: 1678828167711
coo: false
es: automatic
tm: 3
exp: b3
rqm: GET

```

Figures 10 & 11. HTTP communication sessions sent by the Pixel to Facebook that reveal the

“inner text” of the buttons patient clicked in the process of making an appointment.

113. When the user proceeds to the Patient Information form, Defendant’s Pixel communicates and shares this information with Facebook as well.

▼ Request Headers

```
:authority: www.facebook.com
:method: GET
:path: /tr/?id=486716330266417&ev=Microdata&dl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fschedule%2Fbook&rl=
https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%2Fmanuel-f-corrales-md-facs&if=false&ts=1678830326664&
cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Patient%20Information%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=1&o=30&fbp=fb.1.1677774635425.1225890027&it=1678830324935&coo=false&es=automat
ic&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=QtI1Y1lVd2UW0uuBmn2Mb8vC; sb=GrxtY1jj9lKwnpCg7UAhiJMv; c_user=5; dpr=1.5; usida=eyJ2ZXI
iojEsImlkIjojQXJyaG8yMTFocXNlZ3UiLCJ0aW1lIjojXjc4NzYwNzEzfQ%3D%3D; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3
A-1%3A3037%3A3AAcV7JjHXsLHCcRciOYtWK0txoPr6F4ltNzzvzpJCTiA; fr=0yIH3VuDHxaXUDL0r.AWU89wEnKjpn-E1Fgn2j_J_GM
1k.BkEOo2.-f.AAA.0.0.BkEOo2.AWW9bWS7KhM
:referer: https://www.dulyhealthandcare.com/
```

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

114. If, after following these steps, a patient clicks on the “Schedule an Appointment” button, Defendant communicates and shares this action with Facebook via at least three “events,” classified by Facebook 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=QtI1Y1lVd2UW0uuBmn2Mb8vC; sb=GrxtY1jj9lKwnpCg7UAhiJMv; c_user=54; dpr=1.5; usida=eyJ2ZXI0jEsImlkIjoiQXJyaG8yMTFocXNlZ3UiLCJ0aW11IjoxNjc4NzYwNzEzfQ%3D%3D; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AACV7JjHXsLHCcRciOYtWK0txoPr6F4ltNzzvzpJCTiA; 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=QtI1Y1lVd2UW0uuBmn2Mb8vC; sb=GrxtY1jj9lKwnpCg7UAhiJMv; c_user=5; dpr=1.5; usida=eyJ2ZXI0jEsImlkIjoiQXJyaG8yMTFocXNlZ3UiLCJ0aW11IjoxNjc4NzYwNzEzfQ%3D%3D; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AACV7JjHXsLHCcRciOYtWK0txoPr6F4ltNzzvzpJCTiA; 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=Schedule&dl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fschedule%2Fbook%2Fshare&rl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fschedule%2Fbook&if=false&ts=1678831529935&sw=1664&sh=1110&v=2.9.98&r=stable&ec=1&o=30&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=QtI1Y1lVd2UW0uuBmn2Mb8vC; sb=GrxtY1jj9lKwnpCg7UAhiJMv; c_user=5; dpr=1.5; usida=eyJ2ZXIiOiJEsImlkIjojIjY1lVd2UW0uuBmn2Mb8vC; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AAcV7JjHxSLHccRciOYtWK0txoPr6F4ltNzzvzpJCTia; 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 Facebook, 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 Facebook (including the phone number being called) as a “SubscribedButtonClick” event.

▼ Request Headers

