

Kaleigh N. Boyd, OSB No. 253094
MCNAUL EBEL PLLC
600 University Street, Suite 2700
Seattle, WA 98101
Tel: (206) 389-9332
Email: kboyd@mcnaul.com

Additional Counsel Listed on Signature Page

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION**

R.G., on behalf of herself and all others
similarly situated,

Plaintiff,

v.

Oregon Clinic, P.C.,

Defendant.

Case No. 3:26-cv-1666

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff R.G.,¹ at all times relevant herein, has been a patient of Oregon Clinic, P.C., facilities and clinics (“Oregon Clinic” or “Defendant”). She brings this class action lawsuit against the Oregon Clinic in her individual capacity and on behalf of all others similarly situated, and

¹ Plaintiff R.G. brings this action anonymously out of a desire to protect her personal health information from further disclosure under Oregon Law and the parameters set forth by the Health Insurance Portability and Accountability Act of 1996.

alleges, upon personal knowledge as to her own actions, her counsel's investigation, and upon information and belief as to all other matters, as follows:

1. Plaintiff brings this case to address Defendant's unlawful practice of disclosing Plaintiff's and Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") to Google, LLC ("Google") and other unauthorized third parties ("Unauthorized Parties"),² without its patients' knowledge or consent, through the use of tracking software that the Oregon Clinic embedded in its websites.

2. These disclosures occur as a result of the tracking software that the Oregon Clinic purposely installed on its website <https://www.oregonclinic.com/> ("the Website") and its associated patient-facing web properties (collectively, "Web Properties"), including but not limited to Google Analytics, DoubleClick, Google Tag Manager, the Meta Pixel, and related software ("Tracking Tools").³

3. The Tracking Tools share patients' Private Information with Google and other unauthorized third parties in violation of federal and state laws. The Oregon Clinic also developed identifying cookies to track its patients' use of the Website.

² As used herein, the phrase "Unauthorized Parties" is intended to encompass all entities that: (1) received Plaintiff and other patients' Private Information without first executing a HIPAA-compliant business associate agreement with the Oregon Clinic; or (2) received Private Information for marketing purposes prior to receiving a HIPAA-compliant marketing authorization.

³ Although Plaintiff is presently unaware of every type of pixel and tracking tool Defendant deployed on its Web Properties, "Tracking Tools" is used herein to refer to any technology that may currently, or may have previously, divulged Plaintiff's and other patients' PHI or PII without their knowledge or consent.

4. Healthcare patients simply do not anticipate or expect that their trusted healthcare provider will send their private communications, PHI, or PII to Unauthorized Parties, let alone Google, which has a sordid history of privacy violations in its pursuit of ever-increasing advertising revenue.

5. At all times, Plaintiff and Class Members had a reasonable expectation that the Private Information they communicated via the Web Properties in conjunction with their medical care would remain private, secure, and would only be used for their medical treatment.

6. Importantly, the information Google received via the Tracking Tools identifies specific patients, thereby linking them to the Private Information they communicated to the Oregon Clinic via its Web Properties, including patient status, medical symptoms, medical conditions, the specific type of care and treatments sought or received, and more.

7. Google collects and uses the Private Information it receives for marketing, which allows it to deliver target ads based on a person's use of the Website, specific medical condition, and location.

8. Neither Plaintiff nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Google.

9. Defendant breached its statutory and common law obligations to Plaintiff and Class Members by, inter alia: (i) aiding and/or procuring the interception of Plaintiff's and Class Members' communications; (ii) failing to remove or disengage technology that was known and designed to share patients' information; (iii) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Google or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through the Tracking Tools; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to

design and monitor its Website to maintain the confidentiality and integrity of patients' Private Information.

10. As a result of Defendant's conduct, Plaintiff and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) diminution of value of their Private Information; (iv) statutory damages; and (v) the continued and ongoing risk to their Private Information.

11. Plaintiff seeks to remedy these harms and brings causes of action for (1) breach of fiduciary duty/confidentiality; (2) violations of the Electronic Communications Privacy Act ("ECPA") 18 U.S.C. § 2511(1) – unauthorized interception, use, and disclosure; (3) negligence; (4) invasion of privacy (intrusion upon seclusion); (5) breach of implied contract; and (6) unjust enrichment.

PARTIES

12. Plaintiff R.G. is a natural person and citizen of Oregon, residing in Portland, Oregon, where she intends to remain.

13. Defendant Oregon Clinic P.C. is a physician-owned medical practice with approximately 50 locations across the Portland metropolitan area. Its principal place of business is located at 541 NE 20th Ave., Suite 225, Portland, Oregon.

14. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (42 U.S.C. § 1320d and 45 C.F.R. Part 160–45, C.F.R. Part 162, and 45 C.F.R. Part 164).

JURISDICTION & VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds

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

16. This Court also has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges questions of federal law under the ECPA (18 U.S.C. § 2511, *et seq.*).

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

18. Venue is proper under 28 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

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

19. In January 2026, the U.S. Department of Health and Human Services ("HHS") issued a final rulemaking notice regarding modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") to "strengthen the privacy and security protection for individuals' health information." 78 Fed. Reg. 5566 (January 25, 2013).

20. As part of that final rulemaking, which became effective on March 26, 2013, HHS stated that, to be considered protected health information (PHI) under HIPAA, information did "not necessarily [need to] include diagnosis-specific information, such as information about the treatment of an individual." 78 Fed. Reg. at 5598. Instead, "[i]f the information is tied to a covered entity, then it is protected health information by definition since it is indicative that the individual

received health care services or benefits from the covered entity, and therefore it must be protected . . . in accordance with the HIPAA rules.” *Id.*

21. In December 2022, HHS issued a bulletin (the “HHS Bulletin”) warning regulated entities like Defendant about the risks presented by the use of tracking technologies on their websites:

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.⁴

22. In other words, HHS expressly stated that when entities choose to implement tracking technologies, like Defendant has done in this case, the disclosure of patient information via those technologies violates HIPAA Rules *unless* the entities obtain a HIPAA-compliant authorization.

23. The HHS Bulletin further warns that:

While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.⁵

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

⁴ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dept. of Health & Hum. Servs. (June 26, 2024), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited June 12, 2026).

⁵ *Id.*

www.oregonclinic.com. Citing to the 2013 Final Rulemaking, HHS observed that “information that connects the individual to a regulated entity (i.e., that is indicative that the individual has received or will receive health care services or benefits from the covered entity) . . . relates to the individual’s past, present, or future health or health care or payment for care.”⁶

25. The HHS Bulletin went on to state:

Tracking technologies on a regulated entity’s unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. For example, tracking technologies could collect an individual’s email address and/or IP address when the individual visits a regulated entity’s webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.⁷

26. Shortly thereafter, HHS and the FTC issued a letter, once again admonishing the improper use of tracking technologies:

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

⁶ *Id.*

⁷ *Id.*

a breach of security under the FTC's Health Breach Notification Rule.⁸

B. How Websites Work: Source Code, HTTP Requests and Tracking Tools

27. To understand Defendant's unlawful data-sharing practices, it is important first to understand basic web design and Tracking Tools.

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

29. 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.

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

- **Uniform Resource Locator ("URL"):** a web address.
- **HTTP Request:** an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL, GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies:** a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Cookies are sent with HTTP

⁸ *Re: Use of Online Tracking Technologies*, U.S. Dept. of Health & Hum. Servs. and Fed. Trade. Comm'n (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf (last visited June 12, 2026) (emphasis added).

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.

31. A patient’s HTTP Request essentially asks the Website to retrieve certain information (such as the name of a doctor with whom a patient makes an appointment), 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 Web Properties).

32. Every website is comprised of Markup and “Source code.” Source code is simply a set of instructions that commands the website visitor’s browser to take certain actions when the web page first loads or when a specified event triggers the code. Source code is essentially the back-end portion of the website that is invisible to the average website user.

33. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests that are invisibly executed in the background without notifying the person using the web browser. For example, the Tracking Tools in this case are snippets of code that Defendant embedded in its Source Code, thereby instructing the Website to send a second set of transmissions to Google’s own web servers.

34. By contrast, the Markup is the façade of the website, and it is the only part that website visitors actually see when they access a website. As an example, a patient’s HTTP Request

seeks specific information from the Defendant’s Website (e.g., “Find a Doctor” page), and the HTTP Response provides the requested information in the form of “Markup,” forming the webpage’s content and features.

35. Similarly, when a patient visits www.oregonclinic.com and clicks the “Find a Doctor” button, the patient’s browser automatically sends an HTTP Request to Defendant’s web server. Defendant’s web server automatically returns an HTTP Response, which loads the Markup for that particular webpage. As depicted below, patients see only the Markup.

