**UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLORADO**

| | |
|---|---|
| JACQUELYN ANDERSON,<br><br>*on behalf of herself and all others similarly situated*,<br><br>Plaintiff,<br><br>v.<br><br>UNIVERSITY OF COLORADO HEALTH,<br><br>Defendant. | Case No. _____<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Jacquelyn Anderson ("Plaintiff"), at all relevant times herein, was a patient of University of Colorado Health ("UCHealth" or "Defendant"), and used Defendant's website to research doctors, gather information about their specific health conditions, and schedule an appointment at the Loveland, Colorado UCHealth location. Plaintiff brings this class action lawsuit against Defendant in her individual capacity and on behalf of all others similarly situated. Upon her personal knowledge as to her own actions, upon her counsel's investigation, and upon information and belief as to all other matters, Plaintiff alleges as follows:

## RELEVANT BACKGROUND

1. Plaintiff brings this class action lawsuit on behalf of a nationwide class to address Defendant's outrageous, illegal, and widespread practice of collecting, disclosing, and monetizing Plaintiff's and Class Members' confidential personally identifiable information ("PII"), confidential health communications ("CHC"), and protected health information ("PHI") (collectively referred to as "Private Information") to unauthorized third parties, including Alphabet

Inc. ("Google"), without consent, through the use of tracking software that was implemented, configured, and embedded in Defendant's website.

2. Defendant is a non-profit corporation that operates more than 10 hospitals and medical centers.

3. Defendant owns and controls the website www.uchealth.org and associated subpages ("Defendant's Website," the "Website", or "UCHealth's Website"). Defendant holds its Website out to the public, including to Plaintiff and Class Members.

4. Defendant encourages its patients, including Plaintiff and Class Members, to utilize the Website as a confidential means of finding physicians and specialists, gathering information about specific health conditions, scheduling appointments, completing forms, requesting information, and accessing the patient portal.

5. Defendant intentionally installed tracking software on its Website that surreptitiously duplicated and sent customers' private communications to Google, the contents of which include Private Information.

6. Although Plaintiff is presently unaware of every type of pixel and tracking tool Defendant has implemented on its Website, the pre-suit investigation, including the review of the public-facing HAR files showing source code, revealed the presence of a collection of Google tools deployed on various sensitive pages of its Website, including the Portal. As used herein, the term "Tracking Tools" includes the suite of Google marketing tools including Google Analytics, the Google Tag Manager, and similar tools offered by Google in conjunction with its marketing products and other platforms (such as Google Ads Conversion Tracking, "DoubleClick," and Google Ad Remarketing), as well as any other tracking technologies.

7. The Tracking Tools' specific purpose is to provide website owners with the ability

to acquire the raw web user data and to then transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. The Tracking Tools are offered for "free" to companies like Defendant but require the website owner to share and disclosure the web users valuable behavioral web browsing data with unauthorized third-party marketers.

8. To be sure, "data is the new oil of the digital economy." Google and other ad tech companies are motivated to collect data, with Google's online advertising business generating 42.4% of global digital ad revenues in 2023.

9. With the intent to monetize the patient information flowing through its Website, Defendant installed Tracking Tools from Google and, upon information and belief, other third-party marketers (collectively, the "Unauthorized Third-Parties") onto its Website, which provided Defendant with valuable marketing tools to create more efficient and profitable marketing campaigns.

10. UCHealth did not disclose the presence of these Tracking Tools to its patients and Website users.

11. Patients do not anticipate or expect that their trusted healthcare provider will send their Private Information to Unauthorized Third-Parties like Google.

12. By deploying Google tracking on its Website, Defendant maximized the exposure of its patients' sensitive information, including the fact that they sought treatment, as well as their specific health conditions, based on their visits to specialists or treatment-specific pages to advertising ecosystems in order to gain the highest probability of converting new patients with the lowest cost per conversion of a new patient.

13. The Private Information that UCHealth transmitted to Unauthorized Third-Parties reveals (1) the fact that the individual sought treatment; (2) the individual's specific health

conditions, based on the specialists or treatment-specific pages visited; (3) desired medical treatment or therapies; (4) searches and purchases for particular treatments; (5) contact requests; and (6) bill pay information.

14. The information UCHealth divulged to the Unauthorized Third-Parties allowed them to learn that specific individuals went to schedule appointments at UCHealth clinics and other medical centers. It also revealed the fact that an individual is being treated for a specific medical condition, based on the specialist or treatment-specific pages the individual visited on Defendant's Website.

15. Moreover, the Private Information collected and disclosed by Defendant's Tracking Tools is not anonymous. The Tracking Tools capture a number of user specific data that can used to identify the specific user through various cross referencing and algorithmic methods, including persistent user IDs (e.g., the cid and auid), and, upon information and belief, IP addresses and browser fingerprint data points.

16. Simply put, the health information disclosed through the Tracking Tools is personally identifiable health information and is the digital equivalent of disclosing a comprehensive patient list to Google. Indeed, the Unauthorized Third-Parties each offer Tracking Tools free of charge, but the price that Defendant paid was the intercepted patient data. Effectively, Defendant traded its patient list for access to the "free" marketing tools.

17. Defendant is a HIPAA-covered healthcare entity, and thus its disclosure and use of Private Information for marketing is tightly regulated.

18. In addition to being a HIPAA-covered entity, UCHealth is subject to heightened confidentiality obligations pursuant to the Code of Federal Regulations ("CFR"), 42 U.S.C. § 290dd-2, which protects the confidentiality associated with "the identity, diagnosis, prognosis,

or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance use disorder education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States." 42 U.S.C. § 290dd-2(a). In fact, UCHealth's Website addresses both HIPAA and the CFR federal mandates, which applies to their patients.

19. The Federal Trade Commission ("FTC") has also warned hospitals and other entities that "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."

20. Despite these clear laws and regulations, UCHealth has essentially planted a bug on patients' web browsers, which forcibly and invisibly discloses their private and confidential communications to Unauthorized Third-Parties. This is the electronic equivalent of looking over the shoulder of each visitor for the entire duration of their website interaction.

21. There are many analytics companies and marketing campaigns that are HIPAA compliant that would have prevented Defendant's tortious acts; but Defendant opted for known non-HIPAA compliant analytics and marketing tactics to take advantage of the free services and gain access to powerful analytics, audience building, and re-targeting tools.

22. Moreover, UCHealth does not have a HIPAA-compliant Business Associate Agreement ("BAA") in place with any of the Unauthorized Third-Parties to safeguard its patients Private Information, and these companies are publicly vocal that they will not enter into healthcare BAA agreements.

23. In sum, through the use of Tracking Tools, Defendant intentionally transmitted Plaintiff's and Class Members' highly sensitive communications and Private Information to

Unauthorized Third-Parties, including communications that contained private and confidential health information; and further, Defendant utilized marketing tools and tactics with the intent of monetizing the Plaintiff's and Class Members' highly sensitive communications and Private Information. Neither Plaintiff nor any Class Member signed a written authorization permitting UCHealth to disclose or use their Private Information for marketing purposes.

24. As a direct and proximate result of UCHealth's conduct, Plaintiff and Class Members have suffered numerous harms and injuries, including invasion of privacy, breach of fiduciary duty, breach of confidentiality, loss of control of their Private Information, misappropriation of their Private Information, conversion of their Private Information, and the ongoing invasion of privacy and financial harm derived from the continued disclosure, interception, and misuse of their Private Information.

## JURISDICTION AND VENUE

25. The Court has jurisdiction over this action pursuant to 28 U.S.C § 1331 because the case presents a federal question. The Court has supplemental jurisdiction over all state law claims because they arise out of the same transaction and occurrence as the federal claim.

26. The Court has jurisdiction over this action pursuant to 28 U.S.C § 1332(d)(2)(A) as modified by the Class Action Fairness Act because at least one member of the Class, as defined herein, is a citizen of a different state than UCHealth, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

27. This Court has personal jurisdiction over UCHealth. Defendant is incorporated under the laws of Colorado. Defendant maintains its principal place of business at 12401 East 17th Ave., Mail Stop F417, Aurora, CO 80045. UCHealth regularly conducts business in and avails itself of the laws of Colorado.

28. Venue is proper in this District pursuant to 28 U.S.C § 1391 because the wrongful conduct giving rise to this case occurred in, was directed to, and/or emanated from this District. Plaintiff resides in this District, used the Website in this District, and their confidential communications were intercepted in this District.

## THE PARTIES

29. Plaintiff Jacquelyn Anderson is an adult citizen of the state of Colorado and is domiciled in Loveland, Colorado.

30. Defendant University of Colorado Health is a Colorado non-profit corporation that operates a network of more than 10 hospitals and medical centers throughout Colorado, primarily in the Denver metropolitan area, and in Wyoming and Nebraska. UCHealth employs over 36,000 employees.

## COMMON FACTUAL ALLEGATIONS

### A. Underlying Web Tracking Tools & Communications.

31. Devices (such as computers, tablets, or smart phones) 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).

32. 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' devices via their web browsers.

33. Every website is comprised of markup and source code. **Markup** is the forward facing portion of the website that the visitor sees and with which they interact. By contrast, **source code** is the invisible back-end portion of the website. The website user does not see what is happening within the source code during an ordinary website visit, but the source code acts as the set of instructions that commands the website visitor's browser and causes it to take certain actions

when the web page first loads or when a specified event triggers the code. The source code is the mechanism that controls how a website user's browser communicates with the website's server, and vice versa.

34. As a user interacts with a website on their device, several types of web communications are occurring between the user's browser and the website's server, as dictated by the website's source code, including but not limited to:

> **HTTP Requests** are electronic communications sent from the client device's browser to the website's server.
>
> **POST Requests** are a kind of HTTP request. They are the standard method by which a website transmits the information a user types into an online form — such as a name, email address, or message — from the user's browser to the website's server, distinguishing it from methods that display such data openly in the page's web address.
>
> **HTTP Responses** are electronic communications 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 a file, text information, or error codes, among other data.[1]
>
> **Uniform Resource Locators ("URL")** are web addresses that contain details of the HTTP Request and the user's specific search and browsing activities.
>
> **Cookies** are small text files that are set by the website the user is visiting and establish lines of communication between the user's browser and the website server. First Party Cookies are used to store information on the client device which can later be communicated to a server or servers such as user preferences (e.g., remember login info). Users cannot detect or prevent transmissions through first-party cookies. Third-Party Cookies are set by a third-party domain such as Google and are used for targeted marketing purposes. Third-Party cookies can track the user across the web as the user searches and visits other websites.