```

:authority: www.facebook.com
:method: GET
:path: /tr/?id=486716330266417&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%2Falan-h-wang-md&url=
https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%3Fpage%3D1%26per-page%3D10%26search_physician_attribute%3DERCP%252Papillotom
y%26address%3F61820%26I&if=false&ts=1677783789256&cd[buttonFeatures]=%7B%22classList%22%3A%22%26phone-number%22%2C%22destination%22%3
A%22%26tel%3A%221-630-717-2600%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22(630)%20717-2600%22%2C%22numChi
ldButtons%22%3A%22%26tag%22%3A%22a%22%2C%22type%22%3Anull%22%2C%22name%22%3A%22%22%2C%22buttonText%22%3A%22(0)%200-0&cd[formFeatures]=%5B%5
D&cd[pageFeatures]=%7B%22title%22%3A%22Alan%20H.%20Wang%2C%20MD%20%7C%20Duly%20Health%20and%20Care%20-%20DuPage%20Medical%20Group%2
2%7D&sw=1664&sh=1110&v=2.9.97&r=stable&ec=2&o=30&cs_est=true&fbp=fb.1.1677774635425.1225890027&it=1677783668168&coo=false&es=automa
tic&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: c_user=5 ; datr=QtI1Y1lVd2UW0uuBmn2Mb8vC; dpr=1.5; usida=eyJ2ZXIiOiJEsImkIjoIjQXJxdDZlYzE2Y2Ywc2MXQilCJ0aw1lIjoxNjc3NjE4
NjYwFQ%3D%3D; xs=188%3AWgt7jckaf4RNPg%3A2%3A1597289338%3A-1%3A3037%3A%3AAcXlPGjI0JJMBDF4rEpNLYEtI8qYvPKmkyCFEVFNdu; fr=02l3w3T2bxc
F8YgcE.AwVPxsThK9OKrSZmYf8Hm4VaNg.BkAMwM.-f.AAA.0.0.BkAMwM.AWxK8HdI1cc
:referrer: https://www.dulyhealthandcare.com/

```

Figure 16. The information automatically sent to Facebook 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 Facebook 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 Facebook as well:

and associated with their individual Facebook account.

The screenshot shows the Duly Health and Care website. The search bar contains the text "301 N Washington St, Naperville, IL 60540". The search results show a list of physicians, with one highlighted. The browser's developer tools are open, showing the Network tab with a list of requests. The selected request is a GET request to the Facebook API, with the query string parameters visible. The parameters include the user ID (c_user=5) and the search results.

Request Headers

```
:authority: www.facebook.com
:method: GET
:path: /tr/?id=486716330266417&ev=PageView&il=https%3A%2F%2Fwww.dulyhealthandcare.com%2Fphysicians%3Fpage%3D1%2Fsearch_physician_attribute%3D1%2Fhave%2Fdementia%2Faddress%3D301%2FN%2FWashington%2FSt%252C%2FNaperville%252C%2FIL%260540%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=QtI1Y1lVd2UW0uuBmn2Mb8vC; sb=Grxty1jj9lKwnpCg7UAhiJmV; c_user=5; dpr=1.5; usida=eYJ2ZXIiOiJesImkIjojQXJybXdrMTE3djmxdmoilCJ0aw1lIjoxNjc5MDA1MDA5fQ%3D%3D; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AAcXs_TRdB-zSabqgEaL5BTftqq4BwKrrjoeZILjz63Nk; 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 Facebook.

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 website while logged into Facebook will transmit the c_user cookie to Facebook, which contains that user's unencrypted Facebook ID.

114. When accessing dullyhealthandcare.com, for example, Facebook 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...	1
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, Facebook compels the visitor's browser to send a smaller set of cookies²⁸:

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.²⁹ Facebook, at a minimum, uses the fr cookie to identify users.³⁰

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

²⁸ 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.

²⁹ 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 March 18, 2023).

³⁰ *Cookies & other storage technologies*, FACEBOOK.COM, <https://www.facebook.com/policy/cookies/> (last visited March 18, 2023).

as a first-party cookie, and which Facebook uses to identify a browser and a user:³¹

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.³² 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.³³ If that happens, the time resets, and another 90 days begins to accrue.

120. The Facebook 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.³⁴

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., Facebook.³⁵

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.

³¹ *Id.*

³² *Id.*

³³ *Cookies & other storage technologies*, FACEBOOK.COM, <https://www.facebook.com/policy/cookies/> (last visited March 18, 2023).