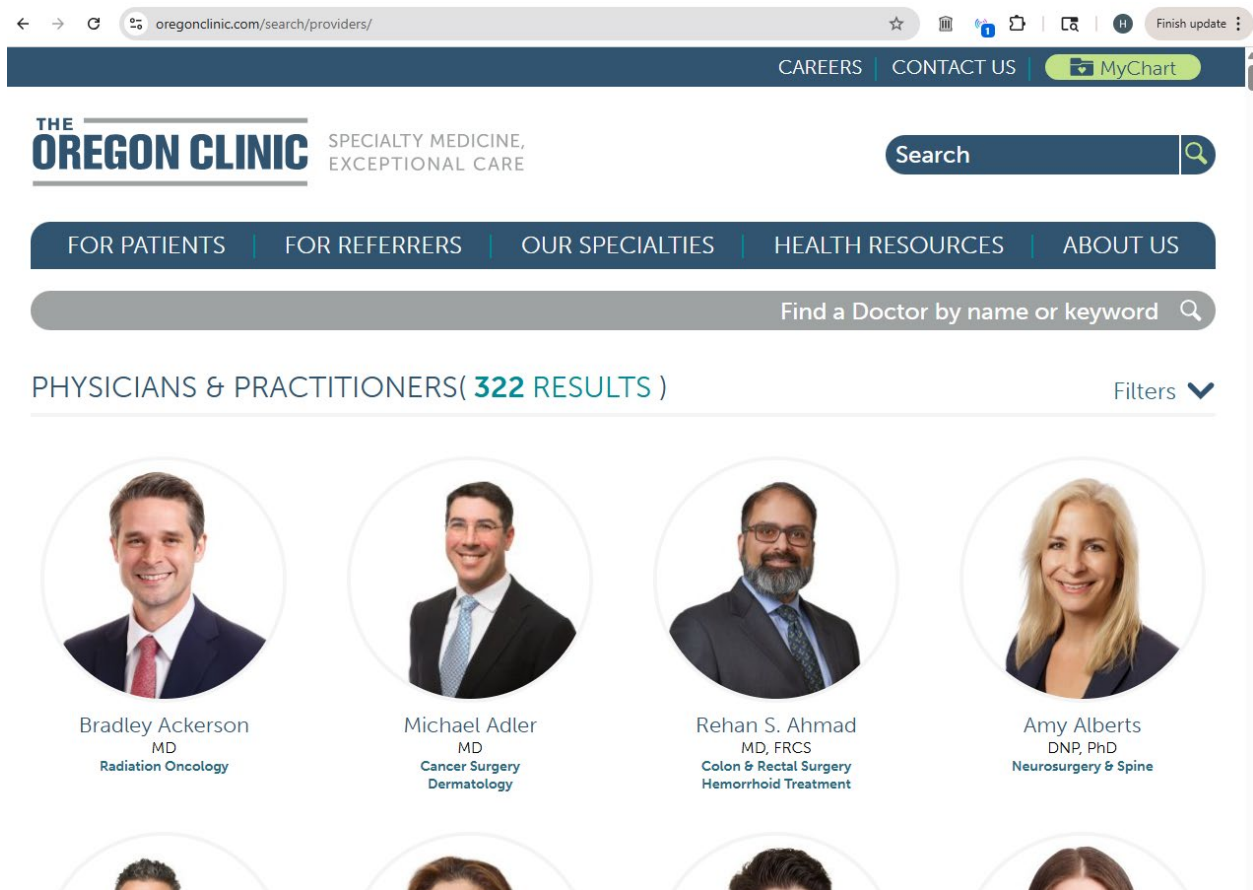


Figure 1: Image depicting the Markup version of oregonclinic.com/search/providers/

36. Oregon Clinic patients visit the Web Properties via an HTTP Request to Oregon Clinic’s server; that server sends an HTTP Response including the Markup that displays the webpage visible to the user and Source Code, including Oregon Clinic’s Tracking Tools.

C. Tracking Tools

37. Third parties, like Google, offer Tracking Tools that businesses and advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of users' online communications. The Tracking Tools are used to gather, identify, target, and market products and services to individuals.

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

39. When a user accesses a webpage that contains Tracking Tools, the user's communications with the host webpage are instantaneously and surreptitiously duplicated and sent to the third party who created the particular Tracking Tool, and, in many instances, onward to additional third parties.

40. For example, the Tracking Tools that Oregon Clinic installed and configured on its Web Properties cause a Website user's web browser to instantaneously duplicate and transmit the contents of their communication with the Oregon Clinic to Google's server.

41. In effect, Oregon Clinic plants a wiretap on every patient's browser. Once the Website loads, that tap is live, intercepting patients' private communications the moment they are made and transmitting them to Google. This all occurs without the patient's knowledge or consent.

42. Defendant intentionally configured the Tracking Tools installed on the Web Properties to capture both the "characteristics" of individual patients' communications with the

Web Properties (e.g., their IP addresses, cookie identifiers, device identifiers, and account numbers) and the “content” of these communications (i.e., the buttons, links, pages, and tabs they click and view, as well as search terms entered into free text boxes and descriptive URLs showing the information being exchanged).

43. Notably, these transmissions occur only when webpages contain Tracking Tools, so Plaintiff’s and Class Members’ Private Information would not have been improperly disclosed to Google via the Web Properties but for Defendant’s decisions to install the Tracking Tools on its Website.

44. The third parties to whom a website transmits data through Tracking Tools do not provide any substantive Website 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).

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

46. In this case, Defendant employed Tracking Tools to intercept, duplicate, and re-direct Plaintiff’s and Class Members’ Private Information to Google and other unauthorized third parties.

D. Defendant Improperly Disclosed Plaintiff’s & Class Members’ Private Information to Google

i. Google’s Tracking Tools

47. Unbeknownst to the patient, their private communications and actions on the Website are sent to Google, including but not limited to the specific text and medical conditions they type into the search bar and all of the other search parameters and filters they select.

48. Oregon Clinic utilized Google advertisements and intentionally installed the Google Tracking Tools on its Web Properties, including but not limited to Google Analytics, Google DoubleClick, and related ad trackers.

49. Google offers an ad targeting option called “Custom Audiences,” which Google employs via its Tracking Tools that website owners, like Defendant, install and customize on their websites.

50. Google operates the world’s largest internet search engine company and generated roughly \$307 billion in revenue in 2023, roughly 76% of which came from selling advertising.⁹

51. Google also tracks people through its widespread internet marketing products and ubiquitous trackers.

52. Google then sells advertising space by highlighting its ability to target users.¹⁰ Google can target users so effectively because it surveils user activity both on and off Google sites and apps. This allows Google to make inferences about users beyond what they explicitly disclose, determining audiences by “[users’] activity using Google products and third-party websites, or estimated based on content certain groups of people are likely to be interested in.”¹¹

53. Google compiles this information into a generalized dataset called “Audience Segments,” which advertisers use to apply highly specific filters and parameters for their targeted advertisements.¹²

⁹ Alphabet Inc., *Reports Fourth Quarter and Full Year 2023 Results*, https://s206.q4cdn.com/479360582/files/doc_financials/2023/q4/goog023-alphabet-2023-annual-report-web-1.pdf (last visited June 10, 2026).

¹⁰ Benefits of Online Advertising and Google Ads, <https://support.google.com/google-ads/answer/6123875?hl=en> (last visited June 10, 2026).

¹¹ About Audience Segments, <https://support.google.com/google-ads/answer/2497941> (last visited June 10, 2026).

¹² *Id.*

54. Google utilizes the precise type of information disclosed by Defendant to identify, target, and market products and services to individuals.

55. Advertisers can select “Custom Audiences,” which enables advertisers to reach “your ideal audience by entering relevant keywords, URLs, and apps.”¹³

56. With Custom Audiences, advertisers can target existing customers directly, and they can also build Audiences similar to their existing customers.

57. As Google puts it: “Google Analytics is a platform that collects data from your websites and apps to create reports that provide insights into your business.”¹⁴

58. Ultimately, Google Analytics, Google Tag Manager, and DoubleClick are bits of code that advertisers can integrate into their websites, mobile applications, and servers, thereby enabling Google to intercept and collect user activity on those platforms.

59. Google Analytics is automatically configured to capture certain data, like when a user visits a webpage, that webpage’s URL and metadata, or when a user downloads a mobile application or makes a purchase.¹⁵ Google Analytics can also track other events. Google offers a menu of “standard events” from which advertisers can choose, including what content a visitor views or purchases. Advertisers can even create their own tracking parameters by building a “custom event.”¹⁶

¹³ *Custom Audiences*, <https://developers.google.com/google-ads/api/docs/remarketing/audience-segments/custom-audiences> (last visited June 10, 2026).

¹⁴ *How Google Analytics Works*, <https://support.google.com/analytics/answer/12159447> (last visited June 10, 2026).

¹⁵ *Google Analytics - The Finer Points*, <https://marketingplatform.google.com/about/analytics/features/> (last visited June 10, 2026).

¹⁶ Google Analytics Help - About Key Events, <https://support.google.com/analytics/answer/9267568> (last visited June 10, 2026).

60. Google offers this code to advertisers, like Oregon Clinic, to integrate into their website. Google Analytics tracks “how many users perform the action and evaluate marketing performance across all channels that lead users to perform the action A key event is an event that measures an action that’s particularly important to the success of your business. When someone triggers the event by performing the action, the key event is recorded in Google Analytics and surfaced in your Google Analytics reports.”¹⁷

61. Google pushes advertisers, like Defendant, to install Google Analytics. Google says Analytics “can track what online behavior led to purchases and use that data to make informed decisions about how to reach new and existing customers.”¹⁸

62. Google tells advertisers that Google Analytics will improve their Google advertising through the following features: “Collects both website and app data to better understand the customer journey; Uses event-based data instead of session-based; Includes privacy controls such as cookieless measurement, and behavioral and key event modeling; Predictive capabilities offer guidance without complex models; Direct integrations to media platforms help drive actions on your website or app.”¹⁹

63. Google explains that Google Analytics logs consumer actions, such as clicking a button, called “events.”²⁰

¹⁷ *Id.*

¹⁸ *Google Analytics Help — The Value Of Digital Analytics*, <https://support.google.com/analytics/answer/12159453> (last visited June 10, 2026).

¹⁹ *Google Analytics Help — Set Up Analytics For A Website And/Or App*, <https://support.google.com/analytics/answer/9304153> (last visited June 10, 2026).