35. A website owner, such as Defendant, can manipulate the website's source code in a manner that allows third parties to access the website user's communications.

36. In this case, Defendant achieved this via Tracking Tools that it installed for the

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

purpose of invisibly gathering patients' data as they used the Website, monetizing that data, and using it for various marketing purposes.

37. The at-issue Tracking Tools are implemented on a website by secretly embedding and configuring the tracking software into the Source Code. Once the Tracking Tools implemented and configured in the Source Code, they automatically intervene and manipulate the web communications between the user's browser and the website server and instruct the website to send a duplicate transmission of the communication to unauthorized third-party servers, i.e., Google.

38. As explained below, Defendant effectively used its Source Code to commandeer and "bug" or "tap" its patients' computing devices, allowing Unauthorized Third-Parties to listen in on their communications with Defendant and thereby intercept those communications, including the Private Information at-issue.

## B. The Google Analytics Tools.

### 1. Defendant Intentionally Deployed Google Analytics, Enabling Google to Collect Private Information from Website Users, Including Plaintiff and Class Members.

39. Defendant implemented and configured Google Analytics in its Website's source code in a variety of ways with the intent to (a) intervene and manipulate Plaintiff's and Class Members' HTTP request communication and (b) collect and share Plaintiff's and Class Members' behavioral data with Google.

40. Google offers a suite of online Tracking Tools, including SDKs (software development kits) and tracking pixels, to help drive ad revenue. One of these SDKs and tracking pixels that Defendant has installed on its Website is Google Analytics.

41. Google Analytics is incorporated into websites, including Defendant's Website, by adding a small piece of JavaScript code to the invisible source code of a webpage. This code

immediately intercepts a patient's interaction with the webpage every time the patient visits it, including what pages they visit and what they click on.

42. Once Google's software code collects the data, it packages the information and sends it to Google Analytics for processing. After the data has been processed and stored in the database, Google uses the data to generate reports, including reports on acquisition, engagement, and demographics.

43. Google pitches Google Analytics as a marketing platform that offers "a complete understanding of your customers across devices and platforms." Google Analytics allows companies that utilize it to "understand how your customers interact across your sites and apps, throughout their entire lifecycle," "take action to optimize marketing integrations across Google's advertising and publisher tools," and "quickly analyze your data with an easy-to-use interface and shareable reports."

44. The Tracking Tools enable advertisers and companies like Defendant to benefit from Google's advertising ecosystem, and the data secretly collected from patients helps create targeted ads. Defendant installed these Tracking Tools.

45. In addition to using the data collection process mentioned above, Google Analytics sends requests to Google, along with unique identifier cookies to track behavior across websites and link it to advertising audiences and targeting signals. These cookies enable Google to create more comprehensive user profiles by connecting web activity to authenticated accounts.

46. Defendant encourages patients to use the Website, a tapped device, and once the Website loads on the patient's browser, the wiretap quietly waits for patients' private communications to trigger the tap, which then intercepts those communications and transmits them to Google.

47. Transmissions only occur on webpages that contain Tracking Tools. Thus, Plaintiff's and Class Members' Private Information would not have been disclosed to Google via this technology but for Defendant's decisions to install the Tracking Tools on its Website.

48. In addition to accessing and using the data intercepted from website users to provide its services, Google also uses the information intercepted by sites like Defendant's to maintain and improve Google's own services, develop new services, measure the effectiveness of its advertising, and personalize content and ads that one sees on Google's and its partners' sites and applications. When combined with Google's vast data resources from its other products and services, the data collected by Google's Tracking Tools can contribute to comprehensive profiles of individuals that can be used for targeting advertisements and other commercial purposes.

**2. The Google Analytics Tools Disclosed the Fact That Plaintiff's and Class Members' Private Information Was Their Own Information.**

49. The Google Analytics code collects PII, such as personally-identifying cookies, that enable Google to associate specific individuals, device information, and more with their Private Information.

50. Defendant utilized Google Analytics's third-party cookies. Although Google created these cookies, Defendant is ultimately responsible for the manner in which individual website users were identified via these cookies, and Google would not have received this data but for Defendant's implementation and use of the Pixel throughout its website.

51. The Google Analytics code on Defendant's Website uses "3PSID," "3PAPISID," and "3PSIDCC" third-party cookies to identify Defendant's patients by linking their browsing activity to their Google account. The values of these cookies are unique to each account holder and persist across sessions and devices.

52. Once the Google Analytics tracker intercepts and processes the raw user data about

"events," it uses the 3PSID, 3PAPISID, and 3PSIDCC cookies to associate this data with unique user identifiers, from which it can link website interactions to individual user profiles and track users across multiple different websites, sessions, and devices when signed into their Google accounts.

53. When creating a Google account, users provide their full name, email address, phone number, home address, work address, and a profile photograph. Therefore, Google can associate data collected alongside its third-party cookies with an email address and other PII, thereby allowing it to link a patient's private communications to their real-world identity.

54. Plaintiff's and Class Members' interactions conveyed Private Information on webpages containing the 3PSID, 3PAPISID, and 3PSIDCC. Moreover, Plaintiff and Class Members provided their PII as a necessary part of creating their Google accounts.

55. Additionally, the Google Analytics Tracker can set a different type of cookie, known as the NID cookie, which is tied to the user's browser rather than to a named account. The NID cookie still contains a unique identifier that persists for approximately six months, and the NID cookie enables Google to track user preferences, browsing behavior, and ad interactions across websites that use Google Analytics or serve Google Ads even if the user is not signed into a Google account on that browser. While the NID cookie does not reveal a named account identity, it still allows Google to build behavioral profiles and serve personalized advertisements based on a user's activity, including activity on websites such as Defendant's Website.

## C. The DoubleClick Tools.

### 1. Defendant Intentionally Deployed Google's DoubleClick, Enabling Google to Collect Private Information from Website Users, Including Plaintiff and Class Members.

56. Another of the Google tracking devices that Defendant has installed on its Website is DoubleClick. DoubleClick is designed to collect information about user behavior on websites

in order to improve the targeting and effectiveness of advertising campaigns. DoubleClick's tracking technologies (the "DoubleClick Tracker") automate the ad buying process and use collected data for targeted advertising initiatives.

57. Like Google Analytics, DoubleClick is incorporated into third-party websites, including Defendant's Website, by adding a small piece of JavaScript code to each page on the site. This code immediately intercepts a patient's interaction with the webpage every time the patient visits it, including what pages they visit and what they click on. The code also collects PII, such as cookies that identify specific individuals, device information, and more.

58. The DoubleClick Tracker distinguishes itself from Google Analytics in that it specifically focuses on advertising functionality. Once Google's software code collects the data, it packages the information and sends it to Google for processing. After the data has been processed and stored in the database, it is used to enable ad retargeting, which allows Defendant to display targeted advertisements to users on other websites based on their previous interactions with the Website.

59. Also like the Google Analytics Tracker, the DoubleClick Tracker can collect data on user interactions with a website and transmit these details to Google. These interactions may include page views, clicks, form submissions, video plays, and other custom-defined actions. While Google Analytics refers to these as "events," the DoubleClick Tracker generally tracks them as "conversions" or "activities," primarily for advertising and attribution purposes.

60. Defendant installed and configured the DoubleClick Tracker on its Website. As a result, the DoubleClick tracking code was present on pages through which patients searched for providers by specialty and name, viewed individual provider profiles, located medical facilities, searched for clinical services and medical conditions, and entered free-text queries. By installing

the DoubleClick Tracker, Defendant caused patients' page views, clicks, searches, and other Website communications to be transmitted to Google. Upon information and belief, Defendant maintained the DoubleClick Tracker on its Website throughout the relevant period.

**2. DoubleClick and its Associated Google Tools Disclosed the Fact That Plaintiff's and Class Members' Private Information Was Their Own Information.**

61. Through the DoubleClick Tracker, Google creates and assigns unique identifiers to website visitors, including through the IDE cookie and, upon information and belief, the DSID cookie. The IDE cookie is a persistent advertising identifier containing a string of numbers and letters. The IDE cookie is unique to each user's browser and is used to record user actions and measure ad effectiveness. This identifier can be associated with a user's browser or device over extended periods of time. The DSID cookie is an account-linked identifier that is set when a user is logged into a Google account. It links browsing activity on non-Google websites to the user's Google account and ensures that the user's ad personalization settings are applied and respected across non-Google sites. The cookies contain unique user identifiers that enable Google to connect user behavior across different websites, devices, and browsing sessions.

62. The DoubleClick Tracker also collects and stores IP addresses in server logs. An IP address is a globally unique numerical identifier that guides or routes communications across the Internet. Internet service providers assign IP addresses to networking devices such as modems or routers.

63. IP addresses function as the essential addressing system of the internet. Just as a telephone number routes calls to the correct household, an IP address is necessary for routing internet communications to the correct location. Importantly, IP addresses reveal the general geographic location of internet users. Free online "IP lookup" services use databases that map IP addresses to geographic areas and potentially specific households, often providing information

about the country, city, county, approximate coordinates, or even the internet service provider associated with the address.

64. The geolocation capability of IP addresses makes them extraordinarily valuable for digital advertising and tracking. IP addresses allow companies to target advertisements to users in specific geographic areas with over 95% accuracy and track user interactions across multiple websites, building detailed profiles of users' browsing habits tied to their location.

65. IP addresses are particularly powerful when combined with persistent identifiers like the IDE cookie. When individuals use their devices across different locations (home, work, coffee shops), each location has its own IP address. By tracking these movement patterns between different IP addresses and correlating them with a cookie, Google can build detailed profiles of individual users' daily routines and behaviors that distinguish them from others who may share the same IP address. This combination of cookies and IP address patterns allows Google to identify and track specific individuals with remarkable precision, even when multiple people share the same household or workplace network.

66. For these reasons, Europe's General Data Protection Regulation ("GDPR") classifies IP addresses as "personal data," recognizing that even data that has been de-identified or pseudonymized but can be used to re-identify a person remains personal data. When Google combines IP addresses with the IDE cookie and the sensitive health information intercepted from the Website, it creates a comprehensive digital profile that can identify specific individuals and their medical interests.