³⁴ *First-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/first-party-cookie> (last visited March 18, 2023). This is confirmable by using developer tools to inspect a website's cookies and track network activity.

³⁵ *Third-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/third-party-cookie> (last visited March 18, 2023). This is also confirmable by tracking network activity.

123. Facebook, 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. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to disclose her personally identifiable information and protected health information nor did she authorize any assistance with intercepting her communications.

126. Plaintiff was never provided with any written notice that Defendant disclosed its Website users' PHI nor was she provided any means of opting out of such disclosures.

127. Despite this, Defendant knowingly and intentionally disclosed Plaintiff's PHI to Facebook.

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>m=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%25search_physician_attribute%3DI%2Bhave%2Bdementia%20address%3D%301%2BN%20Washington%20St%252C%20Naperville%252C%20IL%2060540%20IL&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_U1AEZrWr900ybmUwevqYyIU-3Gxm2QkzEKadVFxR8ML63sON1MYL6CQ.; __Secure-3PAPISID=i3IluFlqWdaz-ur/AMwmJ7ifeUDk6wpwO; NID=511=Slj7MEpsxA9YskZ6y6he94iasDKcmbpyLDOFwZZWuB-S0zm01PmafXLUkXy6p2cBhgYxFpLDtLMhXCLobT1vOWr2an0T0

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, Plaintiff is entitled to privacy in her protected health information and confidential communications.

131. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (i)

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

132. Plaintiff did not discover that Defendant disclosed her personally identifiable information and protected health information to Facebook and assisted Facebook with intercepting its communications until March 2023.

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.³⁶

134. On a web page titled HIPAA Privacy Practices & Forms, Duly sets forth its Notice

³⁶ See <https://www.dulyhealthandcare.com/privacy-policy> (last visited March 18, 2023).

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.³⁷

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.³⁸

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).

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,

³⁷ <https://www.dulyhealthandcare.com/hipaa-privacy-policy> (last visited March 18, 2023).

³⁸ On information and belief, the current version of the Notice (as of January 2023) is attached as **Exhibit A** hereto.

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 Plaintiff’s 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.³⁹

136. Defendant violated their own HIPAA Notice by unlawfully intercepting and disclosing Plaintiff’s and Class Members’ Private Information to Facebook 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.

³⁹ See Ex. A (emphasis added).

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").⁴⁰

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.***⁴¹

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

⁴⁰ HHS.gov, 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 March 18, 2023).

⁴¹ *Id.* (Emphasis added).

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.***⁴²

142. Plaintiff and Class Members face just the risks about which the government expresses concern. Defendant has passed along Plaintiff's 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.***⁴³

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

⁴² *Id.* (emphasis added).

⁴³ *Id.* (emphasis added).

*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.*⁴⁴

145. 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 Plaintiff's and Class Members' rights.

I. Defendant's Violation of HIPAA

146. Defendant's disclosure of Plaintiff's and Class Members' Private Information to entities like Facebook also violated HIPAA, which provided Plaintiff 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.

147. 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.

148. HIPAA prohibits health care providers from "us[ing] or disclos[ing] 'protected

⁴⁴ *Id.* (emphasis added).

health information' except as permitted or required by" the HIPAA Privacy Rule. 45 C.F.R. § 164.502.

149. "A covered entity may determine that health information is not individually identifiable health information only if" either "a person with appropriate knowledge of and experience with generally accepted statistical and scientific methods for rendering information not individually identifiable: a) applying such principles" determines that the risk is "very small" that the information could be used alone, or in combination with other information, to identify individuals, and documents the methods that justifies such a determination, or identifiers are removed that include: Internet Protocol (IP) address numbers; account numbers; URLs, device identifiers, and "any other unique identifying number, characteristic or code," except codes assigned by the healthcare organization to allow itself to reidentify information from which it has removed identifying information.

150. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be Protected Health Information.

