

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JANE DOE, on behalf of herself and
allothers similarly situated,

Plaintiff,

v.

CRH HEALTHCARE, LLC d/b/a
PEACHTREE IMMEDIATE CARE;
PEACHTREE IMMEDIATE CARE UC,
LLC; PEACHTREE IMMEDIATE
CARE FP, LLC; and CRH GEORGIA,
LLC;

Defendants.

Civil Action No. 1:25-cv-06353-
TWT

**FIRST AMENDED CLASS
ACTION COMPLAINT**

JURY TRIAL DEMANDED

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Jane Doe¹ (“Plaintiff”) brings this class action against Defendants CRH Healthcare, LLC d/b/a Peachtree Immediate Care; Peachtree Immediate Care UC, LLC; Peachtree Immediate Care FP, LLC; and CRH Georgia, LLC (collectively, “Defendants”) in her individual capacity and on behalf of all others similarly situated, and alleges the following.

¹ To avoid further injury and damages to Plaintiff relating to the disclosure of her confidential and highly sensitive PII and PHI by Defendants, Plaintiff will move the Court for permission to proceed anonymously. *See Doe v. Archdiocese of Atlanta*, 328 Ga. App. 324, n. 20, 761 S.E.2d 864, 869 (2014).

NATURE OF THE ACTION

1. Plaintiff brings this case individually and on behalf of other similarly-situated patients (collectively, “Class Members”) to address Defendants’ illegal and widespread practice of disclosing patients’ confidential information including protected health information (“PHI”) (collectively referred to as “Private Information”) to Alphabet Inc. d/b/a Google (“Google”).

2. Defendants own and control its website <https://www.peachtreemed.com/> (collectively, the “Website”) and encourage and/or require patients to use the Website to, among other things, book medical appointments, locate treatment facilities, pay bills, search medical specialties and treatment options, obtain telehealth services, and more.

3. Defendants installed Google tracking and data collection tools on the Website to share patients’ PII and PHI with Google and other unauthorized third parties in violation of federal and state laws (the “Google Collection Tools”).

4. Despite Defendants’ express promise to patients that Defendants “will not disclose your PHI other than with a written authorization from you or your personal representative,”² Defendants used

² See <https://www.peachtreemed.com/privacy-notice/> (last visited Oct. 15, 2025).

the Google Collection Tools to divulge patients' Private Information for marketing and analytic purposes.

5. Information about a person's physical and mental health is among the most confidential and sensitive information in our society. In fact, to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "HIPAA Privacy Rule") governing how health care providers must safeguard and protect Private Information.

6. Under the HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

7. HHS has further issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("Regulated Entities"), including Defendants, under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies. The Bulletin expressly provides that Regulated 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.

8. Healthcare patients do not anticipate that their trusted healthcare provider will send their Private Information collected via its webpages to a hidden third party without the patients' consent. Neither Plaintiff nor any other Class Member signed a written authorization permitting Defendants to send their Private Information to Google.

9. Plaintiff's reason for her appointment ("new illness/infection"), along with the selection each Class Members made for their appointments, the selected locations, and details about patients' URL navigations were disclosed to Google because of Defendants' use of the Google Collection Tools.

10. Defendants created a confidential physician-patient relationship with Plaintiff and Class Members by holding themselves out as medical providers, collecting Private Information for the purpose of diagnosis and treatment, and facilitating appointments with licensed medical practitioners, thereby giving rise to duties of confidentiality, trust and loyalty inherent in the physician-patient relationship.

11. Defendants breached their statutory and common law obligations to Plaintiff and Class Members by failing to adequately review their marketing programs and web-based technology to ensure the Website was safe and secure; failing to remove or disengage technology that was known and designed to share web-users' information; failing to obtain the written consent of Plaintiff and Class Members to disclose their Private

Information to Google; and otherwise failing to design and monitor the Website to maintain the confidentiality and integrity of patients' Private Information.

12. As a result of Defendants' conduct as set forth herein, Plaintiff and Class Members have suffered injuries including invasion of privacy, statutory damages, and the continued and ongoing risk to their Private Information.

13. Plaintiff seeks to remedy these harms in this action and brings causes of action against Defendants for: (1) negligence and negligence per se; (2) breach of fiduciary duty; (3) breach of implied contract; (4) breach of express contract; (5) unjust enrichment; and (6) violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(1), *et seq.*

PARTIES

14. Plaintiff Jane Doe is a natural person and citizen of Georgia and a resident of Fulton County, Georgia.

15. On multiple occasions in the past two years, Plaintiff accessed Defendants' Website to search for locations of facilities, schedule appointments and procedures, and review and pay medical bills.

16. On or around August 9, 2024, Plaintiff, seeking confidential treatment for a urinary tract infection, scheduled an appointment at the Sharpsburg location of Peachtree Immediate Care on Defendants' website. In order to book the appointment, Plaintiff was required to provide

extensive personal and medical information, including selecting “new illness/infection” as her stated reason for seeking care and submitting identifying and details such as her full name, date of birth, sex assigned at birth, telephone number, and email address.

17. Plaintiff has a Google account.

18. Plaintiff reasonably expected that her online communications and disclosures with Defendants were solely between herself and Defendants and that such communications and disclosures would not be transmitted to or disclosed to a third party, including Google.

19. Plaintiff never consented to Defendants’ transfer of her Private Information to third parties or for Defendants to enabling third parties, including Google, to access or interpret her Private Information.

20. Defendant CRH Healthcare, LLC is a Delaware limited liability company with its principal place of business is in Atlanta, Georgia.

21. Defendant CRH Healthcare, LLC does business as Peachtree Immediate Care, which operates over 70 urgent care centers throughout Georgia and is the largest urgent care network in Georgia.

22. Defendant CRH Georgia, LLC is a Delaware limited liability company with its principal place of business in Atlanta, Georgia.

23. Defendant Peachtree Immediate Care UC, LLC is a Georgia limited liability company with its principal place of business in Atlanta, Georgia.

24. Defendant Peachtree Immediate Care FP, LLC is a Georgia limited liability company with its principal place of business in Atlanta, Georgia.

25. Upon information and belief, Defendants CRH Georgia, LLC, Peachtree Immediate Care UC, LLC, and Peachtree Immediate Care FP, LLC are subsidiaries of Defendant CRH Healthcare, LLC and are jointly responsible for the operation of the Peachtree Immediate Care business, including all matters relating to the Website.

26. As healthcare providers, Defendants are Regulated Entities under HIPAA.

JURISDICTION AND VENUE

27. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges questions of federal law under the ECPA (18 U.S.C. § 2510, *et seq.*).

28. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from at least one Defendant.

29. This Court has personal jurisdiction over Defendants because they are headquartered or principally operate in this District and the acts

and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

30. Venue is proper under 28 U.S.C. § 1391(b)(1) and (b)(2) because Defendants reside in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

31. Defendants use their Website to connect Plaintiff and Class Members to Defendants' digital healthcare platforms with the goal of increasing profitability.