67. The DoubleClick Tracker also works in concert with Google's vast advertising network, which spans millions of websites. This means that the scope and impact of the interception facilitated by Defendant extends far beyond the Website, potentially affecting users'

experiences across the entire Internet ecosystem. When combined with Google's other data sources, the information intercepted through the DoubleClick Tracker enables even more precise identification and tracking of individuals.

68. Upon information and belief, Google combines the Personal Information intercepted through the DoubleClick Tracker with other data points in its possession (including data points obtained through the Google Analytics Tracker) to create comprehensive user profiles that include intimate details about individuals' medical conditions, treatment interests, and healthcare-seeking behaviors. These profiles can then be monetized through targeted advertising that may reveal or allude to users' private health concerns.

**D. A Web User's Journey on Defendant's Website.**

69. The following paragraphs will walk through the process of what Plaintiff and Class members would experience when utilizing Defendant's Website, as well as showing what was happening secretly in the Source Code surveilling their activity.

**1. The "Schedule an Appointment" Webpage**

70. UCHealth encourages users to schedule a medical care appointment online through the "Schedule an Appointment."

71. Upon the user's navigation to the "Schedule an Appointment" webpage, each of the Tracking Tools fired and transmitted POST Requests to Google that contained the title of the page visited, "Schedule an Appointment," alongside the user's personal Google identifier.

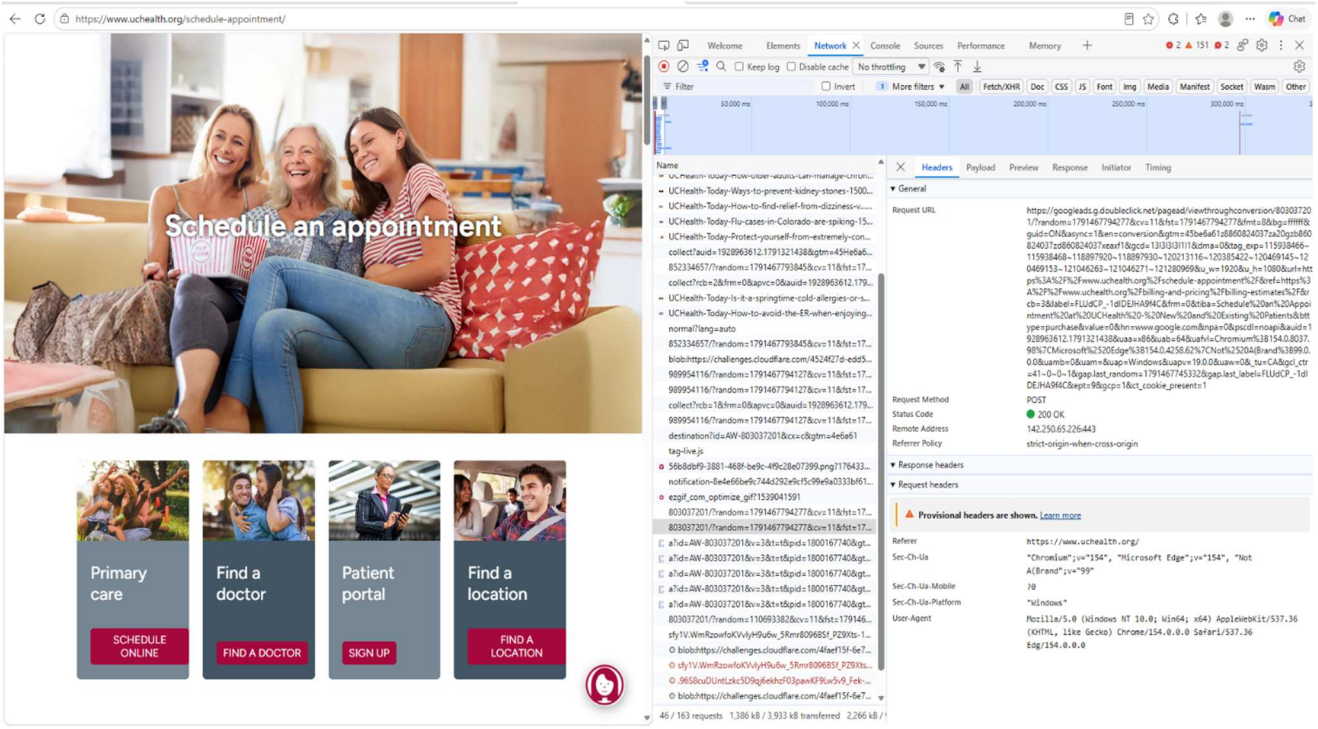


*Figure 1: Screenshot of network traffic taken from Defendant's website which shows that the Tracking Tools are actively installed and firing on Defendant's "Schedule an Appointment" Webpage.*

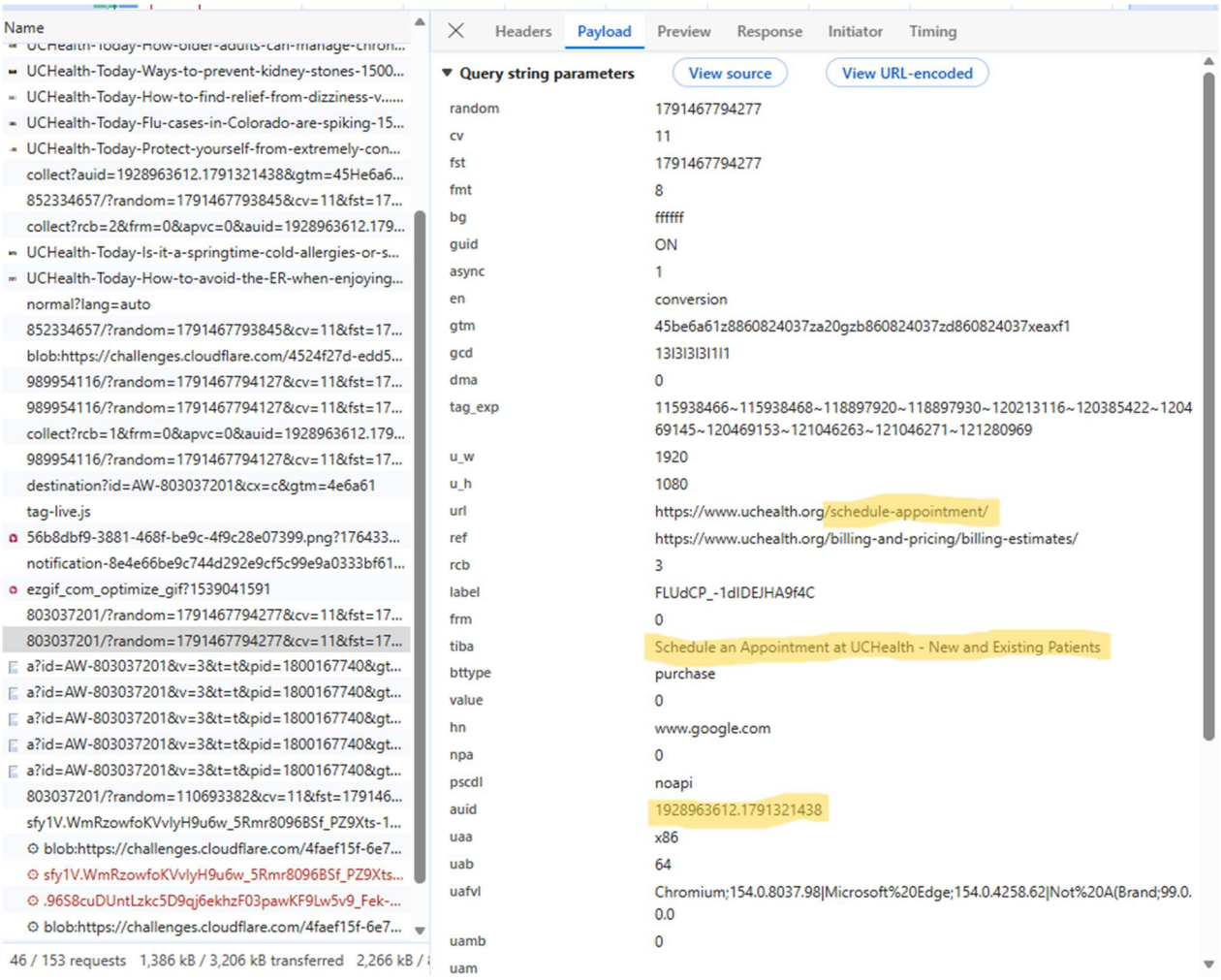


*Figure 2: The information sent to Google is parsed to reveal the user visited the site to schedule an appointment. The user's visited URL was sent alongside their personal identifiers, such as the "auid," via the Google Tag Manager, Google Analytics, and the DoubleClick Tracking Tools.*