²⁰ *About Events*, <https://support.google.com/analytics/answer/9322688> (last visited June 10, 2026).

64. Google advises web developers to place Google tracking code early in the source code for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website.²¹

65. Google DoubleClick (now known in part as “Google Marketing Platform” and “Google Ad Manager”) is a separate but interrelated ad-serving platform that tracks and serves advertisements to users across the web.

66. If a healthcare provider, such as Defendant, installs Google Analytics and DoubleClick code as Google recommends, patients’ actions on the provider’s website are contemporaneously redirected to Google. When a patient clicks a button to book an appointment, Google’s source code commands the patient’s computing device to send the content of the patient’s communication to Google while the patient is communicating with their healthcare provider—traveling directly from the user’s browser to Google’s server.

67. In other words, by design, Google receives the content of a patient’s communication immediately when the patient clicks an appointment button, even before the healthcare provider receives it.

68. This contemporaneous and secret transmission contains the original GET request sent to the host website, along with additional data that Google Analytics and DoubleClick are configured to collect. This transmission is initiated by the Google code installed by Defendant and concurrent with the patients’ communications with the host website. Two sets of code are thus automatically run as part of the browser’s attempt to load and read Defendant’s Web Properties, Defendant’s own code, and the Google code Defendant embedded.

²¹ *Google Analytics Help — Set Up Analytics For A Website And/Or App*, <https://support.google.com/analytics/answer/9304153> (last visited June 10, 2026).

69. Oregon Clinic, through its installation and use of Tracking Tools, disclosed to Google the content of patient communications while its patients were exchanging communications with Oregon Clinic's Web Properties, which Google then used to target patients with ads based on those communications.

E. Google Uses Identifiers to Match the Health Information It Collects with Specific Google Users

70. Google tracks, among other types of data, “events,” which include instances when a patient downloads a document, engages with a webpage by putting in their login information, or navigates to a certain part of the webpage and clicks a button.

71. A first-party cookie, unique to Oregon Clinic’s Website, differs from third-party cookies in that it will not be identical when a user visits another website.

72. On Defendant’s Website, there are also third-party cookies placed by Google. Defendant does not use a cookie banner where users are given the option to consent to or reject third-party cookies. Instead, third-party cookies are automatically permitted by Defendant on their Website.

73. Google collects and stores the information DoubleClick obtains, including the “IDE” cookie (which is used to identify an individual, as each IDE cookie is unique for each user), IP addresses, and other cookies that uniquely identify browsers.

74. Google also collects and stores the “DSID” Google DoubleClick cookie. This cookie is used to identify users who are signed into their Google accounts and enables ads to follow the user to other sites.

75. Google Analytics event’s ‘tid’, is the tag ID of the Google Analytics (GA4) tracking code used by Defendant (identified in this case as “G-TN1LDF1J7N”), and it is how Google identifies Oregon Clinic’s Google Analytics account.

76. Google Analytics also captures the ‘cid’ parameter. The ‘cid’ parameter is a first-party cookie that helps Google identify Oregon Clinic’s users. Consequently, Google can connect these events with individual users of Defendant’s Web Properties.

77. Upon information and belief, Google uses first-party cookies, third-party cookies, tracking technologies, unique identifiers, as well as other methods, such as IP addresses, that can be used to identify users of Defendant’s Website.

78. Accordingly, Oregon Clinic’s Website through the Tracking Tools routinely provides Google with Oregon Clinic’s patients’ cid parameter cookies, IP addresses, and/or device IDs and the other information they input into the Website, including not only their medical searches, but also treatment requests, and the webpages they view. This is precisely the type of identifying information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.

79. Plaintiff’s and Class Members’ identities can be easily determined based on the cid parameter and other cookies, IP address, and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

80. On information and good faith belief, Google processes it, analyzes it, and assimilates it into data sets, and uses a behind-the-scenes process to identify specific users and match their profiles with data collected by the Tracking Tools, such as Google Analytics and DoubleClick, including specific actions taken by patients on websites in which Google tracking code is installed.

81. This disclosed Personal Information allows Google to know that a specific patient is seeking confidential medical care and the type of medical care being sought, and in addition to permitting Defendant to target those persons with Defendant’s ads, Google also then sells that

information to marketers who will target Plaintiff and Class Members online.

F. Defendant's Google Tracking Tools Disseminate Patient Information via its Website

82. The following example illustrates the point. If a patient uses the Website to find a doctor, Defendant's Website directs them to communicate Private Information, including the particular specialty the patient is seeking and the patient's preferred physician characteristics. Unbeknownst to the patient, each and every communication is sent to Google via Defendant's Tracking Tools, including the physician the patient selects, the location of that physician, the patient's attempt to call that physician for an appointment, and any text or phrases the patient types into the search bar.

83. As seen in Figure 2 below, a prospective patient navigated to the "Find a Doctor" page on Defendant's Website and was prompted to input their desired search criteria, including specialty, location, and physician's preferred gender.

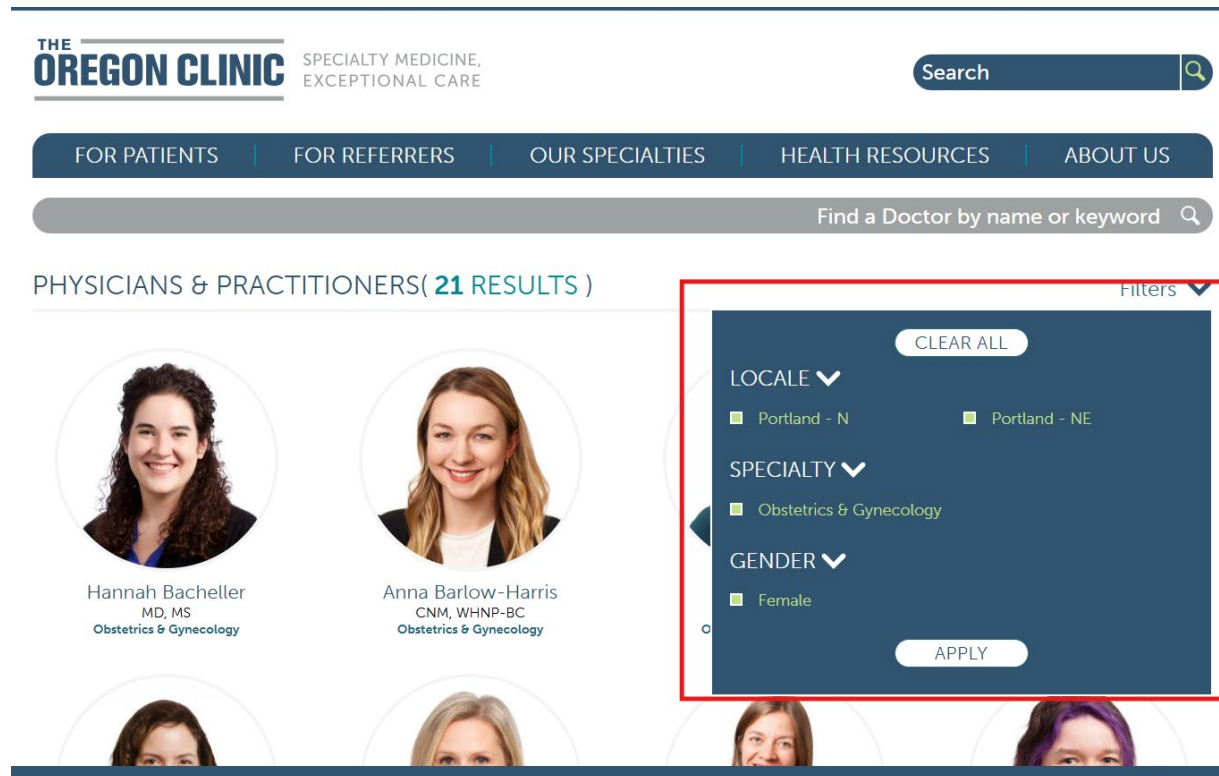


Figure 2. Search parameters entered by user on oregonclinic.com wanting a female physician, in Portland, Oregon, specializing in Obstetrics and Gynecology. Screenshots are presented here for illustrative purposes.

84. Unbeknownst to ordinary patients, this particular webpage, which is undoubtedly used to communicate Private Information for the purpose of seeking medical treatment, contains Defendant's Tracking Tools. Figure 3 below shows the "behind the scenes" portion of the website that is invisible to ordinary users. Importantly, each entry in the column represents just one instance in which Defendant's Tracking Tools sent this particular user's information to Google.