151. The Department of Health and Human Services 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:

If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.⁴⁵

⁴⁵ HHS.gov, 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/forprofessionals/privacy/special-topics/de-identification/index.html> (last visited March 18, 2023).

152. Consistent with this restriction, the HHS has issued marketing guidance that provides that: “[w]ith 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 to third parties without obtaining authorization from each person on the list.”⁴⁶

153. Here, Defendant provided PHI to third parties in violation of this rule.

154. Commenting on a June 2022 report discussing the use of the Meta Pixel 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.”⁴⁷

155. Defendant’s placing of the third-party tracking code on its Web Properties is a violation of Plaintiff’s and Class Members’ privacy rights under federal law. While Plaintiff does not bring a claim under HIPAA itself, this violation evidences Defendant’s wrongdoing as relevant to other claims.

⁴⁶ HHS.gov, MARKETING, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html> (last visited March 18, 2023).

⁴⁷ HHS.gov, Advisory Board, 'DEEPLY TROUBLED': SECURITY EXPERTS WORRY ABOUT FACEBOOK TRACKERS ON HOSPITAL SITES, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html> (last visited March 18, 2023).

J. Plaintiff's & Class Members' Private Information Has Financial Value.

156. Plaintiff's and Class Members' Private has financial and economic value.

157. Indeed, 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.

158. Data harvesting is the fastest growing industry in the nation.

159. 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.

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

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

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

163. Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user.

164. In 2022, that value is expected to be \$200 billion industry wide, or \$434 per user, also a conservative estimate.

165. 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-to-detailed-medical-records-11579516200?mod=hp_list_pos3) are

becoming commonplace).⁴⁸

166. 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 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.⁴⁹

167. 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

⁴⁸ 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 March 18, 2023).

⁴⁹ 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 March 18, 2023).

in the patient's best interest.

* * *

168. 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 happen as tech companies continue to march into the medical sector.⁵⁰

169. 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.⁵¹

170. Duly gave away Plaintiff’s and Class Members’ communications and transactions on its Website without permission.

171. The unauthorized access to Plaintiff’s and Class Members’ Private Information has diminished the value of that information, resulting in harm.

⁵⁰ *Id.*

⁵¹ Time, HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY, <https://time.com/4588104/medical-data-industry/> (last visited March 18, 2023).

K. Defendant Violated Industry Standards

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

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

174. 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)[.]

175. 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.

176. 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.⁵²

⁵² <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf> (last visited March 20, 2023).

L. Plaintiff's & Class Members' Expectation of Privacy

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

178. Indeed, at all times when Plaintiff 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.

M. IP Addresses are Personally Identifiable Information

179. 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 Facebook through the use of the Pixel.

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

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

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

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

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

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

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

187. 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).

188. 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).

189. Consequently, Defendant’s disclosure of patients’ IP addresses violated HIPAA and industry privacy standards.

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

190. The sole purpose of the use of the Facebook Pixel on Defendant’s Web Properties was marketing and profits.

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

192. Upon information and belief, Defendant was advertising its services on Facebook, and the Pixel was used to “help [Defendant] understand the success of [its] advertisement efforts on Facebook.”

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

194. Upon information and belief, Defendant re-targeted patients and potential patients to get more patients to use its services. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

REPRESENTATIVE PLAINTIFF PATRICIA MAYER'S EXPERIENCES

195. 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.

196. 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.

197. Plaintiff Mayer researched providers, specific health conditions and treatments, looked for Defendant's locations close to her address, and scheduled doctor's appointments for herself via the Defendant's Website and Portal.

198. Plaintiff Mayer also utilized Defendant's Portal to refill prescriptions, look at her bills and payments and to see her test results.

199. 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.

200. 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.

201. 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.

202. As described herein, Defendant worked along with Facebook to intercept Plaintiff Mayer's communications, including those that contained her Private Information.

203. Defendant willfully facilitated these interceptions without Plaintiff Mayer's knowledge, consent or express written authorization.