32. In furtherance of that goal, and to increase the success of their advertising and marketing, Defendants purposely installed the Google Collection Tools to its webpages within the Website.

33. In doing so, Defendants shared patients' private and protected communications with Google, including communications that contain Plaintiff's and Class Members' Private Information. These private communications include users' PHI.

34. PHI is "individually identifiable health information" transmitted by or maintained in "electronic media" or "any other form or medium." Individually identifiable health information (IIHI) is "information that is a subset of health information, including demographic information collected from an individual" that (1) "[i]s created or received by a health care provider; (2) "[r]elates to the past, present, or future . . . health or

condition of an individual” or “the provision of health care to an individual”; and (3) “[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.”

35. As set forth herein, Defendants intentionally configured the Google Collection Tools installed on the Website to capture both the “characteristics” of individual patients’ communications with the Defendants’ Website (e.g., their IP addresses, cookie identifiers, device identifiers and account numbers) and the “content” of these communications (i.e., the buttons, links, pages and tabs they click and view) such that Google can use the information transmitted by the Collection Tools to identify the website user involved.

36. Defendants used Google Collection Tools to convey sensitive patient information to third parties, including, for example, information patients typed into registration and appointment forms, the reason for an appointment, the location of an appointment, and descriptive URLs detailing where patients navigated within the Website.

37. To better understand Defendants’ unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows.

I. Google Analytics.

38. Google Analytics is designed to capture and transmit a wide range of user interactions, including page views, search queries, button

clicks, form submissions, transaction details, and error events, providing Defendants with real-time reporting on patient activity.

39. By default, Google Analytics collects IP addresses, device/browser identifiers, and referral URLs, linking these with specific actions taken on the site. It further records acquisition data, showing whether a patient arrived via search, referral, or advertising, and engagement data, including the pages viewed, forms completed, and time spent on sensitive treatment-related pages.

40. Google Analytics applies machine learning models to predict user behavior, such as the likelihood of completing an appointment request or abandoning a scheduling flow. Defendants' implementation therefore enabled the generation of predictive audiences tied to patients' healthcare interactions.

41. The platform integrates with Google Ads, Display & Video 360, and Search Ads 360, allowing data collected from Defendants' healthcare website to be combined with Google's advertising systems for retargeting, attribution, and cross-platform campaign optimization.

42. Google Analytics also enables conversion paths and attribution modeling, showing the steps patients took on Defendants' site before booking an appointment. This allows Google to evaluate the contribution of each click, referral, or ad impression in leading to a conversion, thereby exposing sensitive health-related pathways to external analysis.

43. Google Analytics uses cookies to track users across sessions and devices. The primary cookie used by Google Analytics is the “_ga” cookie, which contains a unique client identifier used to distinguish users. This cookie persists and is used to calculate visitor, session, and campaign data for Google Analytics reports.

44. Google Analytics also uses the “_gid” cookie, which stores information about how visitors use the Website and helps create analytics reports. The “_gid” cookie is set when a user visits the Website.

45. Additionally, Google Analytics uses the “_gat” cookie to throttle the request rate and limit the collection of data on high-traffic sites.

II. Google DoubleClick

46. Google DoubleClick is Google’s advertising technology platform that enables advertisers to manage, deliver, and measure digital advertising campaigns. DoubleClick uses tracking pixels and cookies to collect information about users’ browsing behavior across websites.

47. When a user visits a website that has DoubleClick tracking code installed, such as Defendants’ Website, DoubleClick drops cookies on the user's browser to track their activity. These cookies allow DoubleClick to identify and track individual users as they move across different websites, building detailed profiles of their interests, behaviors, and demographics.

48. DoubleClick then uses this information to enable targeted advertising, allowing advertisers like Defendants to display ads to users

based on their browsing history and inferred interests, including their visits to healthcare websites and the specific medical information they sought.

49. In other words, by employing DoubleClick to analyze patients' activity on the Website, Defendants could better target patients with ads based on their online behavior.

50. For example, if a patient searched for a specific medical condition on the Website (e.g., articles about stress), DoubleClick could transmit that information to Defendants (including the URL involved, such as <https://www.peachtreemed.com/md-insights-stress/>) and link the information to the patient's Google account, allowing Defendants to later target that patient with specific ads related to his or her previous search. Further, if that user clicked on the button to find therapy options for stress management, the Google Collection Tools would transmit to Google that the user visited <https://www.peachtreemed.com/therapy/> through a link on the <https://www.peachtreemed.com/md-insights-stress/> page, which would allow Google to retarget this user for stress management and therapy to manage it.

51. The DoubleClick technology integrates seamlessly with Google Analytics, allowing Defendants to combine first-party data from their Website with DoubleClick's third-party advertising data to create comprehensive user profiles and implement sophisticated retargeting campaigns.

52. In exchange for disclosing the Private Information of its patients, Defendants are compensated by Google in the form of enhanced advertising services and more cost-efficient marketing.

III. Google's Use of IDE and NID Cookies to Identify Users.

53. By choosing to install the Google Collection Tools tool on their Website, Defendants ensured that patients' activity on the Website was contemporaneously redirected to Google.

54. This information includes, but is not limited to, when a patient scheduled an appointment; information that a patient typed into an appointment form; the reason the patient is seeking the appointment (e.g., a drug test); the location of the appointment; when a patient clicked a button to call their provider from Defendants' website; descriptive URLs detailing where patients navigated within the Website; the nature of patients' clicks on categories within the Website; and similar communications.

55. Google uses specific cookies to identify and track users across its advertising network and services. Two critical cookies used by Google are the IDE cookie and the NID cookie, both of which enable Google to personally identify individual users and link their activities across different websites and services.

56. The IDE cookie is set by Google DoubleClick and stored under the domain doubleclick.net. The IDE cookie contains a unique identifier that

Google DoubleClick uses to track users across websites that have implemented Google advertising services.

57. When a user visits Defendants' Website with DoubleClick tracking code installed, the IDE cookie is either set on the user's browser (if not already present) or read from the user's browser (if previously set by visiting another website with DoubleClick tracking). This cookie allows Google to recognize that same user across multiple websites and track their browsing behavior over time.

58. The IDE cookie enables Google to build comprehensive profiles of users' interests, behaviors, and demographics based on their activities across all websites in Google's advertising network.

59. When Defendants transmit patients' Private Information to Google through the Google Collection Tools, Google can associate that health information with the specific individual identified by their IDE cookie value.

60. The NID cookie is set by Google and stored under the domain google.com. The NID cookie contains a unique identifier that Google uses to remember users' preferences and other information, such as their preferred language, their search history, and their interactions with Google services.

61. Google uses the NID cookie primarily for customizing search results and advertisements on Google properties. The NID cookie is updated each time a user interacts with Google services.