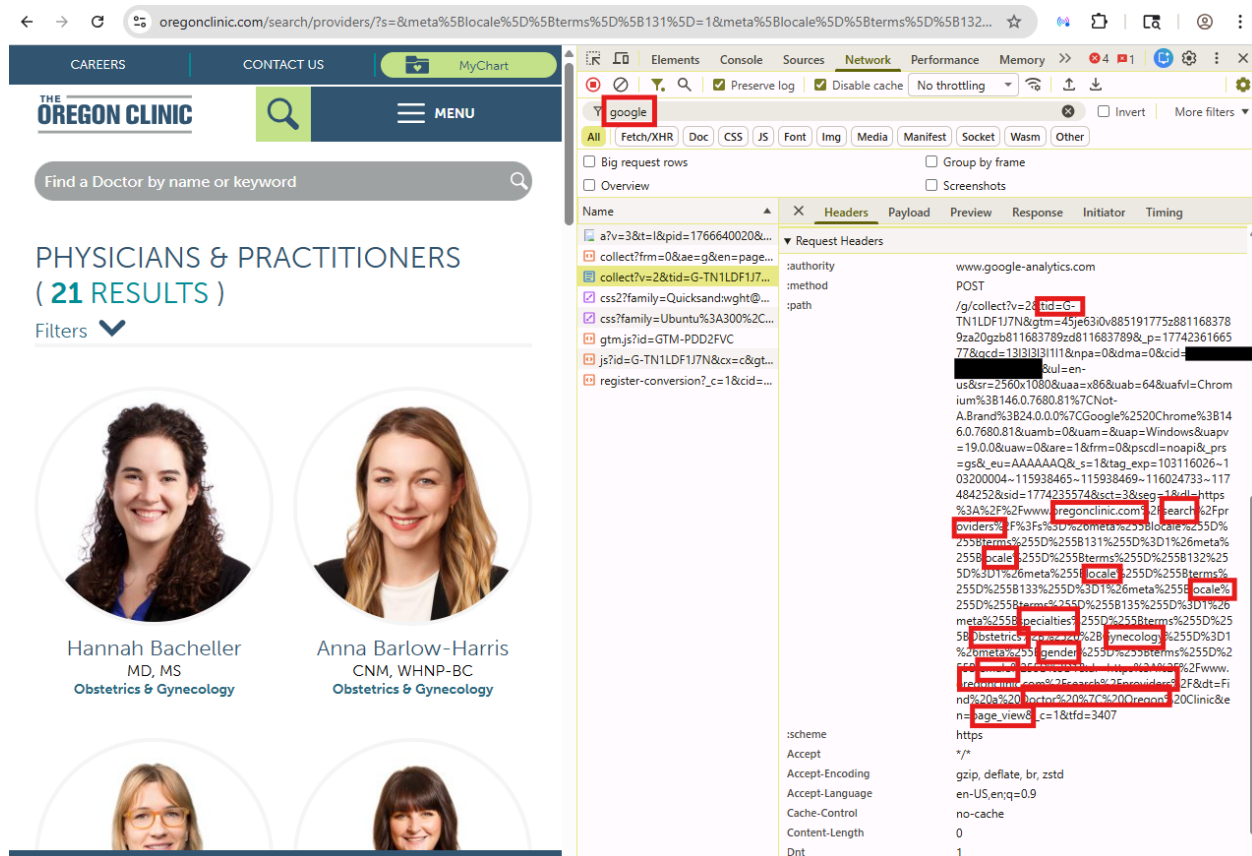


Figure 3. Screenshot taken from oregonclinic.com which shows the markup (user-facing portion of the website) alongside the network traffic. Each entry in the column to the right represents just one instance in which the user's information was transmitted to Google via Defendant's tracking tools.²²

²² The user's cid is blacked out to protect their anonymity.

85. Thus, without alerting the user, Defendant's Tracking Tools send each and every communication the user made via the webpage to Google and, as demonstrated in the images below, the communications Defendant sends to Google contain the user's Private Information.

86. Figure 4 below reveals what information is sent to Google when the user takes the next action and selects the physician that fits the searched parameters.

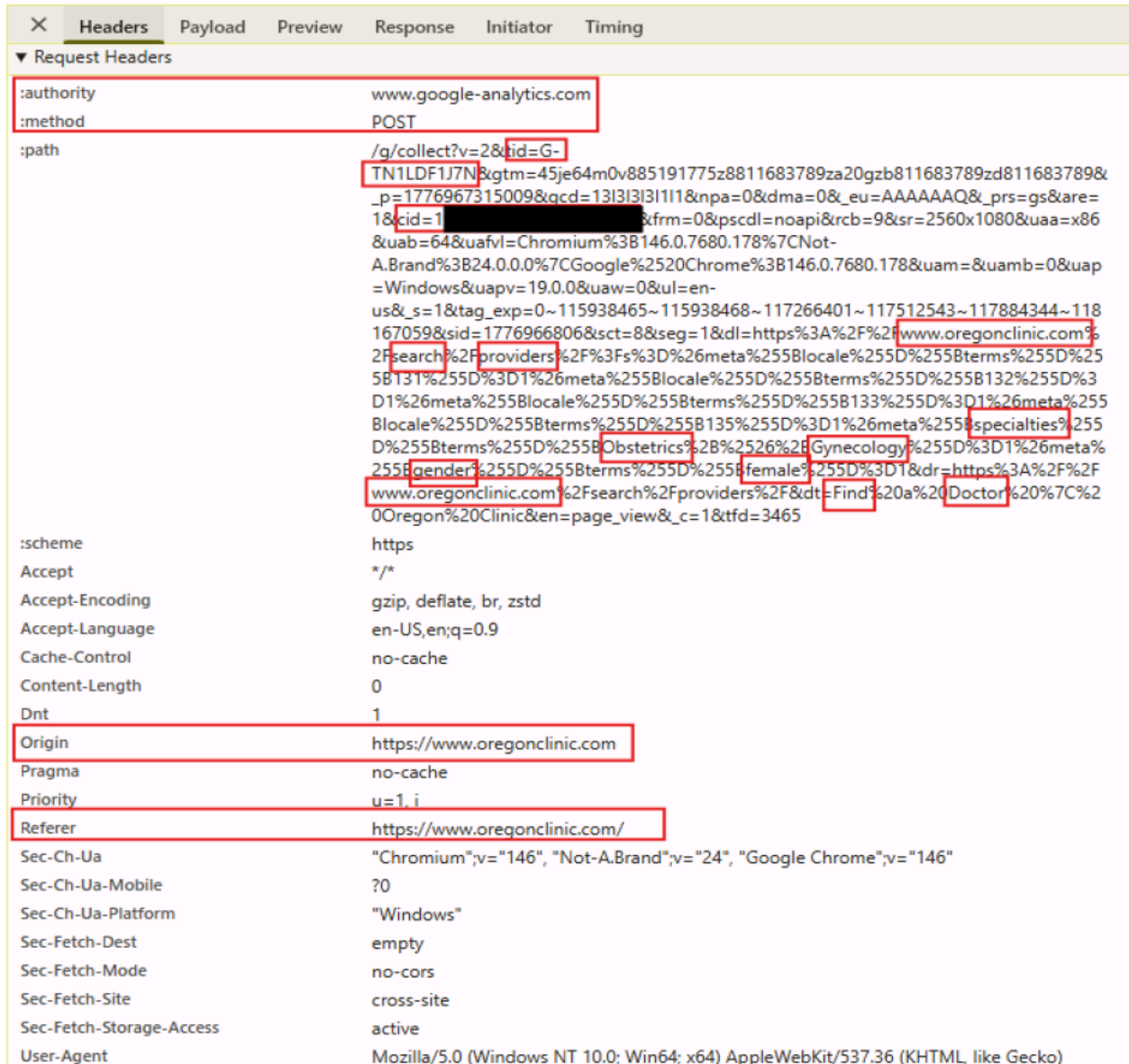


Figure 4. zoomed in Screenshot taken from user's network traffic report during their physician search on oregonclinic.com.

87. The first line of highlighted text, “tid:G-TN1LDF1J7N” refers to Defendant’s Google Analytics ID and confirms that Defendant has downloaded Google Analytics into its Source Code for this particular webpage.

88. The additional lines of highlighted text show Defendant has disclosed to Google that the user: (1) is a patient seeking medical care from Defendant via <https://www.oregonclinic.com>; (2) is seeking treatment from a specialist (Obstetrics and Gynecology); (3) is seeking treatment from a specific physician (Hannah Bacheller); and (4) is seeking treatment by a physician of a particular gender (Female).

89. As seen below, Figure 5 demonstrates that the user’s Google Account ID (highlighted as “cid=” in the image above) was sent alongside the other data.²³

90. In addition to their search for providers, other actions that patients take such as searching locations, looking to pay a bill, or navigating to the associated MyChart page are also transmitted via the Tracking Tools. This is simply unacceptable, and there is no legitimate reason for sending this information to Google or any other third party.

//

//

²³ As in the prior image, the cid information is redacted.

X	Headers	Payload	Preview	Response	Initiator	Timing
x						
	tid	G-TN1LDF1J7N				
	gtm	45je63i0v885191775z8811683789za20gzb811683789zd811683789				
	_p	1774277941186				
	gcd	13I3I3I1I1				
	npa	0				
	cid	[REDACTED]				
	ur	en-us				
	sr	2560x1080				
	uaa	x86				
	uab	64				
	uafvl	Chromium;146.0.7680.81 Not-A.Brand;24.0.0.0 Google%20Chrome;146.0.7680.81				
	uamb	0				
	uam					
	uap	Windows				
	uapv	19.0.0				
	uaw	0				
	are	1				
	frm	0				
	pscdl	noapi				
	_prs	gs				
	_eu	AgAAAAQ				
	_s	1				
	tag_exp	103116026~103200004~115938466~115938468~116024733~117484252				
	sid	1774276275				
	sct	4				
	seg	1				
	dl	https://www.oregonclinic.com/search/locations/				
	dr	https://www.oregonclinic.com/pay-your-bill/				
	dt	Find a Location Oregon Clinic				
	en	page view				
	_c	1				
	tfd	5135				

Figure 5. Screenshot taken from the user's traffic report depicting the "Payload" and corresponding "Headers" associated with the user's online activity and communications to Defendant.

91. In each of the examples above, the patient's website activity and the contents of the patient's communications are sent to Google alongside their PII information. Several different methods allow marketers and third parties to identify individual patients when the patient is logged into their Google account on their web browser or device. When this happens, the patient's identity is revealed via third-party cookies that work in conjunction with Google's Tracking Tools. For example, the tools transmit the patient's cid and other identifying information, thus allowing Google to link the user's online communications and interactions to their individual Google Account.