204. Defendant transmitted to Facebook Plaintiff Mayer's Facebook ID, computer IP address and information such as appointment type, physician selected, button/menu selections

and/or content typed into free text boxes.

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

206. Defendant did not inform Plaintiff Mayer that it had shared her Private Information with Facebook.

207. Plaintiff Mayer is diagnosed with a specific medical condition and submitted information to Defendant's Website and Portal about scheduling medical appointments for her condition.

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

209. 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.

TOLLING

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

CLASS ACTION ALLEGATIONS

211. Plaintiff Mayer brings this action on behalf of herself and on behalf of all other persons similarly situated (the "Class") pursuant to 735 ILCS 5/2-801.

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

All individuals residing in the State of Illinois whose Private Information was disclosed to a third party without authorization or consent through the Pixel on Defendant's Web Properties.

213. 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.

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

215. **Numerosity**: The Nationwide Class Members are so numerous that joining all members is impracticable. Upon information and belief, there are hundreds of thousands (if not millions) of individuals whose PII and PHI may have been improperly disclosed by Duly, and the Class is identifiable within Defendant's records.

216. **Commonality & Predominance**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

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

- f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PHI and PII;
- g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;
- h. Whether Defendant violated the consumer protection statutes invoked herein;
- i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- j. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;
- k. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices and
- l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their PII and PHI.

208. **Typicality & Adequacy:** Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of Defendant's incorporation of the Facebook Pixel. Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

209. **Superiority and Manageability:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other

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

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

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

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

213. **Class-wide Injunctive Relief:** Unless a class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein and Defendant may continue to act unlawfully as set forth in this Complaint as Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

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

- a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;
- b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information with respect to Defendant's privacy policy;
- c. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

- d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;
- f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties and
- g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.⁵³

COUNT I

VIOLATION OF ILLINOIS EAVESDROPPING STATUTE

720 ILCS 5/14-1, *et seq.*

(On Behalf of Plaintiff & the Class)

217. Plaintiff repeats and realleges each and every allegation contained in the Complaint as if fully set forth herein.

218. 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).

219. 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

⁵³ Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

consent of all of the parties.”

220. 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).⁵⁴

221. 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).

222. 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.

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

224. The Illinois Eavesdropping Statute defines “private conversation” as “any oral

⁵⁴ 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, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution.”

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).

225. The private conversations recorded and transmitted by Defendant to undisclosed third-parties included, but were not necessarily limited to, Plaintiff and Class Members’ 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.

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

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

228. Plaintiff 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.

229. 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.

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

231. As a result, Plaintiff 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 II

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

232. Plaintiff repeats and realleges each and every allegation contained in the Complaint as if fully set forth herein.

233. Duly is a “person” as defined by ILCS § 505/1(c).

234. Plaintiff and the other Class Members are “consumers” as defined by 815 ILCS § 505/1(e).

235. Duly’s conduct as described herein was in the conduct of “trade” or “commerce” as defined by 815 ILCS. § 505/1(f).

236. Duly’s unfair acts and practices against Plaintiff 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.

237. Plaintiff and Class Members received and paid for health care services from Duly.

238. Plaintiff 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.

239. Plaintiff and other Class Members’ payments to Duly for health care services were for household and personal purposes.

240. Duly’s practice of disclosing Plaintiff’s 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.

241. Duly's unfair business practices were targeted at all Duly patients, including Plaintiff and other Class Members.

242. 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.

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

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

245. 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.

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

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

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

249. Duly acted intentionally, knowingly and maliciously to violate Illinois's Consumer

Fraud and recklessly disregarded Plaintiff's and Class Members' rights.

250. As a direct and proximate result of Duly's unfair, unlawful and deceptive acts and practices, Plaintiff 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.

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

- a. Duly harmed Plaintiff's and other Class Members' interest in privacy;
- b. Sensitive and confidential information that Plaintiff 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 Plaintiff and other Class Members and derived benefit therefrom without Plaintiff's and other Class Members' authorization, informed consent or knowledge and without sharing the benefit of such value.
- e. Plaintiff 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 Plaintiff and other Class Members' personal information.