62. When a user who has previously used Google services visits Defendants' Website, the NID cookie allows Google to identify that user and link their activities on Defendants' Website with their Google profile and search history. This creates a direct connection between the user's identity, their Google activities, and the Private Information disclosed by Defendants.

63. The IDE and NID cookies are "third-party cookies," meaning they are set by a domain other than the website the user is visiting.

64. Google tracks and stores every IDE cookie value and NID cookie value associated with each user. Google maintains records linking these cookie values to specific user accounts, IP addresses, device identifiers, and other personal identification information.

65. Through the IDE and NID cookies, Google can determine with precision which specific individual accessed Defendants' Website, what medical information they sought, what appointments they scheduled, what treatments they researched, and what health conditions they have. This information is then associated with that individual's broader Google profile, which may include their name, email address, physical address, phone number, and comprehensive browsing history.

66. Discovery in cases against Google, including *Calhoun v. Google* and *In re Google RTB Consumer Privacy Litigation*,³ which have been made public, have shown that Google can identify users based on the IDE cookie, the NID cookie, and users' Client ID or "cid." The Client ID is a parameter in the URL string in the Google Analytics query string called "cid."

67. Internally, Google refers to the IDE cookie as "Biscotti," the NID cookie as "Zwieback," and the Google User ID as "GAIA." Documents found in the *Calhoun* case revealed that Google internally maps the Client ID to the Biscotti ID, the Zwieback ID, and the GAIA ID.⁴ Thus, Google can trace a transmission from Google Analytics or DoubleClick to an individual person who uses Google.

68. Because Google has the ability to trace a transmission from Google Analytics or DoubleClick to an individual person, these transmissions are PHI when they relate to the past, present, or future health condition of an individual or the provision of health care to an individual.

³ *Calhoun v. Google*, N.D. Cal., No. 20-cv-05146; *In re Google RTB Consumer Privacy Litigation*, N.D. Cal., No. 21-cv-02155. Discovery from Google and expert reports from Professor Zubair Shafiq explaining those documents were used by Plaintiffs in both cases.

⁴ *Calhoun v. Google*, N.D. Cal., No. 20-cv-05146, Dkt. No. 551-3, Ex. EEE, Rebuttal Report of Professor Zubair Shafiq, pp. 149-150 of 435; Dkt. 730-3, Zubair Decl., pp. 4-5 (explaining how Google internally names identifiers and to which cookies/information those identifiers correspond).

69. When Plaintiff and Class Members visited Defendants' Website, they did not consent to third-party cookies being placed on their browsers to track their medical activities and link that information to their personal identities through Google's advertising network.

70. Google uses the IDE and NID cookies in combination with other identifiers, including IP addresses and device fingerprints, to create persistent user profiles that follow individuals across devices and over time. Even if a user clears their cookies or uses a different device, Google can often re-identify them through cross-device tracking techniques that analyze behavioral patterns and associated account information.

71. By installing Google Analytics and DoubleClick tracking code on the Website, Defendants enabled Google to drop the IDE and NID cookies on Plaintiff's and Class Members' browsers, thereby allowing Google to identify them personally, track their medical activities on the Website, and link that sensitive health information to their persistent Google profiles.

72. The information transmitted alongside the IDE and NID cookies included the specific webpages Plaintiff and Class Members visited on Defendants' Website, the buttons they clicked, the forms they filled out, the medical conditions they searched for, the physicians they sought to contact, and the appointments they scheduled. All of this Private Information was transmitted to Google with the unique identifiers

contained in the IDE and NID cookies, allowing Google to know precisely which individual was seeking which type of medical care.

73. Google uses the data collected through the IDE and NID cookies, including the Private Information disclosed by Defendants, for multiple commercial purposes, including: (a) building detailed user profiles for targeted advertising; (b) measuring advertising campaign effectiveness; (c) selling audience segments to advertisers; (d) improving Google's machine learning algorithms; and (e) enhancing Google's competitive position in the digital advertising market.

74. The combination of Google Analytics, DoubleClick tracking, and the IDE and NID cookies creates a comprehensive surveillance system that follows users across the internet, collecting and aggregating data about their most private activities, including their healthcare needs and medical conditions, all without meaningful notice or consent.

IV. Defendants' Methods of Transmitting Plaintiffs and Class Members' Private Information to Unauthorized Third-Parties.

75. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser.

76. Every website is hosted by a computer server that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

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

78. When an individual visits Defendants' Website, an HTTP Request is sent from that individual's web browser to Defendants' servers. The HTTP Response from Defendants' servers sends the requested information in the form of "Markup," which is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen.

79. Every website is comprised of Markup and "Source Code." Source Code is a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code. These Markup and Source Code files are often downloaded by the users' browsers and stored in temporary storage called cache.⁵

80. Google tracking pixels embedded in Defendants' Source Code act like a traditional wiretap. When patients visit Defendants' Website,

⁵ Cloudflare, "What is caching?", <https://www.cloudflare.com/learning/cdn/what-is-caching/> ("Every time a user loads a webpage, their browser has to download quite a lot of data in order to display that webpage. To shorten page load times, browsers cache most of the content that appears on the webpage, saving a copy of the webpage's content on the device's hard drive.") (last accessed October 31, 2025).

Defendants' server sends an HTTP Response including the Source Code that contains the Google tracking pixels. Once the Webpage loads in the patient's browser, the software-based wiretap quietly waits for a communication from the patient to trigger the tap, which intercepts those communications intended only for Defendants and transmits them to Google.

81. The tracking pixels work with the IDE and NID cookies and the Client ID to track and gather all the information from users. When a patient's browser executes the tracking pixel code, it automatically reads any Google cookies present on the browser, including the IDE and NID cookies, and transmits those cookie values to Google along with the patient's Private Information.

82. Thus, without any knowledge, authorization, or action by a user, Defendants use their source code to commandeer patients' computing devices, causing the device's web browser to contemporaneously and invisibly re-direct the patients' communications to Google, along with the IDE and NID cookie values that allow Google to identify precisely which individual is communicating that Private Information.

V. Defendants Disclosed Plaintiff's and Class Members' Private Information to Google Without Authorization or Consent.

83. Defendants utilize Google Collection Tools and intentionally installed tracking pixels on their Website and servers to secretly track patients by recording their activity in violation of their common law, contractual, statutory, and regulatory duties and obligations.