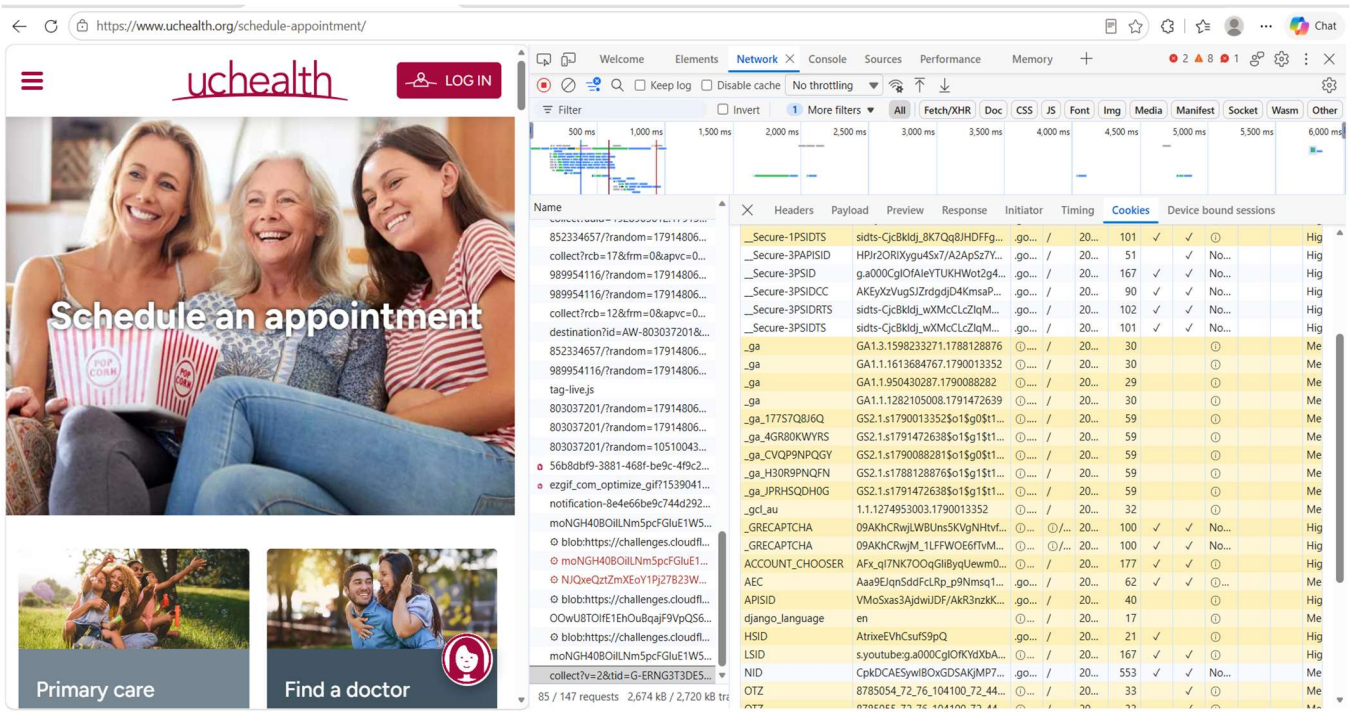


*Figure 3: Google Analytics deployed the cookies in white (not yellow-highlighted) on the scheduling webpage. The 3PAPISID, 3PSID, 3PSIDCC, 3PSIDRTS, 3PSIDTS, and NID cookies are depicted.*

72. As depicted above, Tracking Tools were configured in the Source Code of the Schedule an Appointment webpage. Review of the public-facing networking traffic revealed the presence of Google Tag Manager, Google Analytics, and DoubleClick Tracking Tools, all of which communicated a specific Google user's visit to the webpage.

73. This combination of information communicated that the specific user intends to schedule an appointment with UCHealth. In Figure 2 specifically, the user navigated to the "Schedule an Appointment" page from the "Billing and Pricing page," which Google can see from the "ref" tag (shown right under the highlighted "url" tag in Fig. 2 above). Google can also draw inferences from the webpages from which a user came.

**2. Finding a Doctor**

74. UCHealth has a repository of medical professionals labelled by specialty and

location that can be viewed through from the "Find a Doctor" webpage. Each doctor has their own webpage that communicates the doctor's name and explains their specialties and locations. For example, Dr. Kristine Erlandson appears as "kristine-erlandson-md" in her personal webpage URL, https://www.uchealth.org/provider/kristine-erlandson-md/.

75. Upon the user's navigation to a specific doctor's webpage, each of the Tracking Tools fired and transmitted POST Requests to Google that contained details about the page visited, alongside the user's personal Google identifier.

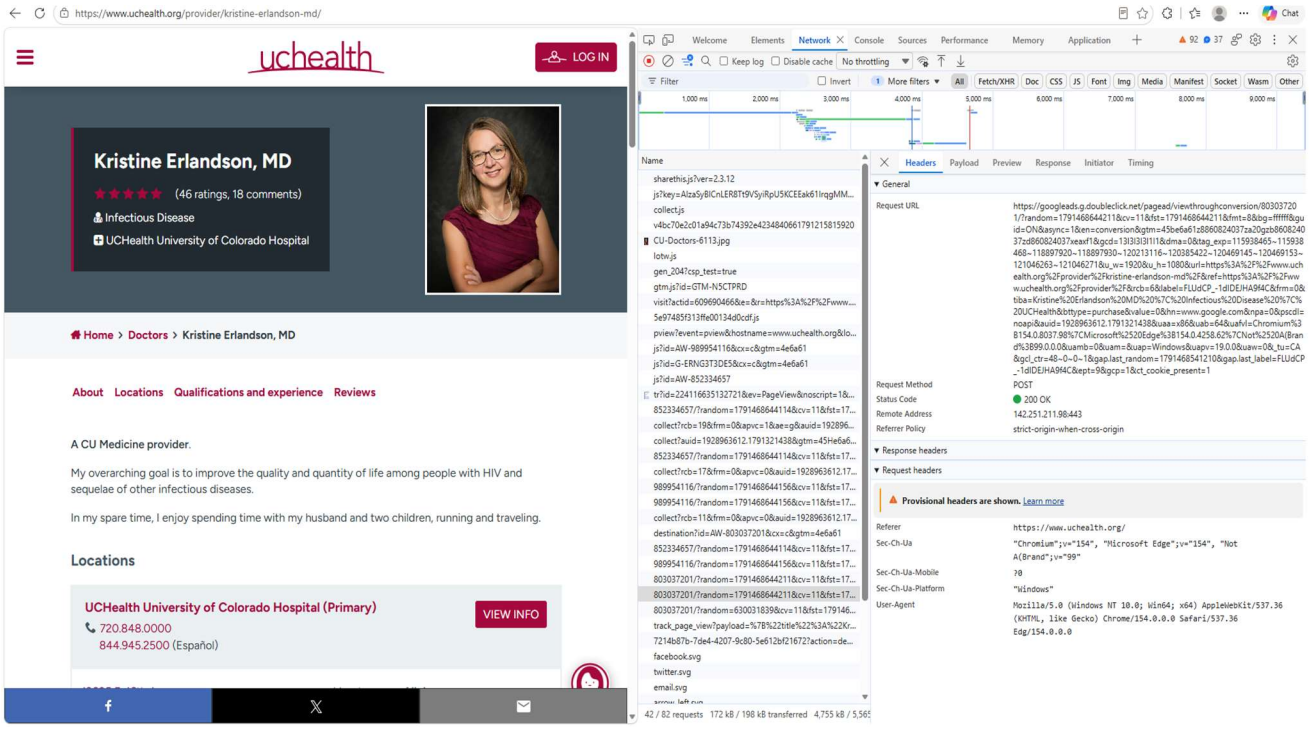


*Figure 4: Screenshot of network traffic taken from Defendant's website which shows that the Tracking Tools are actively installed and firing on Defendant's individual doctors' webpages.*

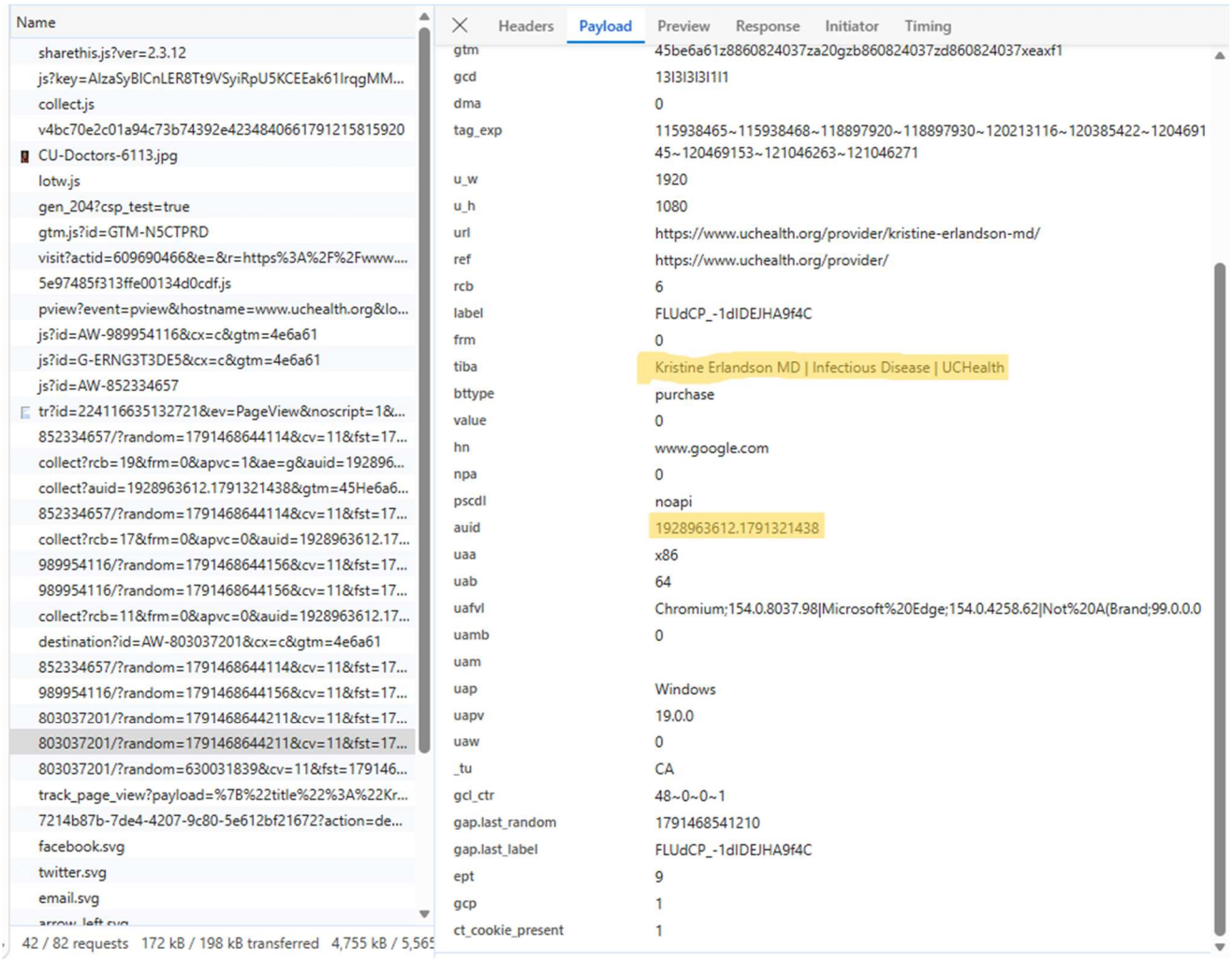


*Figure 5: The information sent to Google is parsed to reveal the user reviewed Dr. Kristine Erlandson, an infectious diseases specialist. The user's visited URL was sent alongside their personal identifiers, such as the "auid," via the Google Tag Manager, Google Analytics, and the DoubleClick Tracking Tools.*