92. As seen in Figure 6, Defendant also revealed its website visitors' identities via first-party cookies such as the `_ga` cookie that Google uses to identify a particular browser and user:



<code>_ga</code>	GA[REDACTED]	.oregonclinic.com
<code>_ga_TN1LDF1J7N</code>	GS2:[REDACTED]	.oregonclinic.com
<code>_gcl_au</code>	[REDACTED]	.oregonclinic.com

Figure 6. Screenshot from Defendant's network traffic report depicting the first-party cookie `_ga`.

93. Importantly, the `_ga` cookie is transmitted to Google even when the user's browser is configured to block third-party tracking cookies because the `_ga` cookie functions as a first-party cookie, i.e., a cookie that was created and placed on the website by Defendant.

94. Google Analytics uses both first- and third-party cookies.

95. In summation, Google, at a minimum, uniquely identifies users with the `_ga`, and cid values track website visitors' sensitive communications and online activity. Google can link this data with visitors' corresponding Google Accounts. Because the Tracking Tools are automatically programmed to transmit data via both first-party and third-party cookies, patients' information and identities are revealed to Google even when they have disabled third-party cookies within their web browsers.

96. Further, even if the patient utilizes a different browser or uses a browser on their phone, Google still uses additional trackers for its ad services, namely Google Tag Manager and DoubleClick, as depicted below.

97. DoubleClick enables advertisers to integrate tracking codes into their websites. The data collected, combined with information from HTTP requests, helps create targeted ads.

98. DoubleClick also builds independent user profiles, allowing advertisers to optimize targeting.

99. The “IDE” cookie identifier, used to display ads, plays a key role in tracking users’ interactions across the web. It helps measure the effectiveness of advertisements by tracking actions users take after viewing or clicking on an ad, such as making a purchase or visiting specific pages.

100. Google collects and stores the information DoubleClick obtains, including the “IDE” cookie (which is used to identify an individual, as each IDE cookie is unique for each user), IP addresses, and other cookies that uniquely identify browsers. As seen in Figure 7 below, Google obtains the IDE cookie and IP addresses it can associate this information with a specific user, because Google is accessing individuals’ Private Information via the Website.

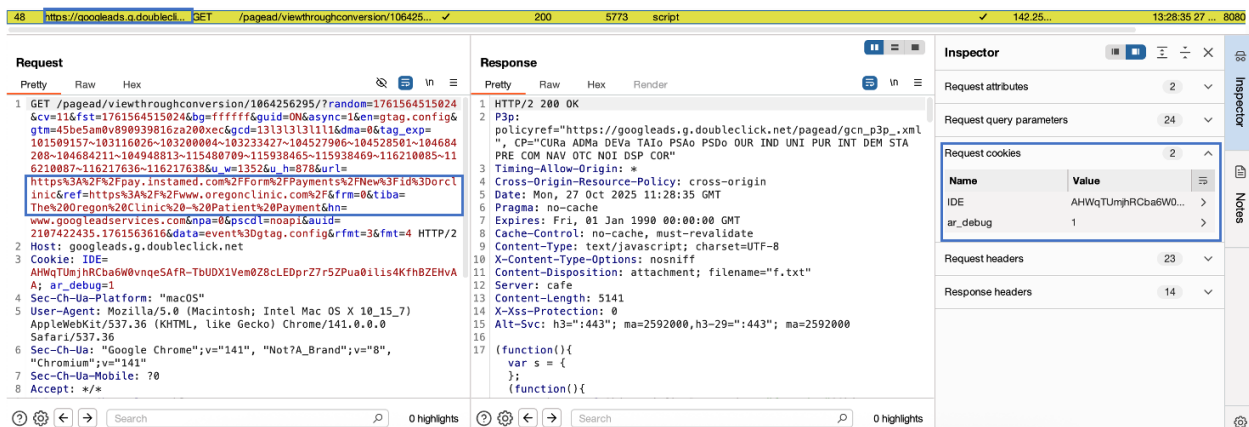


Figure 7. Screenshot from Defendant's Website when the user utilizes a web browser showing DoubleClick trackers active.

101. As seen in Figure 8 below, Google Tag Manager is also deployed on the Website as a tool to load and execute third-party trackers on the website. The execution of the Google Tag Manager script on the website can gather website user's data as they navigate the website.

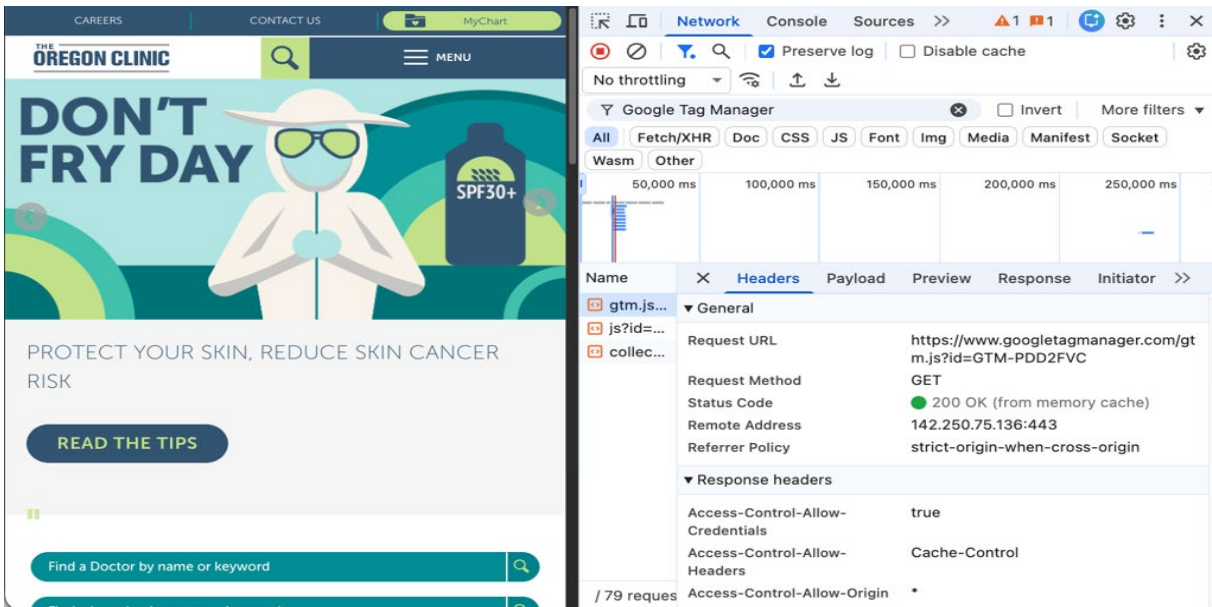


Figure 8: Screenshot from Defendant's website when the user utilizes a web browser showing Google Tag Manager script is active.

G. Additional Tracking Tools are Active on the Website

102. In addition to the Tracking Tools explained above, Oregon Clinic deploys other third-party Tracking Tools on its website including, but not limited to, the Meta Pixel.

103. Meta offers website owners an analytics tool called "Meta Pixel" which allows the owners to track users' actions on their website and measure the effectiveness of advertising by adding Meta Pixel's source code to their website.

104. The Meta Pixel uses the "c_user" third-party cookie to link users with an individual Facebook account and facilitate cross-site tracking. This cookie value is connected to a user's Facebook Profile ID and thus identifies a user individually via a Facebook account. Meta also

utilized the “fr” cookie for targeted advertising and to gather analytics. This cookie contains a unique identifier that allows Meta to track users’ behavior across websites and devices.

105. As seen in Figures 9 and 10 below, the Website includes the Meta Pixel.

106. Additional discovery will reveal the full extent and nature of the tracking and unlawful transmission of the Plaintiff’s Private Information to third parties that occurred via the Meta Pixel.