84. While seeking and using Defendants' services as a medical provider, Plaintiff and Class Members communicated their Private Information, including name, phone number, email, and reason for requesting the visit to Defendants via the Website. Defendants then relayed that information to Google via the Google Collection Tools. Examples of this can be seen below, where Defendants share with Google a user's request for an appointment for a drug screening at one of Defendants' locations:

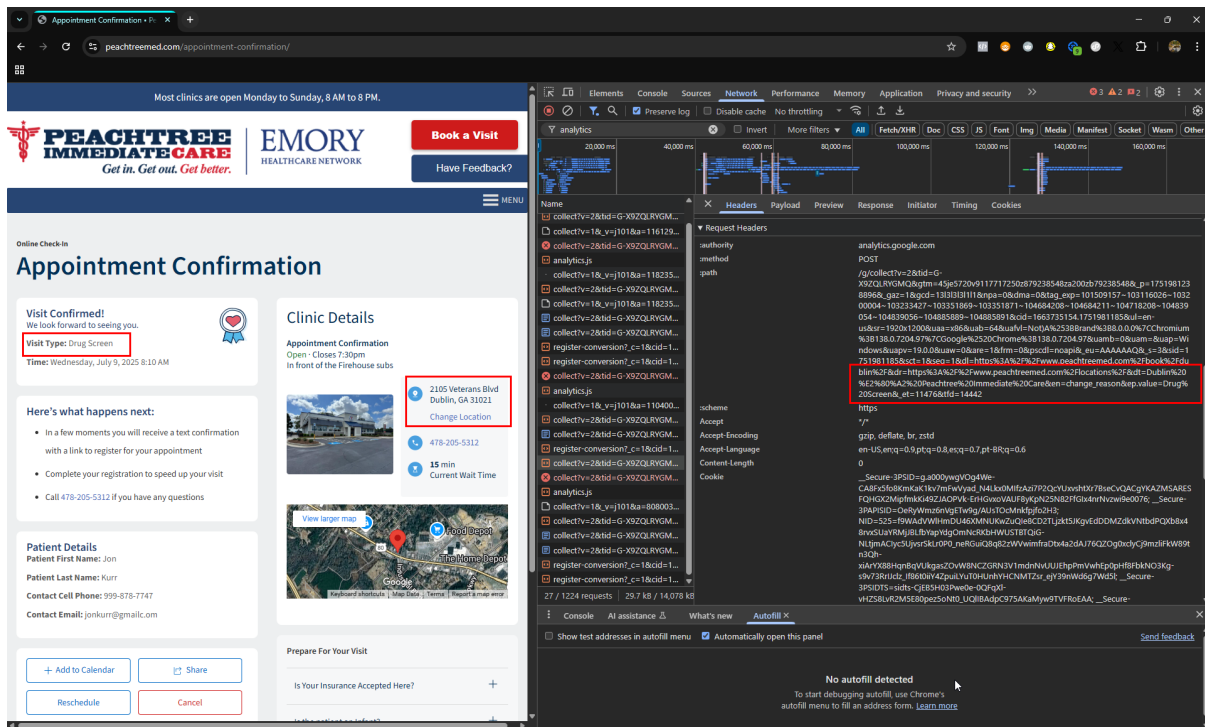


Figure 1
Full Screen View of User Appointment Confirmation

MENU

Online Check-In

Appointment Confirmation

Visit Confirmed!

We look forward to seeing you.

Visit Type: Drug Screen

Time: Wednesday, July 9, 2025 8:10 AM



Here's what happens next:

- In a few moments you will receive a text confirmation with a link to register for your appointment
- Complete your registration to speed up your visit
- Call 478-205-5312 if you have any questions

Patient Details

Patient First Name: Jon

Patient Last Name: Kurr

Contact Cell Phone: 999-878-7747

Contact Email: jonkurr@gmail.com

+ Add to Calendar

Share

Reschedule

Cancel

Clinic Details

Appointment Confirmation

Open · Closes 7:30pm

In front of the Firehouse subs



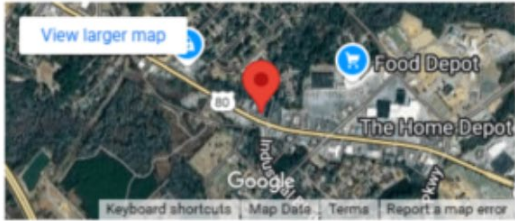
2105 Veterans Blvd
Dublin, GA 31021

Change Location

478-205-5312

15 min
Current Wait Time

View larger map



Keyboard shortcuts · Map Data · Terms · Report a map error

Prepare For Your Visit

Is Your Insurance Accepted Here?

+

Figure 2
Close Up View of Webpage

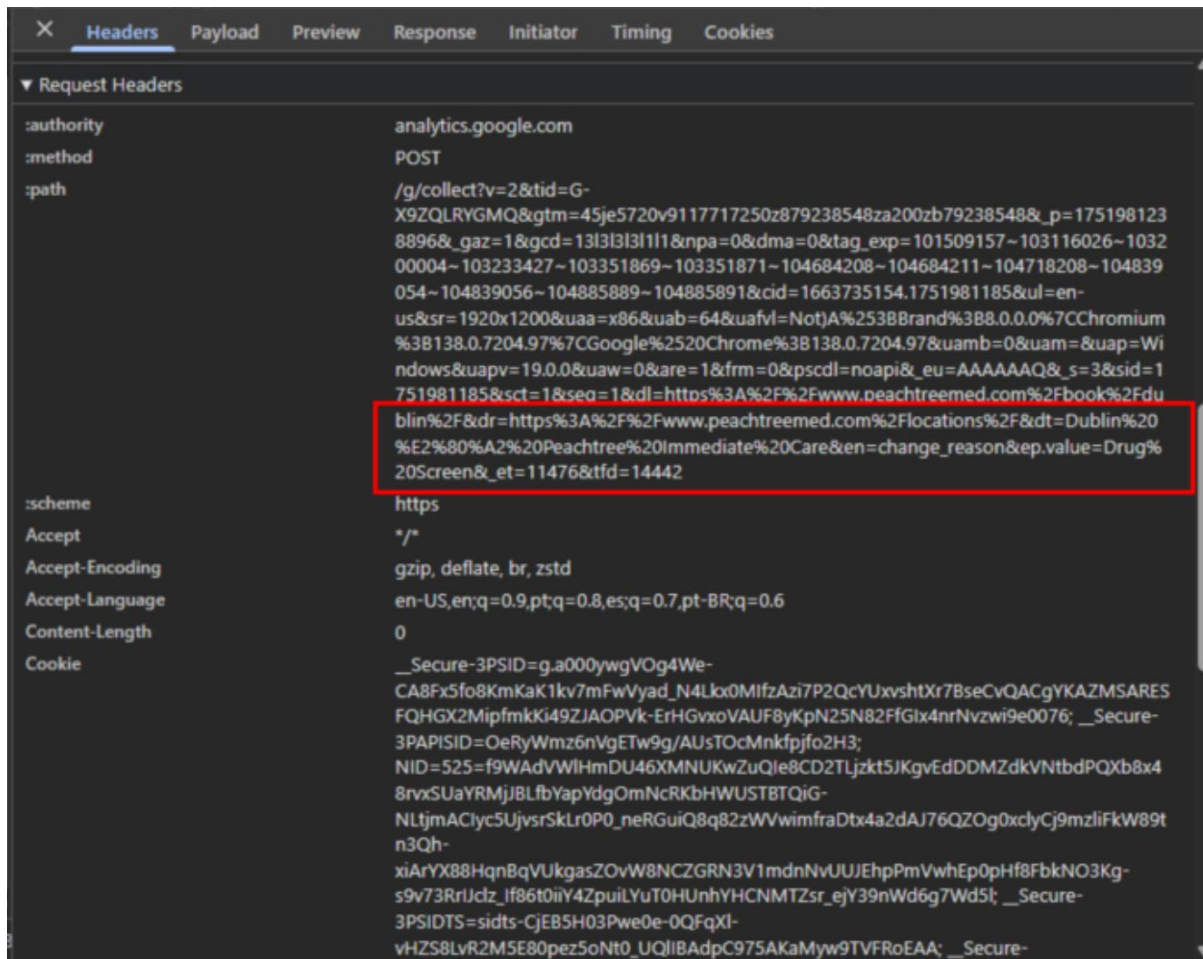


Figure 3

*Close up View of Google Analytics Transmission
Stating the appointment reason was “Drug Screen”*