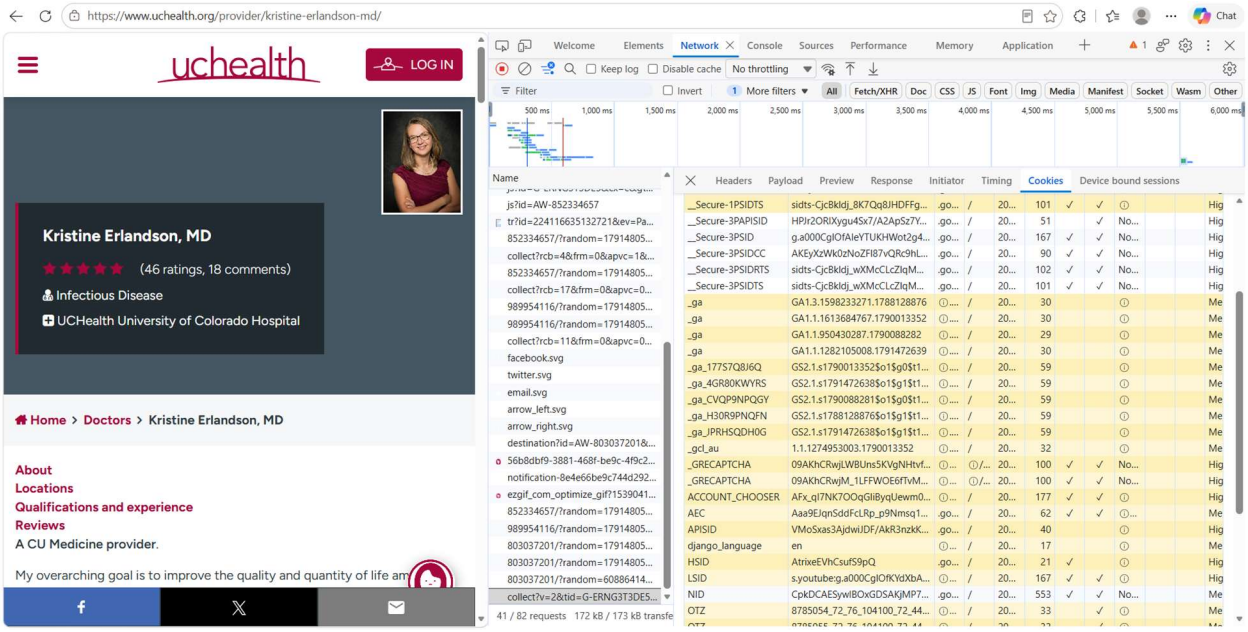


*Figure 6: Google Analytics deployed the cookies in white (not yellow-highlighted) on the doctor webpages. The 3PAPISID, 3PSID, 3PSIDCC, 3PSIDRTS, 3PSIDTS, and NID cookies are depicted.*

76. As depicted above, Tracking Tools were configured in the Source Code of the individual doctor webpages. Review of the public-facing networking traffic revealed the presence of Google Tag Manager, Google Analytics, and DoubleClick Tracking Tools, all of which communicated a specific Google user's visit to each webpage.

77. This combination of information communicated that the specific user reviewed Dr. Kristine Erlandson, an infectious disease specialist who publicly shares that her goal is to "improve the quality and quantity of life among people with HIV and sequelae of other infectious diseases." Google can infer that the user needs a specialist in infectious diseases like HIV, and that they can narrow the user's location based on the doctor's locations.

**3. Reviewing Conditions**

78. UCHealth also provides webpages where users can learn more about their conditions. As one navigates the conditions webpages, they can narrow their search to more

detailed descriptions of their conditions. For example, the "Gynecology" page hyperlinks the subpage "Infertility and Reproductive Care." The webpage on infertility reveals the user's visit to that webpage and condition. For example, the URL for the infertility page, https://www.uchealth.org/services/womens-care/infertility-reproductive-care/, contains "womens-care/infertility-reproductive-care."

79. Upon the user's navigation to a specific condition's webpage, each of the Tracking Tools fired and transmitted POST Requests to Google that contained details about the page visited, alongside the user's personal Google identifier.

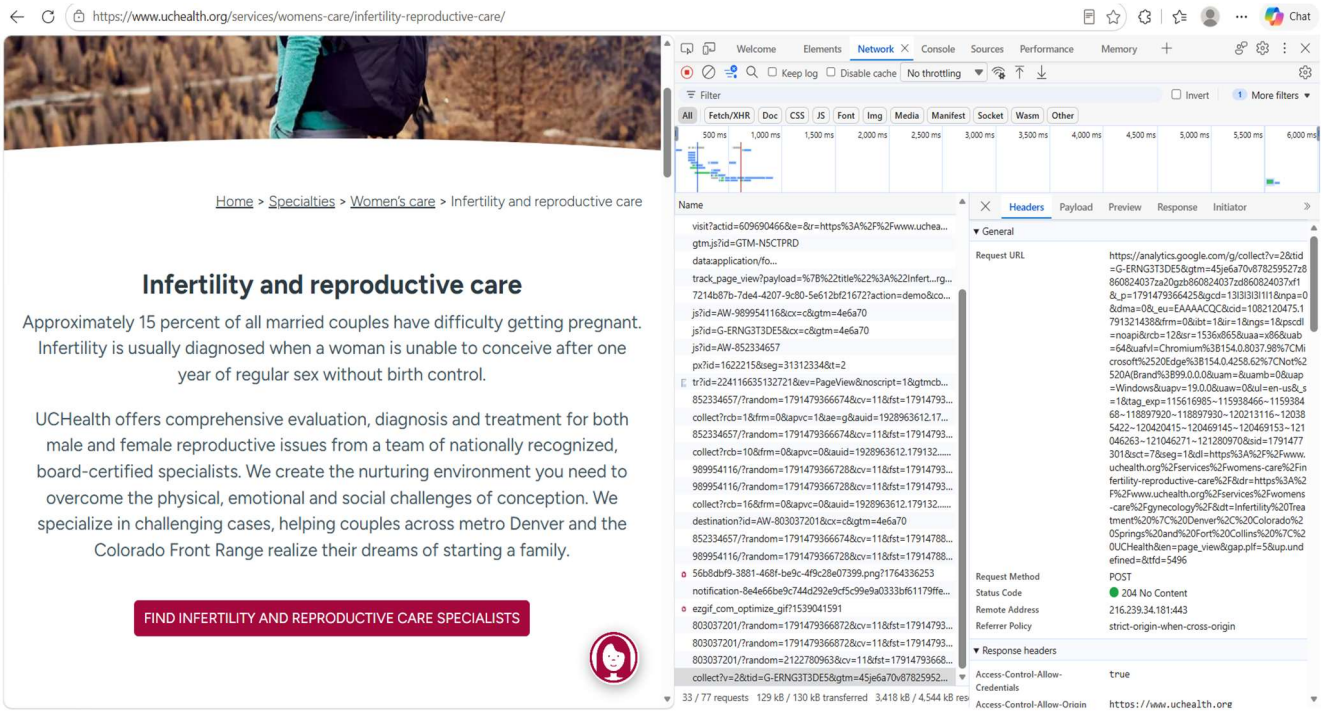


*Figure 7: Screenshot of network traffic taken from Defendant's website which shows that the Tracking Tools are actively installed and firing on Defendant's individual conditions' webpages.*

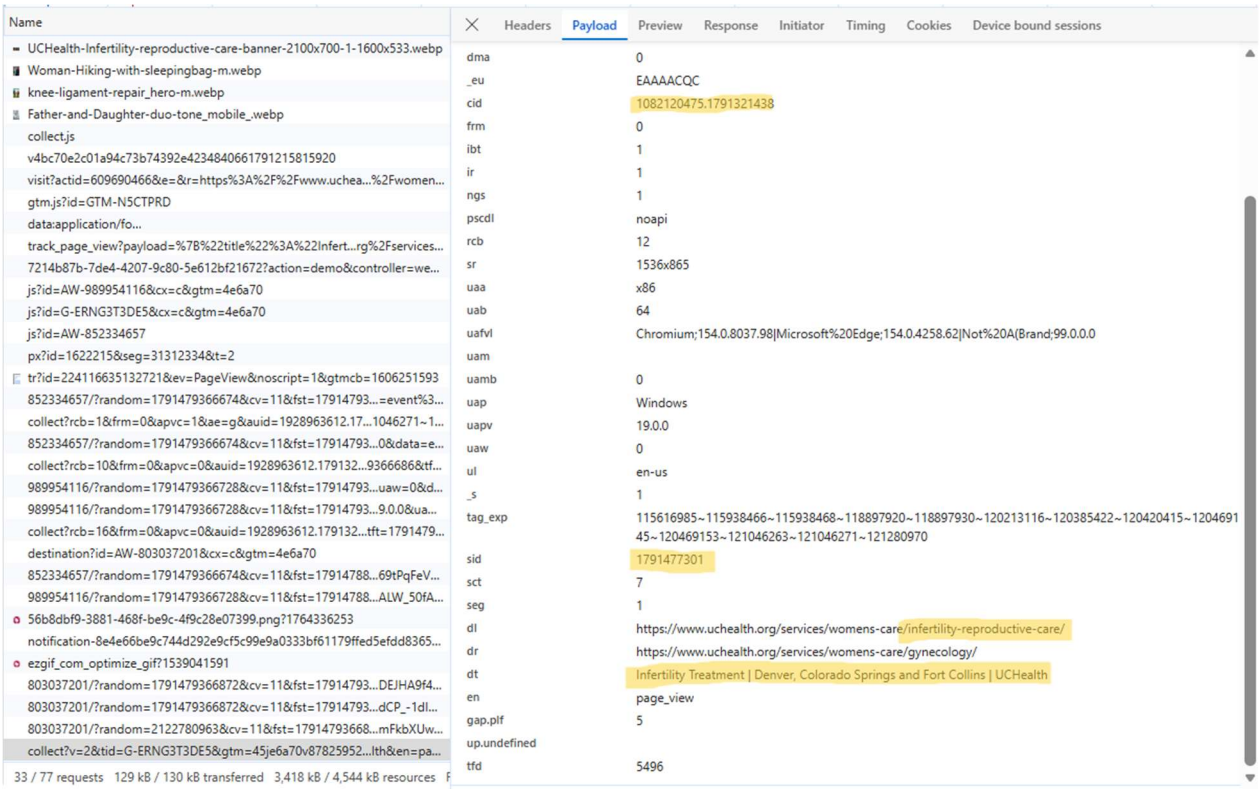


*Figure 8: The information sent to Google is parsed to reveal the user reviewed the infertility page. The user's page details sent alongside their personal identifiers, such as the "cid," via the Google Tag Manager, Google Analytics, and the DoubleClick Tracking Tools.*