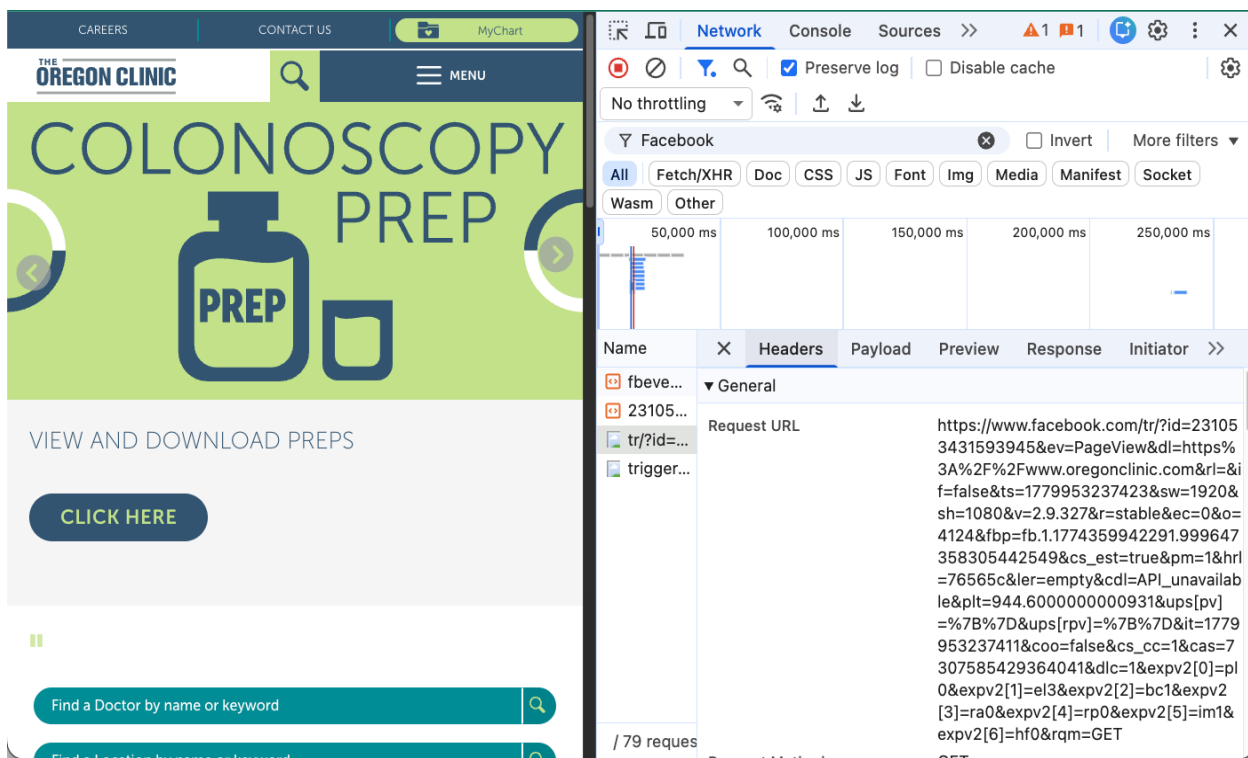


Figure 9: Screenshot from Defendant's Website when the user utilizes a web browser showing Meta Pixel script is active.

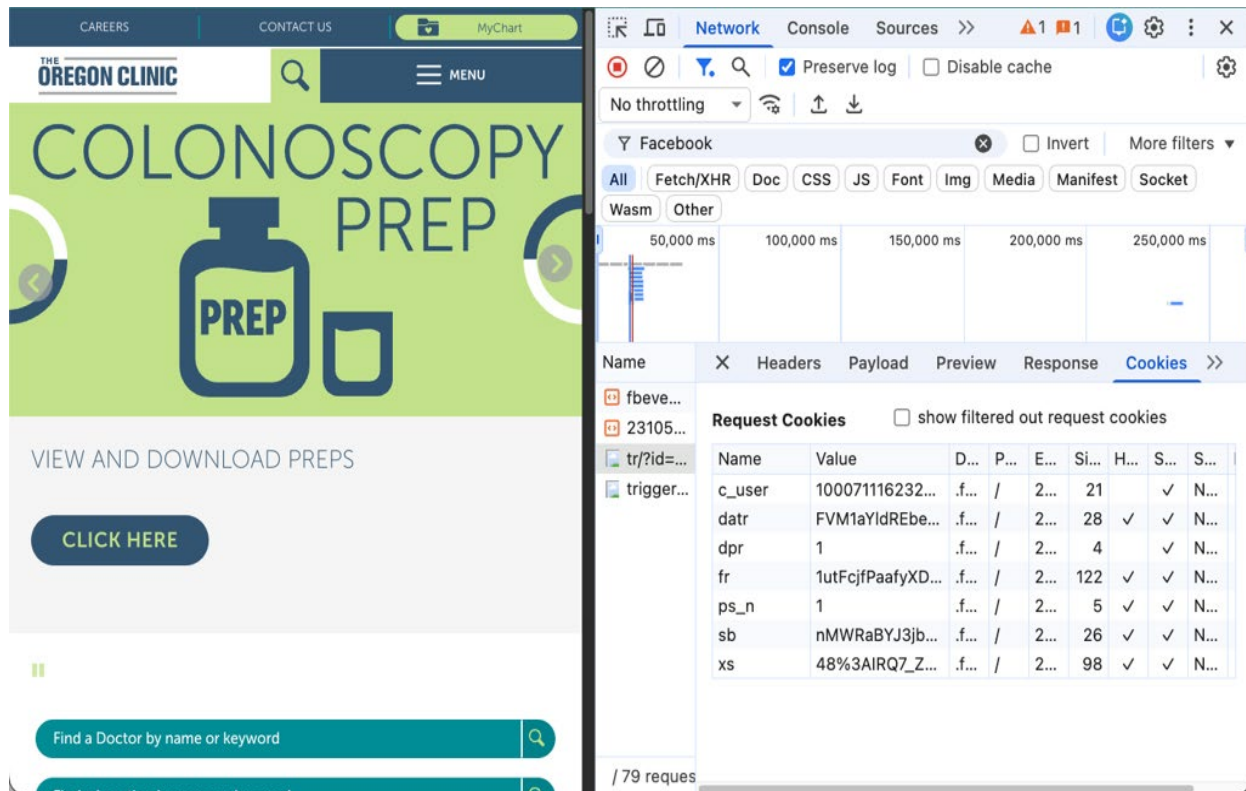


Figure 10: Screenshot from Defendant's Website when the user utilizes a web browser showing Meta Pixel script is active and c_user and fr cookies are deployed.

H. Plaintiff R.G.'s Experience

107. Plaintiff R.G. has been a patient of Oregon Clinic and has received healthcare services from Oregon Clinic for more than five (5) years, including through the present date.

108. Plaintiff has used Defendant's Website and Patient Portal on numerous occasions to communicate Private Information to Defendant in order to receive healthcare services from Defendant or Defendant's affiliates, at Defendant's direction, and with Defendant's encouragement.

109. Plaintiff has had a Google account for several years.

110. Plaintiff has had a Facebook account for approximately 18 years.

111. As a patient of Oregon Clinic, Plaintiff R.G. has received medical treatment from Oregon Clinic on many occasions, including appointments with specialists such as her Gastroenterologist, Podiatrist, Urologist and Gynecologist.

112. In addition to screenings and routine care, Plaintiff R.G. has also sought and received care for the treatment of a wart.

113. On numerous occasions, Plaintiff R.G. has used Defendant's Website to find and obtain medical treatment for her specific medical conditions, including the healthcare needs mentioned above.

114. Plaintiff R.G. has used Defendant's Web Properties frequently and regularly to do the following: (1) type her PHI into the search bar in order to identify treatments and services related to her medical conditions; (2) identify specific doctors and specialists, including those identified in paragraph 111; (3) access MyChart; (4) pay her medical bills; (5) book appointments with specialists; (6) access her medical records and test results; and (7) communicate information with Defendant, such as by uploading documents to the Patient Portal.

115. Plaintiff most recently accessed Defendant's Patient Portal and broader Website on or about January 23, 2026.

116. As a result of Defendant's decisions to install and use Tracking Tools on its Web Properties, Unauthorized Parties, including Google, received the contents of Plaintiff R.G.'s communication each time she communicated with the Web Properties.

117. These communications contained Plaintiff R.G.'s PHI and PII, including details revealing the types of treatments she sought and received, the specialists with whom she made appointments, and other information related to her past, present, and future medical care.

118. Plaintiff R.G. recalls seeing online advertisements related to her use of Defendant's Website following her visits, indicating that her Private Information was used by third parties to serve her targeted advertisements consistent with the health-related content she searched on Defendant's Website.

119. As Defendant's patient, Plaintiff R.G. reasonably expected that her online communications with Defendant were solely between herself and Defendant and that such communications would not be transmitted to or disclosed to Unauthorized Parties let alone to Google, which does not execute HIPAA-compliant Business Associate Agreements.

120. But for her status as Defendant's patient, Plaintiff R.G. would not have disclosed her Private Information to Defendant via its Website.

121. During her time as a patient, Plaintiff R.G. never consented to the use of her Private Information for marketing purposes, nor did she consent to Defendant enabling Unauthorized Parties to receive this information.

122. During the same transmissions, the Website routinely provided Unauthorized Parties with patients' IP addresses, device IDs, and/or user accounts or other information they input into Defendant's Website, like their home address, zip code, or phone number. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients. Plaintiff R.G.'s and Class Members' identities could be easily determined—and, on information and belief, was determined—based on the first- and third-party cookies, IP address, and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

123. After intercepting and collecting this information, Google processes it, analyzes it, and assimilates it into datasets for marketing.

124. Google is able to identify specific patients, including Plaintiff, through its internal systems and identity graphs, which links online activity to Google account holders' profiles.

125. In sum, Defendant's Tracking Tools transmitted Plaintiff's highly sensitive communications and Private Information to Google, including communications that contained private and confidential information, without Plaintiff's knowledge, consent, or express written authorization.

126. Plaintiff R.G. suffered injuries in the form of: (i) invasion of privacy; (ii) diminution of value of the Private Information; (iii) statutory damages; (iv) the continued and ongoing risk to her Private Information; and (v) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to her medical status and other confidential information she communicated to Defendant via the Website.

127. Plaintiff R.G. has a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure, and she also has an interest in knowing which Unauthorized Parties, aside from Google, have received her PII and PHI since she first started using the Website.

I. Defendant's Conduct Is Unlawful and Violated Industry Norms

1. Defendant Violated HIPAA Standards

128. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.²⁴

129. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually

²⁴ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

identifiable health information (collectively defined as ‘protected health information’) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.”²⁵

130. The Privacy Rule broadly defines “protected health information” (“PHI”) as individually identifiable health information (“IIHI”) that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

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

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

²⁵ *HIPAA For Professionals*, U.S. Dept.of Health & Hum. Servs. (Jul. 19, 2024), <https://www.hhs.gov/hipaa/for-professionals/index.html> (last visited June 12, 2026).

serial numbers; N. Web Universal Resource Locators (URLs); O. Internet Protocol (IP) address numbers; . . . and R. Any other unique identifying number, characteristic, or code” 45 C.F.R. § 160.514.