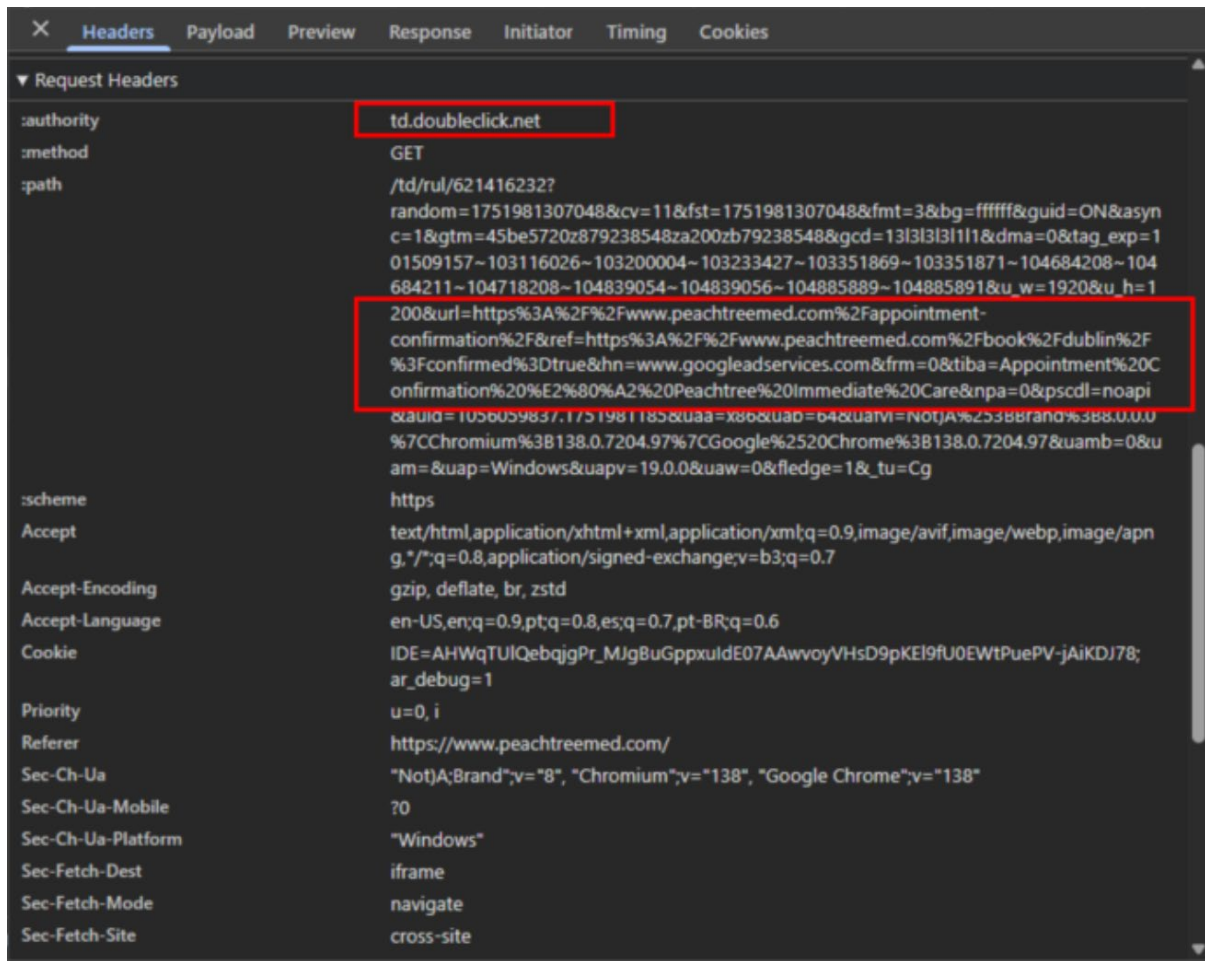


Figure 4
*Close-Up View of DoubleClick Transmission
 Showing a Confirmed Appointment at the Dublin Location*

85. Figures 1, 2, 3, and 4 above are screenshots taken from appointment made on <https://www.peachtreemed.com/>. It shows that when the user made the appointment for a Drug Screen in the Dublin, Georgia location, that exact information was transmitted to Google along with the user's NID and IDE cookies.

86. Figures 1, 2, 3 and 4 above reflect the same process and configuration used to collect and share Plaintiff's Private Information when she scheduled her appointment on August 9, 2024. An identical inquiry into

the secret NID and IDE cookies deployed at the time Plaintiff scheduled her appointment would show that she selected the “new illness/infection” option for the appointment for the “Sharpsburg” location.

87. At the very moment Plaintiff was seeking medical treatment for a urinary tract infection, her Private Information was simultaneously being intercepting and transmitted to third parties for advertising and tracking purposes.

88. Plaintiff and Class Members were not aware that their Private Information would be shared with Google as it was communicated to Defendants because, amongst other things, Defendants did not disclose this fact.

89. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendants to disclose their Private Information to Google.

90. Defendants’ tracking pixels sent non-public Private Information to Google, including but not limited to Plaintiff’s and Class Members’: (1) status as medical patients; (2) health conditions; (3) desired medical treatment or therapies; (4) appointment requests; (5) desired locations or facilities where treatment was sought; and (6) phrases and search queries conducted via the general search bar.

91. Importantly, the Private Information Defendants’ tracking pixels sent to Google was sent alongside Plaintiff’s and Class Members’ IDE

and NID cookie values, IP addresses, and device identifiers, which allows Google to link individual patients' communications with Defendants to their unique Google profiles and therefore their personal identities.

92. Through the IDE and NID cookies, Google can identify the specific individuals whose Private Information was being disclosed by Defendants. Google can also match the IDE and NID cookie values to the individual's existing user profiles, which contain detailed demographic information, browsing histories, and personally identifying information such as names, email addresses, and physical addresses.