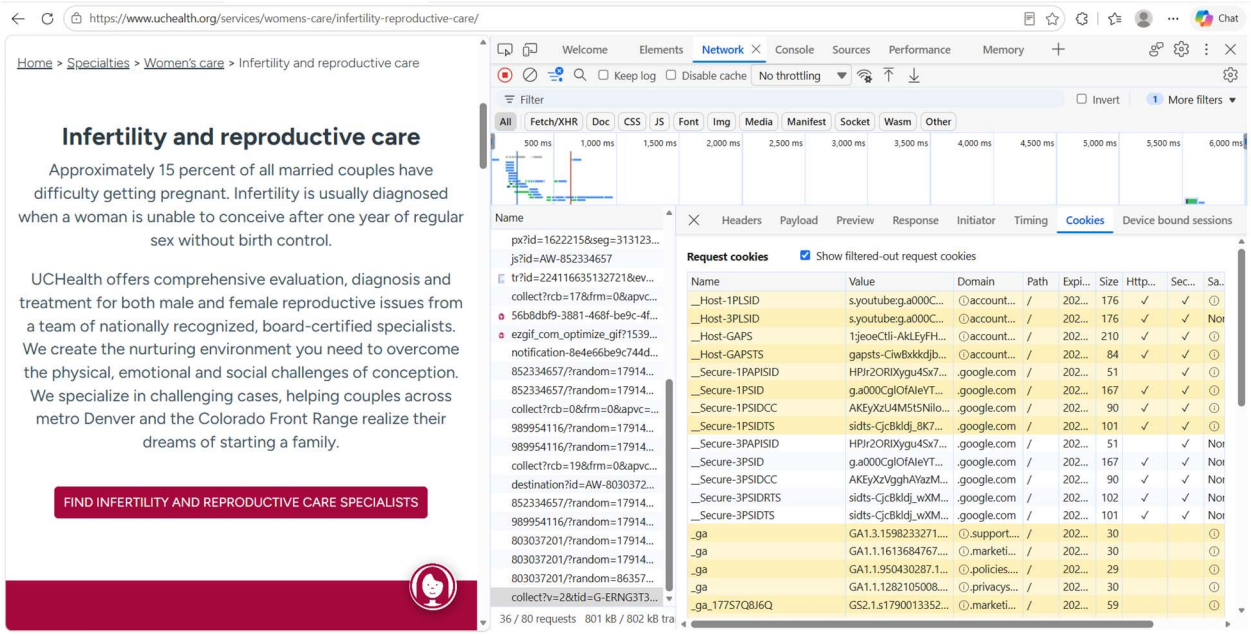


*Figure 9: Google Analytics deployed the cookies in white (not yellow-highlighted) on the conditions webpages. The 3PAPISID, 3PSID, 3PSIDCC, 3PSIDRTS, 3PSIDTS, and NID cookies are depicted.*

80. As depicted above, Tracking Tools were configured in the Source Code of the individual condition webpages. Review of the public-facing networking traffic revealed the presence of Google Tag Manager, Google Analytics, and DoubleClick Tracking Tools, all of which communicated a specific Google user's visit to each webpage.

81. The combination of information sent from the infertility page tells Google that the specific user has a condition or needs a certain treatment, such as female infertility care. When combined with the other webpages that a user might visit, Defendant enabled Google to draw highly sensitive, detailed conclusions about the user's medical conditions and patient status.

**4. Other Webpages**

82. The pre-suit investigation into Defendant's Website's networking traffic revealed that the Tracking Tools also fired on the following pages: the UCHealth "Events and Classes" webpages for accessing classes on specific conditions and health circumstances; the "Billing and Pricing" webpage and associated subpages; the "Virtual Urgent Care" webpage; the individual

health center location webpages; and more.

**E. Plaintiff Did Not Provide Consent or Authorization.**

83. Each of these web communications were disclosed without Plaintiff's or Class Members' express written consent and without a BAA between Defendant and Google.

84. The user is greeted with a cookie banner which is wholly insufficient to obtain the user's consent to Tracking Tools for several reasons. The cookie banner is permissive such that users need not accept cookies or otherwise interact with the banner in any capacity prior to using the website.

85. Tracking occurs by default such that, even in the absence of affirmative acceptance, the Tracking Tools are firing. This includes situations where the person simply closes the banner or otherwise ignores it entirely.

86. HHS issued guidance which explicitly states that: "Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do not constitute a valid HIPAA authorization."[2]

87. Moreover, as detailed above, cookies are not the only manner in which a user's confidential communications with Defendant are intercepted by third party tracking technologies like Google. Therefore, the existence of this banner is insufficient to obtain the user's consent to Tracking Tools as a whole.

88. Setting that aside, even if the cookie banner were sufficient, which it is not, Defendant still violated HIPAA because it has not executed BAAs with Google. As a result, these entities should never be receiving any PHI or PII from Defendant regardless of whether it is used

[2] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited August 11, 2026).

for marketing, analytics, or any other purpose.

89. Defendant did not properly ask users whether they consent to share their Private Information prior to sharing such information.

90. Related to cookie banners, Defendant's lackluster written policies did not disclose Defendant's wiretapping for multiple reasons. *First*, Defendant's privacy policies do not mention Google or any Unauthorized Third-Parties' collection of information through the Tracking Tools.

91. *Second*, Defendant's privacy policies do not mention the capturing of any data through deployment of the Tracking Tools.

92. *Third*, Defendant's policies remain threadbare, boilerplate, and uninformative such that no reasonable person would be notified that Tracking Tools operate on the Website.

93. *Finally*, if the practice of divulging Plaintiff's and Class Members' sensitive information could ever possibly fall under Defendant's policies, the clauses are inconspicuously hidden and buried in text, and the Website fails to provide an adequate cookie banner or notice of the existence of the clauses, such that Plaintiff and Class Members did not assent to its terms.

94. As such, users who interact with Defendant's Website and provide their PII, CHC, and PHI are not informed that Defendant will track and share their information and communications with third parties. And users, like Plaintiff and Class Members never agreed to any such Privacy Policy while using the website.

**F. The Data Broker Ecosystem.**

95. Data brokers obtain large volumes of consumer information without consumer knowledge to resell the data for marketing campaigns. The FTC has investigated the practices and found that "data brokers collect and store billions of data elements covering nearly every U.S.

consumer."[3]

96. Data brokers combine online and offline data to market to consumers online. Data brokers combine and analyze data about consumers to make inferences about them, including sensitive inferences related to health conditions. Some data brokers have been found to store data indefinitely posing significant privacy risks.[4]

97. Data brokers do not obtain the data directly from consumers, rather they obtain it through various sources including partnerships with third party marketers that utilize tracking tools. While each data broker source may provide only a few data elements about a consumer's activities a data broker can combine the data sets to form a more detailed profile of the consumer's life.

98. In fact, the unauthorized data collection from third party trackers, tags, and pixels has resulted in a proliferation and expansion of the data broker ecosystem. The web trackers serve as pivotal components in the data broker ecosystem by facilitating the collection of online activities, preferences, and demographics. This aggregated data is then analyzed and sold to various entities interested in understanding consumer behavior and targeting specific demographics.[5]

99. The U.S. data broker market is projected to grow from $280.82 billion in 2023 to $382.16 billion in 2030. This expansion is largely driven through the data harvested from the

---

[3] *FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information*, FTC (May 27, 2014), https://www.ftc.gov/news events/news/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more-transparent give-consumers-greater.

[4] *Id.*

[5] ONLINE DATA PRIVACY REPORT: WEBSITE PRIVACY AND COMPLIANCE CHALLENGES (Mar. 2024), https://lokker.com/api/directus-assets/419fdf43-83ba-4dba-9821-d8eff94f956a (last visited July 21, 2026).

pixels and trackers on the website.

100. As far as medical advertising, the data brokers routinely utilize the data sets to predict which consumers are most likely to use, e.g., brand name medicine, order prescriptions by mail, research medications online, or respond to pharmaceutical ads or other treatment advertisements. These predictive models are then sold and used for targeted advertising.

101. The lack of transparency in the data brokering ecosystem makes it impossible to be absolutely certain, without discovery, the ways that Google and Unauthorized Third-Parties sold or traded the data they received through the Tracking Tools at issue.

102. However, it is indisputable that the data at issue, given that it's medical data, is highly valuable for segmentation and profile building.

103. Once the data is shared and disclosed to any of the Unauthorized Third-Parties, the patients, Class Members, and Defendant lose control over its usage and distribution.

**G. Defendant Violated Healthcare Industry Norms.**

104. In January 2013, 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).

105. As part of that final rulemaking, which became effective on March 26, 2013, HHS stated that, to be considered 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*.

106. In December 2022, HHS issued a bulletin (the "HHS Bulletin") warning regulated entities like Defendant about the risks presented by the use of Tracking Tools 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.**[6]

107. In other words, HHS has expressly stated that entities like Defendant that implement Google Tracking Tools and disclose patient information have violated HIPAA Rules unless those entities obtain a HIPAA-compliant authorization.

108. The HHS Bulletin further warned 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.**[7]

109. Additionally, HHS has warned healthcare providers that Protected Information is not limited exclusively to patient portals, and thus Defendant still has an obligation to protect information on non-password protected (i.e., "unauthenticated") webpages. Citing to the 2013 Final Rulemaking, HHS observed that "information that connects the individual to a regulated

---

[6] *See* Archive: *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, HHS (Dec. 1, 2022), available at https://web.archive.org/web/20221201192812/https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited June 02, 2026) (emphasis added).