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

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

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

136. As alleged above, there is an HHS Bulletin that highlights the obligations of “regulated entities,” which are HIPAA-covered entities and business associates, when using tracking technologies.²⁶

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

138. Defendant’s actions violated HIPAA Rules per this Bulletin.

139. Google is a “business associate” of Defendant as that term is defined under HIPAA, 45 C.F.R. § 160.103, because Google creates, receives, maintains, and/or transmits protected health information on behalf of Defendant through the operation of the Tracking Tools described above.

140. HIPAA-covered entities, such as Defendant, may disclose PHI to a business associate only pursuant to a written Business Associate Agreement (“BAA”) that requires the business associate to appropriately safeguard the information. 45 C.F.R. § 164.502(e).

141. Google does not enter into BAAs with respect to its standard Google Analytics, Google Tag Manager, or DoubleClick advertising products. Google’s own help documentation states: “Google does not intend uses of Google Analytics to create obligations under HIPAA and makes no representations that Google Analytics satisfies HIPAA requirements. If you are a Covered Entity or Business Associate under HIPAA, you may not use Google Analytics for any purpose involving Protected Health Information.”²⁷

²⁶ See *HIPAA For Professionals*, U.S. Dept. of Health & Hum. Servs. (Jul, 19, 2024), <https://www.hhs.gov/hipaa/for-professionals/index.html> (last visited June 12, 2026).

²⁷ Google Analytics Help, *HIPAA and Google Analytics*, <https://support.google.com/analytics/answer/13297105> (last visited July 29, 2026); see also Piwik PRO, *Is Google Analytics HIPAA-Compliant?* (Feb. 19, 2026) (confirming Google

142. Upon information and belief, Defendant did not execute a HIPAA-compliant Business Associate Agreement with Google covering the Tracking Tools installed on the Website.

143. Accordingly, Defendant's disclosure of Plaintiff's and Class Members' PHI to Google via the Tracking Tools constitutes an impermissible disclosure under 45 C.F.R. § 164.502(a) and the HHS Bulletin described above.

144. Nor did Defendant obtain a valid, HIPAA-compliant patient authorization under 45 C.F.R. § 164.508 permitting the disclosure of PHI to Google for marketing purposes.

145. Defendant's Notice of Privacy Practices, did not disclose to patients that their PHI would be shared with Google or other third-party advertising and analytics vendors via Tracking Tools embedded on the Website.

146. Defendant's conduct in disclosing Plaintiff's and Class Members' PHI to Google without a BAA and without HIPAA-compliant authorization violated the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, and the HHS Bulletin's express guidance.

147. While HIPAA does not provide a private right of action, HIPAA and its implementing regulations, along with the HHS Bulletin, inform the applicable standard of care and the reasonable expectations of privacy that Plaintiff and Class Members held with respect to their Private Information, and are relevant to Plaintiff's state common-law and statutory claims below.

148. At least one federal court has held that allegations a healthcare provider's use of tracking technologies violated HIPAA by disclosing individually identifiable patient health information for commercial gain are sufficient, at the pleading stage, to support a properly alleged federal crime under 42 U.S.C. § 1320d-6.

“explicitly states it doesn't satisfy HIPAA requirements and won't sign a business associate agreement (BAA) with covered entities”)

149. Defendant’s conduct described herein also violates independent state-law duties and statutes, as set forth below.

2. Defendant Violated Oregon Law

151. Oregon law has established policies and procedures for the maintenance, preservation, and storage of patient medical records.

152. Oregon law provides that “(1) It is the policy of the State of Oregon that an individual has: (a) The right to have protected health information of the individual safeguarded from unlawful use or disclosure.” Or. Rev. Stat. Ann. § 192.553.

153. Oregon law also provides in Or. Rev. Stat. Ann. § 192.558 that PHI may only be used or disclosed consistent with prior authorization or without such authorization in particular circumstances.

154. Defendant’s disclosure of PHI by use of Tracking Technologies does not fit within any prior authorization or circumstances provided in Or. Rev. Stat. Ann. § 192.558.

155. Oregon’s constitutional and common-law protections for informational privacy likewise recognize a reasonable expectation of privacy in one’s confidential medical information, even where that information is held by a healthcare provider—an expectation Defendant violated through its undisclosed use of the Tracking Tools to transmit Plaintiff’s and Class Members’ Private Information, including the specific patient search, provider-selection, and appointment-related communications described in Section F above (see ¶¶ 82–101), to Google.

3. Defendant Violated Industry Standards

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

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

158. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care... Patient privacy encompasses a number of aspects, including, ... personal data (informational privacy)

159. 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.

160. 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 with ethics guidelines for confidentiality.

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

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

162. Indeed, at all times when Plaintiff and Class Members provided their Private Information to Defendant, they each had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with Unauthorized Parties for a commercial purpose unrelated to patient care.

163. Plaintiff and Class Members would not have used Defendant's Website, would not have provided their Private Information to Defendant, and would not have paid for Defendant's healthcare services, or would have paid less for them, had they known that Defendant would disclose their Private Information to Unauthorized Parties.

K. IP Addresses Are PII

164. On information and belief, through the use of the Tracking Tools, Defendant also disclosed and otherwise assisted Unauthorized Parties with intercepting Plaintiff's and Class Members' IP addresses and other persistent identifiers.

165. An IP address is a number that identifies the address of a device connected to the Internet, and it is used to identify and route communications on the Internet.

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

167. Over 70% of online websites use Google's visitor-tracking products, Google Analytics and Google Ad Manager.

168. Whenever a user visits a website that is running Google Analytics and Google Ad Manager, Google's software scripts on the website surreptitiously direct the user's browser to send a secret, separate message to Google's servers in California, which includes the user's IP address, the user's geolocation, information contained in Google cookies, any user-ID issued by the website to the user, and information about the browser the user is using.

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

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

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

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

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

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

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

173. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients to use its services. Defendant did so through use of the intercepted patient data it obtained, procured, and/or disclosed in the absence of express written consent.

174. By utilizing the Tracking Tools, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby

benefitting Defendant while invading the privacy of Plaintiff and Class Members and violating their rights under federal and Oregon law.

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

175. Plaintiff's data and Private Information has economic value. Google has recognized the value of user data and has even instituted a pilot program in which it pays users \$3 per week to track them online.

176. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as \$434 per user, for a total of more than \$200 billion industry wide.

177. The value of health data in particular is well-known and has been reported on extensively in the media. For example, *Time Magazine* published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.²⁸

178. Similarly, *CNBC* published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."²⁹

²⁸ See *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, <https://time.com/4588104/medical-data-industry/> (last visited June 10, 2026)

²⁹ See *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 June 10, 2026)

179. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. “No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable.”³⁰

180. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (“Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy.”).

181. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing historical information.

182. Additionally, healthcare data is extremely valuable to bad actors. **Health care records may be valued at up to \$250 per record on the black market.**³¹

TOLLING

183. Any applicable statute of limitations has been tolled by the “delayed discovery” rule.

184. Shortly before this Complaint was filed Plaintiff, through the investigation of undersigned counsel, learned about Defendant’s interception and unlawful disclosure of her Private Information to third parties in the manner described herein.

³⁰ Vero, *How to Collect Emails Addresses on Twitter*, <https://www.getvero.com/resources/twitter-lead-generation-cards/> (last visited June 10, 2026).

³¹ Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data* (June 30, 2021), <https://www.securelink.com/blog/healthcare-data-new-prize-hackers> (last visited June 10, 2026),

185. Plaintiff did not know (and had no way of knowing) that her Private Information was intercepted and unlawfully disclosed to Google and other third parties because Defendant kept this information secret and the Tracking Tools are invisible on the Website.

CLASS ACTION ALLEGATIONS

186. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated (“the Class”) pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

187. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All individuals residing in the United States who are, or were, patients of Defendant or any of its affiliates, who used Defendant’s Website in conjunction with their medical care.

In the alternative, Plaintiff seeks to represent an “Oregon Class” defined as:

All individuals residing in Oregon who are, or were, patients of Defendant or any of its affiliates, who used Defendant’s Website in conjunction with their medical care.

The Nationwide Class and Oregon Class are collectively referred to as the “Class.”

188. 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.

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

190. Numerosity, Fed. R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of

thousands of individuals whose PII and PHI may have been improperly disclosed via Defendant's Tracking Tools, and the Class is identifiable within Defendant's records.

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

- Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
- Whether Defendant had a duty not to disclose its patients' Private Information to Unauthorized Parties;
- Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to Google for marketing purposes;
- Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been divulged;
- Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;
- Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;
- Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct; and
- 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 Private Information.

192. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use of Tracking Tools, due to Defendant's misfeasance.

193. Adequacy, Fed. R. Civ. P. 23(a)(4). 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.

194. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for the 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.

195. Policies Generally Applicable to the Class, Fed. R. Civ. P. 23(b)(2). This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole.

196. Issue Certification, Fed. R. Civ. P. 23(c)(4). Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

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

198. Unless a class-wide injunction is issued, Defendant may continue disclosing the Private Information of Class Members and may continue to act unlawfully as set forth in this Complaint.

COUNT I
BREACH OF FIDUCIARY DUTY/CONFIDENTIALITY
(On Behalf of Plaintiff and the Class)

198. Plaintiff incorporates paragraphs 1 through 197 as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

199. Medical providers have a duty to their patients to keep non-public medical information completely confidential, and to safeguard sensitive personal and medical information. This duty arises from the implied covenant of trust and confidence that is inherent in the physician-patient relationship.