93. Defendants deprived Plaintiff and Class Members of their privacy rights when they: (1) implemented third-party tracking technology (i.e., Google Analytics and DoubleClick) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Google—an unauthorized third party; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

94. Under HIPAA, an IP address is considered personally identifiable information. HIPAA defines personally identifiable information to include any unique identifying number, characteristic or code and specifically lists the example of IP addresses. See 45 C.F.R. § 164.514(b)(2).

The IDE and NID cookies similarly constitute unique identifying numbers that can be used to identify specific individuals.

VI. Defendants Violated HIPAA Standards and Industry Standards.

95. Under federal law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient for marketing purposes without the patient's express written authorization.

96. The Office for Civil Rights at HHS has issued guidance making clear that HIPAA-covered entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors.

97. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient relationship. The American Medical Association's Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

98. Plaintiff and Class Members were aware of Defendants' duty of confidentiality when they sought medical services from Defendants. At all times when Plaintiff and Class Members provided their Private Information to Defendants, they had a reasonable expectation that the information would remain private and that Defendants would not share the Private Information with third parties for a commercial purpose.

99. Under Georgia law, healthcare providers owe a duty to patients to maintain the confidentiality of medical records and information. See

O.C.G.A. §§ 31-33-2, 31-33-8. These statutes recognize that patients have a reasonable expectation of privacy in communications with healthcare providers relating to their medical conditions and treatment.

100. Defendants were enriched and benefitted from the use of the tracking technologies and unauthorized disclosures. In exchange for disclosing the Private Information of their patients, Defendants received enhanced advertising services from Google, more cost-efficient marketing, and reduced advertising costs, thereby benefitting Defendants.

101. Plaintiff's data and Private Information has economic value. Google regularly uses data that it acquires to create audiences and sells that information to advertising clients. Data harvesting is one of the fastest growing industries in the country, and the value of health data in particular is well-known and has been reported on extensively.

102. Defendants have active advertising campaigns on Google platforms, including dozens of active ads on just Google Search for locations at Peachtree Immediate Care.⁶

103. In exchange for disclosing users' Private Information, Defendants are compensated in the form of enhanced advertising services and more cost-efficient marketing on Google's platform. Google teaches

⁶ Google Ads Transparency Center, CRH Healthcare, LLC, <https://adstransparency.google.com/advertiser/AR10177861894858080257?region=US> (last accessed October 31, 2025).

users of the Collection Tools of how to use the data from the Tools to retarget users.⁷

104. Upon information and belief, Defendants re-targeted users and potential users to get more patients to use their services. By using the Google Collection Tools, the Defendants advertising and retargeting efforts were reduced in price, thus monetarily benefitting Defendants.

VII. Defendants Violated Google's Policies.

105. Since Google will not sign a business associate agreement for Google Analytics and DoubleClick, Google tells users of its tools that they “must refrain from using Google Analytics in any way that may create obligations under HIPAA for Google. HIPAA-regulated entities using Google Analytics must refrain from exposing to Google any data that may be considered Protected Health Information (PHI), even if not expressly described as PII in Google's contracts and policies.”

106. Google tells HIPAA-regulated entities to refrain from putting Analytics on any webpage that “implicates Google's access to, or collection of, PHI, and may only use Google Analytics on pages that are not HIPAA-covered.”

⁷ Google Analytics Help, “[GA4] Enable remarketing with Google Analytics data,” <https://support.google.com/analytics/answer/9313634> (last accessed October 31, 2025).

107. Importantly, Google identifies the exact kinds of pages on Defendants' websites as webpages that should not have Google's Collection Tools:

Unauthenticated pages that are related to the provision of health care services, including as described in the HHS bulletin, are more likely to be HIPAA-covered, and customers should not set Google Analytics tags on HIPAA-covered pages.

Please work with your legal team to identify pages on your site that do not relate to the provision of health care services, so that your configuration of Google Analytics does not result in the collection of PHI.⁸

VIII. Defendants Violated Their Privacy Policies.

108. Defendants' privacy policies represent to Plaintiff and Class Members that Defendants will keep Private Information private and confidential, and it will only disclose Private Information under certain circumstances.

109. Specifically, Defendants' privacy policies represents to patients and other website users as follows:

Other than as stated above, we will not disclose your PHI other than with a written authorization from you or your personal representative. Subject to compliance with limited exceptions permitted under state or federal law, we will not use or disclose psychotherapy notes, or other sensitive PHI, use or disclose your health information for marketing purposes or sell your health information, unless you have signed an

⁸ Google Analytics Help, "HIPAA and Google Analytics," <https://support.google.com/analytics/answer/13297105> (last accessed October 31, 2025).

authorization. You may revoke an authorization by notifying us in writing, except to the extent we have taken action in reliance on the authorization.⁹

110. As stated above, among other things, Defendants' privacy policy promises patients and users that (1) they will not share PHI without a written authorization; and (2) they will not use or disclose health information for marketing purposes or sell health information.

111. Notwithstanding these representations, Defendants installed Google Collection Tools on their Website and, therefore, automatically transmitted Private Information from everyone who visited their Website to Google. These actions were in violation of Defendants' own privacy policies and without Plaintiff and Class Members' knowledge or consent.

112. For Defendants to be authorized to disclose patient PHI to Google, they would have to have a business associate agreement with Google. However, Google does not provide business associate agreements for either Google Analytics or Google Ads (e.g., DoubleClick) technologies.¹⁰

⁹ See <https://www.peachtreemed.com/privacy-notice/> (last visited Oct. 15, 2025).

¹⁰ See Google Workspace, "HIPAA Included Functionality," September 30, 2025, https://workspace.google.com/terms/2015/1/hipaa_functionality/ (outlining the Google services that are applicable for a HIPAA Business Associate agreement, and not including Google Analytics or Google Ads) (last accessed October 30, 2025); Google, "HIPAA and Google Analytics," <https://support.google.com/analytics/answer/13297105?hl=en> ("Google makes no representations that Google Analytics satisfies HIPAA requirements and does not offer Business Associate Agreements in connection with this service.") (last accessed October 30, 2025).

113. At all times relevant to this Complaint, Defendants did not notify Plaintiff or Class Members that they were using the Private Information they communicate on the Website for commercial purposes.

114. Google did not secure any informed consent or written permission allowing them to use Private Information communicated on Defendants' Website for commercial purposes.

115. Defendants violated their own privacy policy by unlawfully intercepting and disclosing Plaintiff's and Class Members' Private Information to Google and third parties without adequately disclosing that they shared Private Information with third parties and without acquiring proper consent or authorization to share the Private Information.

TOLLING

116. Any applicable statute of limitations has been tolled by the delayed discovery rule. Plaintiff did not know (and had no way of knowing) that her PII and PHI was intercepted and unlawfully disclosed to Google because Defendants kept this information secret.

CLASS ACTION ALLEGATIONS

117. 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.