[7] *Id.*

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 an individual's past, present, or future health, health care, or payment for care."[8]

110. 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.**[9]

111. In addition, HHS and the FTC have recently issued a letter, once again admonishing entities like Defendant to stop using Tracking Tools:

> 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

[8] *Id.*

[9] *Id.* (emphasis added).

as constitute a breach of security under the FTC's Health Breach Notification Rule.[10]

## H. Defendant Violated the Law.

### 1. Defendant Violated HIPAA.

112. 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.

113. 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.[11]

114. The HIPAA Privacy Rule, located at 45 C.F.R. Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[12]

115. The Privacy Rule broadly defines PHI as individually identifiable health

---

[10] *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 02, 2026).

[11] HIPAA, 42 U.S.C. § 1320d-6; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

[12] HHS.gov, *The HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited Sept. 11, 2026).

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.

116. 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.

117. 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 serial numbers;

N. Web Universal Resource Locators (URLs);

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

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

118. The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514.

119. 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.

120. 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.

121. The U.S. Office of Legal Counsel considers a defendant to have "knowingly" violated HIPAA when the defendant broadly had "knowledge of the facts that constitute an offense."[13] The defendant does not need to specifically know that its acts were illegal.

122. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to

[13] *See Scope of Criminal Enforcement Under 42 U.S.C. § 1320D-6*, 29 U.S. OP. OFF. LEGAL COUNSEL 76 (June 1, 2005), 2005 WL 2488049, at *7.

Defendant when it is knowingly disclosing individually identifiable health information relating to an individual.

123. 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."

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

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[14]

125. In its guidance for Marketing, the HHS further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, *the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing*. … Simply put, a covered entity may not sell protected

[14] Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule at *5 (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Sept. 11, 2026).

> health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*.[15]

126. The Office for Civil Rights at HHS has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies, such as the Tracking Tools. The Bulletin expressly used to provide (in bold type) 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."[16] In other words, HHS had expressly stated that the manner of Defendant's implementation of Tracking Tools violates HIPAA Rules.[17]

---

[15] *Marketing*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (last visited Sept. 24, 2026) (emphasis added).

[16] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Sept. 22, 2026).

[17] This guidance was recently vacated in part by the Federal District Court for the Northern District of Texas due to the court finding it in part to be the product of improper rulemaking and it is cited for reference only until the OCR updates its guidance, should it do so in the future. *See Am. Hosp. Ass'n v. Becerra*, No. 4:23-cv-01110-P, ECF No. 67 (N.D. Tex. June 20, 2024). Notably, the court's order found only that the OCR's guidance regarding covered entities disclosing to third parties users' IP addresses while users navigated unauthenticated public webpages ("UPWs") was improper rulemaking. The Order in no way affects or undermines the OCR's guidance regarding covered entities disclosing personal identifiers, such as Google or Facebook identifiers, to third parties while patients were making appointments for particular conditions, paying medical bills or logging into (or using) a patient portal. *See id.* at 3-4, 31, n. 8 (vacating the OCR guidance with respect to the "Proscribed Combination" defined as "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers" but stating that "[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document."). Furthermore, the FTC bulletin on the same topics remains untouched, as do the FTC's enforcement actions against health care providers for committing the same actions alleged herein.

**2. Defendant Benefitted from Its Illegal Acts.**

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

128. 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 patients' data it obtained, procured, and/or disclosed in the absence of express written consent.

129. 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 benefiting Defendant while invading the privacy of Plaintiff and Class Members and violating their rights under federal and state law.

**3. Plaintiff Had a Reasonable Expectation of Privacy in Their Data.**

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

131. 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 Third-Parties for a commercial purpose unrelated to patient care.

132. Plaintiff and Class Members would not have used Defendant's Website, would not have provided their Private Information to Defendant, 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 Third-Parties.

133. The unauthorized transmissions of the patients' interactions with Defendant's

website are highly offensive to a reasonable person because the online communications are directly linked to their confidential PHI, and their online communications are undoubtedly being shared with Google.

**4. Plaintiff's and Class Members' Information Has Economic Value.**

134. Plaintiff's data and Private Information have economic value. For example, 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.

135. 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."[18] Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.[19]

136. 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.[20]

137. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-

[18] *See, e.g.*, Vahid, *Data Is the New Oil: A Powerful Metaphor with a Catch*, MEDIUM (May 23, 2026), https://medium.com/@vhid/data-is-the-new-oil-a-powerful-metaphor-with-a-catch-35899859bcb6 (last visited Aug. 11, 2026).

[19] *See* Robert J. Shapiro, *What Your Data Is Really Worth to Facebook*, WASHINGTON MONTHLY (July 12, 2019), https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/.

[20] *See How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, TIME (Jan. 9, 2017), https://time.com/4588104/medical-data-industry/ (last visited Sept. 21, 2026).

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."[21]

138. 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."[22]

139. There is also a market for data in which consumers can participate. 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. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

140. 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.

141. Facebook also has paid users for their digital information, including browsing history. Until 2019, Facebook ran a "Facebook Research" app through which it paid $20 a month

[21] *See Hospital Execs Say They Are Getting Flooded with Requests for Your Health Data*, CNBC (Dec. 18, 2019), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html?msockid=35128af7e8496ed33a159d44e9256f5b (last visited Sept. 21, 2026).

[22] Vero, *How To Collect Email Addresses On Twitter*, https://www.getvero.com/resources/twitter-lead-generation-cards/ (last visited Sept. 21, 2026).

for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

142. Moreover, health care data is extremely valuable to bad actors. Health care records may be valued at up to $250 per record on the black market.

143. Google's Tracking Tools are often offered for "free," when they are in fact a bartered exchange whereby Defendant gets access to low-cost advertising and related analytics services in exchange for its patients' private data.

**5. Medical Providers Owe Patients a Duty of Confidentiality**

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

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

146. The 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) . . . .[23]

147. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of a 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 to third parties 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

[23] AMA Code of Medical Ethics, *Opinion 3.1.1: Privacy in Health Care*, https://code-medical-ethics.ama-assn.org/ethics-opinions/privacy-health-care (last visited Oct. 7, 2026).

> 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 purpose(s) for which access would be granted.[24]

148. 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: … [r]elease patient information only in keeping with ethics guidance for confidentiality and privacy***.[25]

## I. Plaintiff's and Class Members Experiences.

### 1. Plaintiff Jacquelyn Anderson

149. Plaintiff Jacquelyn Anderson is a patient of Defendant and first started using the Website in 2015. She frequently uses the Website, and her last visit was in October 2026.

150. Plaintiff Anderson accessed Defendant's Website on both her Windows computer and her iPhone to help her find doctors, review pages dedicated to symptoms and conditions, book appointments, and make payments.

151. During all relevant times, Plaintiff Anderson has also had a Google account in which she was logged on her personal devices and believes that the Private Information she communicated via the Website was also transmitted to Google via Defendant's use of Tracking Tools on the Website. Plaintiff used those same devices to access Defendant's Website.

152. Upon information and belief, the Private Information that Google received from Defendant included specific facts concerning her medical condition and treatments, was personally

---

[24] AMA Code of Medical Ethics, *Opinion 3.2.4: Access to Medical Records by Data Collection Companies*, https://code-medical-ethics.ama-assn.org/ethics-opinions/access-medical-records-data-collection-companies (last visited Oct. 7, 2026).

[25] AMA Code of Medical Ethics, *Opinion 3.3.2: Confidentiality & Electronic Medical Records*, https://code-medical-ethics.ama-assn.org/ethics-opinions/confidentiality-electronic-medical-records (last visited Oct. 7, 2026).

identifiable (linked to Plaintiff), and was not anonymized or redacted.

153. Defendant intercepted and/or facilitated these interceptions without Plaintiff Anderson's knowledge, consent, or express written authorization.

154. As a patient, Plaintiff Anderson reasonably expected that her online communications with Defendant via the Website were solely between herself and Defendant and that Defendant would not transmit her Private Information to Google for marketing purposes.

155. When Plaintiff Anderson used the Website, her device identifiers and other personal identifiers were sent to Google alongside the substance of her communications.

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

157. Plaintiff 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 Plaintiff's medical conditions and other confidential information she communicated to Defendant via the Website.

158. Plaintiff has a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

## TOLLING

159. Any applicable statute of limitations has been tolled by the "delayed discovery" rule.

160. Shortly before this complaint was filed, Plaintiff, through the investigation of undersigned counsel, learned about Defendant's unlawful disclosure and transmission of her Private Information to third parties, such as Google, in the manner described herein.

161. Prior to that date, Plaintiff did not know (and had no way of knowing) that her

Private Information was intercepted and unlawfully disclosed to Google because Defendant kept this information secret and the Tracking Tools are invisible on the Website.

## CLASS ALLEGATIONS

162. 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.

163. The **Class** that Plaintiff seeks to represent is defined as follows:

> All UCHealth patients in the United States who had their Private Information shared with Unauthorized Third-Parties by communicating with Defendant via the Website.

164. Excluded from the Class are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, her or her spouse and immediate family members; and members of the judge's staff.

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

166. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Given the volume of Defendant's business, there are thousands of, if not much more, Class Members. The identities of Defendant's patients and Website visitors may be obtained from Defendant and the third parties to whom Defendant disclosed their information.

167. Commonality: This case presents common questions of law and fact, including but not limited to:

a. Whether Defendant's use of the Tracking Tools resulted in the interception of

Plaintiff's and Class Members' electronic communications in violation of the Electronic Communications Privacy Act;

b. Whether Defendant disclosed Plaintiff's and Class Members' Private Information to Google without consent;

c. Whether Defendant's conduct breached an implied contract with Plaintiff and Class Members;

d. Whether Defendant was unjustly enriched by its collection and disclosure of Plaintiff's and Class Members' Private Information;

e. Whether Defendant owed and breached a duty of care to Plaintiff and Class Members;

f. Whether Defendant invaded Plaintiff's and Class Members' reasonable expectation of privacy;

g. Whether Defendant breached its fiduciary duty and duty of confidentiality to Plaintiff and Class Members; and

h. Whether Plaintiff and Class Members are entitled to damages, restitution, and/or injunctive relief as a result of Defendant's conduct.