200. Medical providers also have a duty to maintain the confidentiality of Plaintiff's PHI under HIPAA and its implementing regulations, as well as Oregon state law governing PHI, Or. Rev. Stat. Ann. §§ 192.553 to 192.581.

201. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

202. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members: (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of disclosure of their Private Information to unauthorized third parties; and (3) to maintain complete and accurate records of what patient information (and where) Defendant did and does store and disclose.

203. Contrary to its duties as a medical provider and its express and implied promises of confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant as well as the contents of those communications, including Private Information.

204. These disclosures were made for commercial purposes without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged. The unauthorized disclosures of Plaintiff's and Class Members' Private Information were intentionally caused by Defendant's employees acting within the scope of their employment. Alternatively, the disclosures occurred because of Defendant's negligent hiring or supervision of its employees or agents, its failure to establish adequate policies and procedures to safeguard the confidentiality of patient information, or its failure to train its employees or agents to properly discharge their duties under those policies and procedures.

205. The third-party recipients included, but may not be limited to, Google. Such information was received by these third parties in a manner that allowed them to identify the Plaintiff and the individual Class Members.

206. Defendant's breach of the common law implied covenant of trust and confidence is further evidenced by its failure to comply with federal and state privacy regulations, including:

- a. By failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- b. By failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- c. By failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);
- d. By failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiffs and Class Members' PHI;
- e. By failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. By failing to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);
- g. By impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*;

- h. By failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);
- i. By failing to keep Private Information confidential as required by Or. Rev. Stat. Ann. § 192.553, *et seq.*; and
- j. By otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

207. The harm arising from a breach of provider-patient confidentiality includes mental suffering due to the exposure of private information and erosion of the essential confidential relationship between the healthcare provider and the patient.

208. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that: their sensitive and confidential information (that Plaintiff and Class members intended to remain private) is no longer private; Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements; Defendant eroded the essential confidential nature of the provider-patient relationship; 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; Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and Defendant's actions violated the property rights Plaintiff and Class members have in their Private Information.

209. Plaintiff and Class Members are entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation.

210. 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.

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

211. Plaintiff incorporates paragraphs 1 through 197 as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

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

213. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

214. The transmissions of Plaintiff's Private Information to Defendant via Defendant's Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

215. The transmissions of Plaintiff's Private Information to medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

216. Electronic Communications. The transmission of Private Information between Plaintiff and Class Members and Defendant via its Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or

photooptical system that affects interstate commerce” and are therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(2).

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

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

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

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

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

221. Specifically, Defendant intercepted Plaintiff’s and Class Members’ electronic communications via the Tracking Tools, which tracked, stored, and unlawfully disclosed

Plaintiff's and Class Members' Private Information to Unauthorized Parties including, but not limited to, Google.

222. These intercepted communications include, but are not limited to, communications to/from Plaintiff and Class Members that contain PII and PHI.

223. Under Oregon's computer crime statute, Or. Rev. Stat. § 164.377(2), a person commits the offense of unlawful use of a computer if the person "knowingly accesses, attempts to access, or uses or attempts to use a computer, computer system, computer network, or computer program knowing that the access or use is not authorized."

224. Defendant violated Or. Rev. Stat. § 164.377(2) in that Defendant knowingly used and accessed Plaintiff's and Class Members' computing devices and data without their authorization, including through placement of the Tracking Tools as well as use of source code that commanded Plaintiff's and Class Members' computing devices to send identifiers and the content of communications with Defendant simultaneously to Defendant, Google, and others.

225. Under Or. Rev. Stat. § 164.377(3), a person commits unlawful access to computer data if the person "knowingly and without authorization alters, damages, destroys, or uses a computer, computer system, computer network, or computer program or knowingly and without authorization takes, copies, or uses information stored in, produced by, or derived from a computer, computer system, computer network, or computer program."

226. Defendant violated Or. Rev. Stat. § 164.377(3) by exceeding its authorization to access Plaintiff's and Class Members' computers, including through use of source code that commanded Plaintiff's and Class Members' computing devices to make unauthorized copies of their electronic data and to send identifiers and the content of communications with Defendant simultaneously to Google and other Unauthorized Parties.

227. Under Or. Rev. Stat. § 165.540(1)(a), it is unlawful for any person to “obtain or attempt to obtain the whole or any part of a telecommunication or a radio communication to which such person is not a participant, by means of any device, contrivance, machine, or apparatus, whether electrical, mechanical, manual, or otherwise, without the consent of all participants in the telecommunication or radio communication.”

228. Defendant violated Or. Rev. Stat. § 165.540(1)(a) when it knowingly and without Plaintiff’s or Class Members’ authorization inserted the Tracking Tools on Plaintiff’s and Class Members’ computing devices. The Tracking Tools, which constitute programs, commanded Plaintiff’s and Class Members’ computing devices to intercept and redirect the content of their communications with Defendant to Google and Unauthorized Parties without the consent of all participants in those communications.

229. Under the Oregon Health Information Privacy Act, Or. Rev. Stat. § 192.558(2), no health care provider or health plan shall disclose health information about a patient without authorization except as expressly permitted. "Health information" includes any information, whether oral or recorded in any form or medium, that identifies or could be used to identify an individual and relates to the past, present, or future physical or mental health or condition of the individual. Or. Rev. Stat. § 192.553(5).

230. Defendant violated Or. Rev. Stat. § 192.558(2) by disclosing Plaintiff’s and Class Members’ Private Information to third parties, including Google, without authorization or consent.

231. Under Oregon’s physician-patient privilege, Or. Rev. Stat. § 40.235, a physician or licensed health care provider cannot disclose any information acquired in the course of professional services given to a patient, when the information was necessary to enable the provider to act in that professional capacity, absent patient consent.

232. Defendant violated Or. Rev. Stat. § 40.235 by disclosing Plaintiff's and Class Members' Private Information, acquired during the provision of medical services, to third parties, including Google, without authorization or consent.

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

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

235. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State, namely, violation of HIPAA, Oregon's Protected Health Information Policy, violation of Oregon's Computer Crime Statutes, violation of Oregon's unlawful interception of communications statute, invasion of privacy, and breach of confidence, among others.

236. Defendant intentionally used the wire or electronic communications to increase its profit margins. For example, this not only bolstered its marketing efforts, it allowed Defendant to use free and/or low-cost analytics tools in lieu of HIPAA-compliant business and marketing solutions.

237. In doing so, Defendant specifically used the Tracking Tools to track and utilize Plaintiff's and Class Members' Private Information for financial gain.

238. Defendant was not acting under color of law to intercept Plaintiff's and the Class Members' wire or electronic communications.

239. Plaintiff and Class Members did not authorize Defendant to acquire the contents of their communications for purposes of invading Plaintiff's privacy via the Tracking Tools.

240. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

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

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

242. Plaintiff incorporates paragraphs 1 through 197 as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

243. Medical providers have a duty to their patients to keep non-public medical information completely confidential, and to safeguard sensitive personal and medical information.

244. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

245. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed Tracking Tools to disclose and transmit Plaintiff's and Class Members' communications, including Private Information, to Unauthorized Parties.

246. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

247. The third-party recipients include, but may not be limited to, Google.

248. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that: Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private; Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements; Defendant eroded the essential confidential nature of the provider-patient relationship; 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; 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; Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and Defendant's actions violated the property rights Plaintiff and Class Members have in their Private Information.

249. Plaintiff and Class Members are entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation.

**COUNT IV
INVASION OF PRIVACY
Intrusion upon Seclusion
(On Behalf of Plaintiff and the Nationwide Class)**

250. Plaintiff incorporates paragraphs 1 through 197 as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

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

252. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to Unauthorized Parties.

253. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

254. Defendant's surreptitious recording and transmission of Plaintiff's and Class Members' Private Information to Unauthorized Parties, including marketing giant Google, is highly offensive to a reasonable person.

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

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

257. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted knowingly when it installed the Tracking Tools onto its Website because the purpose of the Tracking Tools is to disseminate patients' communications with the Website for marketing and advertising as opposed to legitimate medical purposes.

258. Because Defendant intentionally and willfully incorporated the Tracking Tools and encouraged patients to use the Website for healthcare purposes, Defendant had noticed and knew that its practices would cause injury to Plaintiff and Class Members.

259. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and Class Members was disclosed to Unauthorized Parties, causing Plaintiff and the Class to suffer damages.

260. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest, and costs.

261. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant and still in the possession of Google and the wrongful disclosure of the information cannot be undone.

262. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records.

263. Plaintiff, on behalf of herself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

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

264. Plaintiff incorporates paragraphs 1 through 197 as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

265. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiff and the Class Members provided their Private Information and compensation for their medical care.

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

267. 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.

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

269. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information without consent to third parties like Google.

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

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

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

272. Plaintiff incorporates paragraphs 1 through 197 as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

273. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at their expense.

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

275. Defendant was aware of the benefit conferred because it intentionally installed the Tracking Tools for the purpose of receiving the benefits of using patient data for advertising purposes.

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

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff R.G., on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

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

DEMAND FOR JURY TRIAL

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

//

//

//

//

DATE: August 10, 2026

Respectfully Submitted,

/s/ Kaleigh N. Boyd

Kaleigh N. Boyd, OSB No. 253094

MCNAUL EBEL PLLC

600 University Street, Suite 2700

Seattle, WA 98101

Tel: (206) 389-9332

kboyd@mcnaul.com

Heather M. Lopez, *pro hac vice* forthcoming

MILBERG PLLC

280 S. Beverly Drive, PH Suite

Beverly Hills, CA 90212

Tel: 331-240-3015

hlopez@milberg.com

Attorneys for Plaintiff and The Proposed Class