252. Plaintiff, individually and on behalf of the Illinois Class Members, seeks all monetary and non-monetary relief allowed by law.

COUNT III

**VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT,
815 ILCS §§ 510/2, et seq.**

(On behalf of Plaintiff & the Class)

253. Plaintiff repeats and realleges each and every allegation contained in the Complaint as if fully set forth herein.

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

255. 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.

256. Duly’s practice of disclosing Plaintiff’s 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).

257. Duly’s practice of disclosing Plaintiff’s 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.

258. 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.

259. The above unfair and deceptive practices and acts by Duly were immoral, unethical,

oppressive and unscrupulous.

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

261. As a direct and proximate result of Duly's unfair, unlawful and deceptive trade practices, Plaintiff 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.

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

- a. Duly harmed Plaintiff's and other Class Members' interest in privacy;
- b. Sensitive and confidential information that Plaintiff 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 Plaintiff and other Class Members and derived benefit therefrom without Plaintiff's and other Class Members' authorization, informed consent, or knowledge and without sharing the benefit of such value;
- e. Plaintiff 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 Plaintiff and other Class Members' personal information.

263. Plaintiff 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.

264. Because Plaintiff 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, Plaintiff and other Class Members are likely to suffer continuing harm in the future.

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

COUNT IV

BREACH OF CONFIDENCE (On behalf of Plaintiff & the Class)

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

267. Plaintiff 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.

268. 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 Plaintiff's and other Class Members' communications with Defendant including Private Information and the contents of such information.

269. These disclosures were made without Plaintiff's or other Class Members' knowledge, consent or authorization.

270. The third-party recipients included, but were not limited to, Facebook.

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

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

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;
- b. Plaintiff 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 Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
- g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and
- i. Defendant's actions violated the property rights Plaintiff and Class Members have in their Private Information.

COUNT V**INVASION OF PRIVACY**
(On Behalf of Plaintiff & the Class)

273. Plaintiff repeats and realleges each and every allegation contained in the Complaint as if fully set forth herein.

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

275. Plaintiff and other 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.

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

277. Plaintiff and other Class Members had a reasonable expectation of privacy given Defendant's representations, HIPAA Notice of Privacy Practices and Privacy Policy.

278. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

279. Defendant's disclosure of private medical information coupled with individually identifying information is highly offensive to the reasonable person.

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

281. Plaintiff and other 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.

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

283. Plaintiff and other Class Members are also entitled to punitive damages resulting from the malicious, willful and intentional nature of Defendant's actions, directed at injuring Plaintiff and other Class Members in conscious disregard of their rights.

284. Such damages are needed to deter Defendant from engaging in such conduct in the future.

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

COUNT VI

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

286. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

287. Plaintiff 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.

288. Plaintiff 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.

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

290. Plaintiff 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.

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

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

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

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

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

296. Plaintiff seeks all other relief as the Court may deem just and proper.

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

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

298. When Plaintiff 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.

299. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

300. Plaintiff 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.

301. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to third parties, including Facebook.

302. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein. Plaintiff 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.

303. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff PATRICIA MAYER, on behalf of herself and all those similarly situated, respectfully prays for judgment in her 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 Plaintiff as Class Representative and Plaintiff's 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 Plaintiff's and other Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff 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

Plaintiff hereby demands that this matter be tried before a jury.

Date: April 10, 2023

Respectfully submitted,

ALMEIDA LAW GROUP LLC

Firm ID 100530

David S. Almeida (ARDC 6285557)

Elena A. Belov (*Pro Hac Vice forthcoming*)

849 W. Webster Avenue

Chicago, Illinois 60614

(312) 576-3024 (phone)

david@almeidawgroup.com

elena@almeidawgroup.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 Plaintiff & the Putative Class

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on April 10, 2023, 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