168. Typicality: Plaintiff's claims are typical of the claims of the Class because Plaintiff used Defendant's Website and had her personally identifiable information and protected health information disclosed to third parties such as Google without her express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class Members.

169. Adequacy: Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiff's interests are coincident with, and

not antagonistic to, those of the Class Members. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the Class Members.

170. 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. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

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

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

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

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

175. Unless a class-wide injunction is issued, Defendant may continue violating the privacy rights of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

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

177. Issue Certification: 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.

**COUNT I**
**VIOLATIONS OF THE 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)**

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

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

180. 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.

181. **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(12).

182. **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).

183. **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).

184. **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 patients' communications.

185. 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).

186. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via Tracking Tools, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to Unauthorized Third-Parties including Google.

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

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

189. 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).

190. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing criminal or tortious acts in violation of the Constitution or laws of the United States or of any State: namely, HIPAA (42 U.S.C. § 1320d-6) and invasion of privacy, among others. Thus, Defendant's simultaneous forwarding and interception of Plaintiff's and Class Members' Private Information does not satisfy the ECPA's party exemption.

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

a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and

b. Disclosed individually identifiable health information to Google without patient authorization.

192. Defendant intentionally used wire or electronic communications to increase its profit margins. 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.

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

194. Additionally, Colorado recognizes the tort of invasion of privacy. Defendant tortiously invaded Plaintiff's privacy, which constituted a knowing intrusion into a private place, conversation, or matter that would be highly offensive to a reasonable person. From that invasion, Defendant fails to meet the crime-tort exception because its conduct was tortious.

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

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

197. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was criminal, tortious, and designed to violate federal and state legal provisions. As a direct result of Defendant's violations, Plaintiff and Class Members are entitled to: (a) actual damages or statutory damages of $100 per day per violation or $10,000, whichever is greater; (b) punitive damages; and (c) reasonable attorneys' fees and costs under 18 U.S.C. § 2520.

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

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

199. As a condition of utilizing Defendant's digital platforms and receiving services from Defendant, Plaintiff and Class Members provided their Private Information and compensation for their medical care.

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

201. 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.

202. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to Unauthorized Third-Parties. 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 Private Information.

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

## COUNT III
## UNJUST ENRICHMENT
## (Alternative to Count II, On Behalf of Plaintiff and the Class)

204. Plaintiff repeats the allegations contained in all foregoing paragraphs as if fully set forth herein and brings this Count individually and on behalf of the proposed Class, except to the extent inconsistent with this Count. Pursuant to Federal Rule of Civil Procedure 8(d), Plaintiff asserts this Count for unjust enrichment in the alternative to Count II for breach of implied-in-fact contract, individually and on behalf of the proposed Class, in the event the Court determines that no enforceable contract governs the subject matter of the parties' dispute.

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

206. 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.

207. 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.

208. The financial 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 against equity and good conscience for Defendant to be permitted to retain any of the savings, profit or other financial benefits wrongly derived from the misappropriation and misuse of Plaintiff's and Class Members' Private Information as alleged in this Complaint.

209. 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.

210. Alternatively, Defendant should be compelled to provide restitution to Plaintiff and Class Members for the fair market value of the Private Information that Defendant misappropriated and misused for marketing purposes without consent.

211. Further, Plaintiff seeks injunctive relief to prevent the imminent financial and privacy harms arising from the ongoing disclosure, interception, and misuse of Plaintiff's and Class Members' Private Information.

## COUNT IV
## NEGLIGENCE
## (On behalf of Plaintiff and the Class)

212. Plaintiff repeats the allegations contained in all foregoing paragraphs as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

213. Defendant owed Plaintiff and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

214. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed the Tracking Tools to disclose and transmit to third parties

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

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

216. While Defendant intentionally implemented the Tracking Tools, Defendant failed to consider that the Tracking Tools were capable of collecting personally identifiable information that constituted personal health information.

217. It was highly foreseeable that one of the world's most sophisticated digital marketing companies would be able to connect the website data related to past, present, and future medical care with specific individuals.

218. Defendant was negligent in the following ways:

a. Failing to hire outside experts to review the marketing plan to ensure all identifiers were removed;

b. Failing to remove all identifiers as advised by HIPAA regulations;

c. Failing to test its marketing systems for level of entropy that could be used to identify individuals;

d. Failing to adequately train its digital marketing team on data privacy standards and policies;

e. Failing to recognize the connection between its targeted marketing campaigns an ecosystem capable of identifying individuals who visited the Website;

f. Being otherwise negligent.

219. As a direct and proximate result of Defendant's breach, Plaintiff and Class Members sustained numerous injuries including but not limited to the invasion of their privacy,

loss of control of their Private Information, misappropriation and misuse of their Private Information, breach of confidentiality, and the ongoing financial and privacy harms derived from the continued disclosure, interception, and misuse of their Private Information.

220. Consequently, Plaintiff, individually and on behalf of the putative Class seek legal and equitable remedies to address and rectify the negligence described herein including compensatory and consequential damages, loss of benefit of the bargain, conversion (FMV value of the use of the data for marketing), and in the alternative nominal damages. Plaintiff further seeks restitution and disgorgement of profits or cost savings obtained from the improper use of the Private Information. Finally, Plaintiff seeks injunctive relief to prevent the ongoing disclosure, interception, and continued misuse of the Private Information.

## COUNT V
## INVASION OF PRIVACY
## (On behalf of Plaintiff and the Class)

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

222. 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.

223. 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 third parties.

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

225. Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information to Google is highly offensive to a reasonable person.

226. 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.

227. 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.

228. 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 track and disseminate individuals' communications with the Website for the purpose of marketing and advertising.

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

230. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and the Class Members were disclosed to a third party without authorization, causing Plaintiff and Class Members to suffer damages.

231. 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.

232. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members 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.

233. 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. A judgment for monetary damages will not undo Defendant's disclosure of the information to Google, which upon information and belief, continues to possess and utilize that information.

234. 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 VI
## BREACH OF FIDUCIARY DUTY
## (On behalf of Plaintiff and the Class)

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

236. Medical providers have a duty of confidentiality 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.

237. As a fiduciary of the Private Information and medical provider, Defendant further owed Plaintiff and Class Members a duty of loyalty that precluded the misuse and misappropriation of Plaintiff's and Class Members Private Information.

238. 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; and (2) to only use the information for the authorized purpose.

239. Plaintiff and Class Members had reasonable expectations of privacy in their Private Information and the related confidential communications exchanged with Defendant through the Website.

240. Plaintiff and Class Members also reasonably expected that their Private Information would only be utilized for medical purposes.

241. Plaintiff and Class Members did not provide consent for Defendant to appropriate or use their Private Information for commercial and digital marketing purposes.

242. Contrary to its duties as a fiduciary and medical provider and its express and implied promises of confidentiality, Defendant installed Tracking Tools with the intent and purpose to disclose and transmit Plaintiff's and Class Members' Private Information to Google.

243. 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 with the purpose of marketing for new patients. Alternatively, the disclosures of Plaintiff's and Class Members' Private Information occurred because of Defendant's negligent hiring or supervision of its employees, its failure to establish adequate policies and procedures to safeguard the confidentiality of patient information, or its failure to train its employees to properly discharge their duties under existing privacy policies and procedures.

244. Defendant's breaches of their fiduciary duties, and their implied covenants of trust, loyalty, and confidence are evidenced by its failure to comply with federal and state privacy regulations, including:

a. 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. 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. 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. Failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiff's and Class Members PHI;

e. Impermissibly and improperly using and disclosing PHI for marketing in violation of 45 C.F.R. § 164.502, *et seq.*;

f. Failing to hire an expert to review the risk of data sets for re-identification and further failing to remove all digital identifiers from the data sets before disclosing the Private Information.

g. Failing to effectively train all members of its workforce, namely its digital marketing department and regulatory department on the policies and procedures with respect to PHI as necessary and appropriate for the members of its staff to carry out their responsibilities to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);

h. By otherwise failing to safeguard Plaintiff's and Class Members' Private Information; and

i. By otherwise misusing and unjustly profiting from Plaintiff's and Class Member's Private Information.

245. As a direct and proximate result of Defendant's breach of fiduciary duty and confidentiality, Plaintiff and Class Members have suffered numerous harms and injuries, including invasion of privacy, loss of control of their Private Information, misappropriation of their Private Information, conversion of their Private Information, and the ongoing invasion of privacy and financial harm derived from the continued disclosure, interception, and misuse of their Private Information.

246. Consequently, Plaintiff individually and on behalf of the putative Class, seeks the following damages: compensatory, loss of benefit of the bargain, conversion (FMV value of the use of the data for marketing), and in the alternative, nominal. Plaintiff further seeks restitution, disgorgement of profits or cost savings obtained from the improper use of the Private Information. Finally, Plaintiff seeks injunctive relief to address the ongoing breach of the fiduciary duty and financial and privacy harms derived from the continued disclosure, interception, and misuse of their Private Information.

## PRAYER FOR RELIEF

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

1. For an Order certifying the Class and appointing Plaintiff and Counsel to represent such Class;
2. For an award of damages, including, but not limited to, past and future compensatory, actual, consequential, statutory, and nominal damages, as allowed by law in an amount to be determined;
3. For equitable relief in the form of restitution and disgorgement of profits;
4. For injunctive relief requested by Plaintiff, including, but not limited to:
    a. Removal of the Tracking Tools from sensitive parts of the Website;
    b. Deletion of all analytics data collected through the Tracking Tools;
    c. Deletion of Plaintiff's and Class Member data from all identifiable third-party broker lists;
    d. Enjoinment from utilizing any of the Tracking Tools at issue in this matter in the future;
    e. Enjoinment from utilizing any other Tracking Tools or marketing services without first obtaining HIPAA compliance patients' consent and BAA agreements with the third parties; and
    f. Other injunctive relief as ordered by the Court.
5. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
6. For prejudgment interest on all amounts awarded; and
7. 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.

Dated: November 18, 2026

Respectfully submitted,

By:*/s/ Carolyn Cuneo*
Carolyn Cuneo (CO Bar No. 52041)
**MILBERG, PLLC**
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (866) 252-0878
cjcuneo@milberg.com

***Counsel for Plaintiff and the Putative Class***