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

All individuals residing in the United States whose Private Information was disclosed to Google without authorization or consent as a result of using Defendants' Website (the "Class").

119. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

120. Fed. R. Civ. P. 23(a)(1). The Class members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of thousands of individuals whose PII and PHI may have been improperly disclosed to Google.

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

122. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendants' incorporation of Google Collection Tools.

123. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members.

**COUNT I
NEGLIGENCE AND NEGLIGENCE PER SE**

124. Plaintiff repeats and re-alleges all preceding allegations as contained in the Complaint as if fully set forth herein.

125. Defendants encouraged and/or required Plaintiff and Class Members to submit Private Information in order to obtain healthcare services.

126. Upon accepting, storing and controlling the Private Information of Plaintiff and Class Members in their computer systems, Defendants owed, and continue to owe, a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information from disclosure to third parties.

127. Upon accepting Plaintiff's and Class Members' Private Information in the course of providing medical treatment, Defendants owed Plaintiff and Class Members a duty to exercise reasonable care in handling, securing, and safeguarding their Private Information. The confidential relationship between healthcare providers and patients arises from Defendants' exclusive control over patients' medical communications, and the foreseeability that misuse of tracking technologies would expose sensitive health information. Federal and state statutes, industry standards, and professional codes of conduct, including HIPAA (45 C.F.R. § 164.530(c)(1)) and Georgia statutes governing the confidentiality of medical records (O.C.G.A. §§ 31-33-2, 31-33-8); Section 5 of the Federal Trade

Commission Act (15 U.S.C. § 45(n)) further reflect the standard of care Defendants were required to meet.

128. Defendants breached their duty of care by installing and implementing Google Collection Tools on their Website, knowing that such technologies would disclose Plaintiff's and Class Members' Private Information to Google without authorization, and knowing that Google would use the IDE and NID cookies to identify specific individuals and link their Private Information to their personal identities.

129. Defendants otherwise breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

130. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information through their use of the Google Collection Tools and other tracking technologies would result in unauthorized third parties, such as Google, gaining access to such Private Information for no lawful purpose.

131. Defendants' installation of Google Collection Tools caused Plaintiff's and Class Members' browsers, at the moment they submitted medical information, to transmit the contents of their communication, directly breaching their duty of care and proximately causing of injuries and damages to Plaintiff and Class Members.

132. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered damages, including invasion of privacy and loss of confidentiality of their Private Information; loss of the benefit of their bargain; diminution in value of their Private Information; continuing risk to their Private Information; increased infiltrations into their privacy through spam and targeted advertising they did not ask for; and loss of privacy, confidentiality, embarrassment, emotional distress, humiliation, and enjoyment of life.

133. Plaintiff and Class Members are entitled to compensatory damages in an amount to be determined at trial.

COUNT II BREACH OF FIDUCIARY DUTY

134. Plaintiff repeats and re-alleges all preceding allegations as contained in the Complaint as if fully set forth herein.

135. In light of the special relationship between Defendants and Plaintiff and Class Members, whereby Defendants became a guardian of Plaintiff's and Class Members' Private Information, Defendants became a fiduciary by their undertaking and guardianship of Private Information, to act primarily for Plaintiff and Class Members; (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and do store.

136. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendants' relationship with their patients and former patients, in particular, to keep secure their Private Information

137. Defendants exercised dominance over Plaintiff and Class Members' medical identities, leaving Plaintiff and Class Members with no ability to control disclosure of their Private Information.

138. Defendants encouraged Plaintiff and Class Members to use the Website, while Defendants alone possessed superior and exclusive knowledge of the tracking technologies they had deployed.

139. Defendants breached their fiduciary duties to Plaintiff and Class Members by disclosing their Private Information to unauthorized third parties, and separately, by failing to notify Plaintiff and Class Members of this fact.

140. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiff and Class Members.

141. But for Defendants' breach of fiduciary duty, the damage to Plaintiff and Class Members would not have occurred.

142. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal, and/or

punitive damages and disgorgement of ill-gotten gains, in an amount to be proven at trial.

**COUNT III
BREACH OF IMPLIED CONTRACT**

143. Plaintiff repeats and re-alleges all preceding allegations as contained in the Complaint as if fully set forth herein.

144. When Plaintiff and Class Members provided their Private Information to Defendants to obtain medical services, an implied contract arose from the physician-patient relationship Defendants created by holding themselves out as medical providers, collecting information for diagnosis and treatment and facilitating care with licensed practitioners, under which Defendants agreed to safeguard and not disclose their Private Information without consent.

145. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

146. Plaintiff and Class Members relied on Defendants' representations and promises and would not have entrusted Defendants with their Private Information in the absence of an implied contract between them and Defendants obligating Defendants not to disclose this Private Information without consent.

147. Defendants breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to a third party, *i.e.*, Google.

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

149. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendants' breach of implied contract.

COUNT IV BREACH OF EXPRESS CONTRACT

150. Plaintiff repeats and re-alleges all preceding allegations as contained in the Complaint as if fully set forth herein.

151. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts with Defendants for the provision of medical and health care services.

152. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with Defendants when Plaintiff and Class Members first received medical care from Defendants.

153. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendants include Defendants' promise to protect nonpublic, Private Information given to Defendants or that Defendants gathers on their own from disclosure.

154. Posted on Defendants' website is a Notice of Privacy Practices. The notice expressly states: (1) "PHI is protected and confidential"; (2) PHI includes "information about your symptoms, diagnosis, test results, treatment, and any other related medical information"; and (3) Defendants will not "use or disclose your health information for marketing purposes or sell your health information, unless you have signed an authorization."¹¹

155. Defendants did not obtain Plaintiff's or Class Members' signed authorization before disclosing their PHI.

156. Under these express contracts, Defendants and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members and (b) protect Plaintiff's and Class Members' PII/PHI: (i) provided to obtain such healthcare and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

157. Both the provision of medical services and the protection of Plaintiff and Class Members' Private Information were material aspects of these express contracts and exist independent of any duties under state or federal law, such as HIPAA.

¹¹ Notice of Privacy Practices, <https://www.peachtreemed.com/privacy-notice/> (last accessed January 23, 2026).

158. The express contracts for the provision of medical services—contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members’ Private Information—are formed and embodied in multiple documents, including (among other documents) Defendants’ privacy policy.

159. At all relevant times, Defendants expressly represented in their privacy policy, among other things, that Defendants would not share Private Information without a written authorization; and would not use or disclose Private Information marketing purposes or sell that information.

160. Defendants’ express representations, including, but not limited to, express representations found in their privacy policy, formed and embodied an express contractual obligation requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff’s and Class Members’ Private Information.

161. Plaintiff and Class Members provided their Private Information to Defendants pursuant to these representations that Defendants would not share their Private Information with unauthorized third parties, especially for marketing purposes.

162. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To Plaintiff and Class Members, healthcare that does not adhere to industry standard data

security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entered into these contracts with Defendants and/or their affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

163. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendants and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

164. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

165. Defendants materially breached their contractual obligation to protect the nonpublic Private Information Defendants gathered when they disclosed that Private Information to Google through the Google Collection Tools.

166. Defendants materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant privacy policies. Defendants did not maintain the privacy of Plaintiff's and

Class Members' Private Information as evidenced by Defendants' sharing of that Private Information with Google through the Google Collection Tools. Specifically, Defendants did not comply with industry standards, or otherwise protect Plaintiff's and Class Members' Private Information, as set forth above.

167. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Google, was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

168. As a result of Defendants' failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

169. Had Defendants disclosed that their data privacy was inadequate or that it did not adhere to industry-standard privacy measures, Plaintiff and Class Members would not have purchased healthcare from Defendants and/or their affiliated healthcare providers

170. In addition, or in the alternative, Defendants breached the express contracts by breaching the implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms. In Georgia, a breach of contract claim may lie where the defendant acts in bad faith when exercising discretion over the performance of its duties under the contract.

171. Here, Defendants acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties and breached the implied covenant of good faith and fair dealing by presenting its healthcare services as private and secure, while secretly, systematically, and repeatedly disclosing Private Information to Google through the Google Collection Tools, failing to disclose to Plaintiff and Class Members that they disclosed Private Information to Google through the Google Collection Tools, and continuing to disclose Private Information to Google through the Google Collection Tools.

172. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Google, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional

damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

173. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Google.

COUNT V UNJUST ENRICHMENT

174. Plaintiff repeats and re-alleges all preceding allegations as contained in the Complaint as if fully set forth herein.

175. Under Georgia common law, a cause of action for unjust enrichment requires: (1) a benefit conferred upon the defendant by the plaintiff; (2) retention of the benefit by the defendant; and (3) the retention would be inequitable or unjust.

176. Plaintiff and Class Members unintentionally conferred valuable data to Defendants by providing their Private Information, which Defendants used for marketing and advertising purposes.

177. Plaintiff's and Class Members's Private Information has independent economic value. Defendants knew this, which is why they sought to monetize it.

178. Defendants received and retained these benefits, including enhanced advertising services from Google, more cost-efficient marketing, reduced advertising costs, and revenue and profits derived from the

unauthorized use and disclosure of Plaintiff's and Class Members' Private Information.

179. The circumstances are such that it would be unjust and inequitable for Defendants to retain these benefits without compensating Plaintiff and Class Members.

180. Under principles of equity and good conscience, Defendants should be required to disgorge all benefits unjustly obtained.

COUNT VI
THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(1) et seq.

181. Plaintiff repeats and re-alleges all preceding allegations as contained in the Complaint as if fully set forth herein.

182. The ECPA protects both sending and receipt of communications. 18 U.S.C. § 2520(a) provides a private right of action to any person whose electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

183. The transmissions of Plaintiff's and Class Members' Private Information to Defendants via Defendants' Website qualify as "electronic communications" under 18 U.S.C. § 2510(12).

184. By utilizing and embedding Google Collection Tools on the Website, Defendants intentionally intercepted the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

185. Defendants not only intercepted the communications Plaintiff and Class Members on the Website by using Google Collection Tools, but also transmitted the information to third parties such as Google.

186. Defendants captured and transmitted the Private Information of Plaintiff and Class Members to third parties such as Google without the consent of Plaintiff and Class Members and in violation of Defendants' own privacy policies and HIPAA.

187. Defendants were not acting as legitimate parties to Plaintiff's or Class Members' communications when the interceptions occurred and therefore cannot claim they were a "party" to the communications per the definition, per 18 U.S.C. § 2511(2)(d). Plaintiff's communications were intended solely to obtain medical care and were directed to Defendants in their capacity as healthcare providers, not to facilitate disclosure to advertising or analytics companies. By embedding Google Collection Tools that contemporaneously intercepted and rerouted the contents of those communications to Google, Defendants exceeded any permissible participation in the communication and acted as interceptors for an unauthorized third party. The ECPA's party exception therefore does not apply, particularly where, as here, the interception was undertaken for a tortious and unlawful purpose.

188. By intentionally disclosing the electronic communications of Plaintiff and Class Members to Google, while knowing or having reason to

know that the information was obtained through interception, Defendants violated 18 U.S.C. § 2511(1)(c).

189. Plaintiff and Class Members did not authorize Defendants to acquire the content of their communications for purposes of disclosing their Private Information to Google via tracking technologies that use IDE and NID cookies to identify them personally.

190. As a result of Defendants' violations of the ECPA, Plaintiff and Class Members are entitled to relief under 18 U.S.C. § 2520, including equitable relief; actual damages or statutory damages of whichever is greater: \$100 a day for each day of violation or \$10,000; punitive damages; and reasonable attorneys' fees and litigation costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, respectfully requests that the Court enter judgment in her favor and against Defendants, as follows:

- A. Certifying this case as a class action on behalf of the Class defined herein, appointing Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;
- B. Declaring that Defendants' conduct violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1) *et seq.*

- C. Declaring that Defendants' conduct constituted negligence and/or negligence per se, breach of fiduciary duty, breach of implied contract, breach of express contract, and unjust enrichment;
- D. Awarding Plaintiff and Class Members compensatory, actual, and consequential damages in an amount to be determined at trial;
- E. Awarding Plaintiff and Class Members statutory damages as provided by law, including under the ECPA;
- F. Awarding Plaintiff and Class Members punitive and exemplary damages;
- G. Awarding restitution and disgorgement of all revenues and profits that Defendants obtained through their unlawful conduct;
- H. Issuing injunctive relief prohibiting Defendants from continuing the unlawful practices described herein and requiring Defendants to implement appropriate safeguards to protect patients' Private Information;
- I. Awarding Plaintiff and Class Members their reasonable attorneys' fees, costs, and expenses, including expert witness fees; and
- J. Granting such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

DATE: January 23, 2025
Respectfully Submitted,

/s/ Mark Silvey

Mark Silvey

GA Bar # 646837

Justin Day*

**BRYSON HARRIS SUCIU &
DEMAY PLLC**

201 Sevilla Avenue, 2nd Floor

Coral Gables, FL 33134

Phone: (786) 206-8291

jday@brysonpllc.com

James R. DeMay*

Laura Godly*

**BRYSON HARRIS SUCIU &
DEMAY PLLC**

900 West Morgan Street

Raleigh, NC 27603

Phone: (704) 941-4648

dbryson@brysonpllc.com

jdemay@brysonpllc.com

lgodly@brysonpllc.com

Stephen "Buck" Daniel

Ga. Bar No. 777514

RUEB STOLLER DANIEL, LLP

225 Ottley Drive NE, Suite 110

Atlanta, Georgia 30324

Phone: (404) 381-2888

buck@lawrsd.com

**Pro Hac Vice*

Attorneys for Plaintiff