

**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK**

EVA PERRY, JACQUELINE
FLETCHER, and DEBRA L.
GILMORE, *on behalf of themselves and
all others similarly situated,*

Plaintiffs,

v.

OSWEGO HEALTH, INC.,

Defendant.

Case No. 5:26-cv-1294 (BKS/CBF)

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Eva Perry, Jacqueline Fletcher, and Debra L. Gilmore, through their attorneys, bring this class action lawsuit in their individual capacities and on behalf of all others similarly situated against Oswego Health, Inc. (“Oswego” or “Defendant”). Plaintiffs allege the following based on their personal knowledge, their counsel’s investigation, certain facts in the public record, and, where indicated, upon information and good faith belief.

INTRODUCTION

1. Defendant Oswego is a regional healthcare system which serves Oswego County, New York, and the surrounding areas through its hospital, multiple urgent care centers, laboratory and imaging facilities, and multi-specialty medical group of over 100 physicians and medical providers. Oswego offers a broad range of primary and specialty care services, including cardiology, orthopedics, gastroenterology, ENT, general surgery, pulmonology, urology, and

bariatrics, and it provides both hospital-based and outpatient care across the region.¹

2. Oswego generates approximately \$233 million dollars in annual revenue.

3. As part of the medical services it provides, Oswego owns, operates, controls, and maintains a website, <https://www.oswegohealth.org/> (the “Website”). The Website allows current and potential Oswego patients, *inter alia*, to search for and view medical providers and services, hospital and office locations, and various wellness resources.

4. Oswego also operates, controls, and maintains two web-based patient portals (the “Portals”). Oswego’s patient Portals allow Oswego patients, *inter alia*, to remotely access their medical records, review their test results, schedule and view appointments, renew their prescriptions, and pay outstanding medical bills.² The Website and the Portals are referred to herein collectively as the “Web Properties.”

5. Oswego actively encourages patients to use its Web Properties to search for medical providers and services, to schedule doctor’s appointments, to check into urgent care, to access medical records and test results, to pay bills, and to view various wellness resources, among other things. Oswego patients and providers can also communicate with each other via the Portal.

6. Indeed, Oswego specifically invites patients to search for and share detailed information about their own physical and mental health via its Web Properties. And patients, trusting that this information will be safeguarded, in fact share their most intimate and personal medical information with Oswego through the Web Properties.

¹ See <https://www.oswegohealth.org/about-us/who-we-are/> (last visited Jun. 1, 2026).

² One portal is for primary care, and the other portal is for hospital and specialty services. See https://www.medentmobile.com/portal/index.php?main_section=login&practice_id=gjSXmFNr&primary_tab=messages (primary care portal, last visited June 1, 2026); <https://myportal.oswegohealth.org/Phm-PhmHome.HomePage.WR.mthr?hcis=OSW.LIVEF&application=phm> (hospital and specialty service portal, last visited Jun. 1, 2026).

7. Personal medical information concerning physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of such information can have serious consequences, including but not limited to discrimination in the workplace and/or denial of insurance coverage.³

8. Plaintiffs and Class Members who visited and used Oswego’s Web Properties (collectively, the “Users”) understandably thought that, in using the Web Properties, they were exchanging information and communicating only with their trusted healthcare providers.

9. Unbeknownst to the Users, however, Oswego was in fact collecting their sensitive medical and health-related information – including both personally identifiable information (“PII”) and protected health information (“PHI”) (collectively referred to as “PII/PHI” or “Private Information”)⁴ – and sharing that Private Information with third parties, specifically Google, without the Users’ knowledge, and without providing any notice to the Users or obtaining the Users’ consent to do so, in violation of federal and state law and Oswego’s own policies.

10. Specifically, Oswego embedded at least two undetectable “trackers” on its Web Properties – DoubleClick and Google Ads – which trackers collect and transmit to Google an incredible amount of personal and protected data about Users of the Web Properties.⁵ The

³ See Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), available at <https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/> (last visited Jun. 1, 2026) (“While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it’s even more verboten in addiction treatment, as patients’ medical history can be inherently criminal and stigmatized.”).

⁴ PHI is any health-related data (like medical records, test results, medical bills, or treatment or provider information) that is handled by healthcare providers and includes specific patient identifiers (names, Social Security numbers, birth dates, etc.). PHI is strictly protected by the Health Insurance Portability and Accountability Act (“HIPAA”) privacy rule. PII is any information that can be used to identify a person across any industry. PII is generally *not* protected by HIPAA *unless* it is or can be linked to a person’s health-related data.

⁵ The trackers themselves are small snippets of code placed on webpages by the website owner. The

interception, collection, and transmission of this Private Information is instantaneous, invisible, and occurs without any notice to (or consent from) the Users.

11. Indeed, despite intentionally incorporating these tracking technologies into its Web Properties and servers, Oswego never informed its Users that the Private Information they communicated via its Web Properties was being collected and intentionally disclosed to Google or any other third party. Nor did Oswego ever seek or obtain its Users' consent to disclose their Private Information.

12. To the contrary, Oswego's Privacy Policy *expressly denied* that Oswego would share the Users' Private Information with any third parties without its Users' express written consent.⁶

13. Despite this, and unbeknownst to Plaintiffs and Class Members, Oswego did exactly that, installing tracking technologies on its Web Properties to collect information – including Users' Private Information – from the Users and disclosing that information to unauthorized third parties like Google for Oswego's own pecuniary gain.

14. The information that Oswego collected from its Users and transmitted to Google and other third parties via its tracking technologies includes, but is not limited to, the following: (a) Users' access to the Oswego patient Portals; (b) the text of Users' search queries; (c) medical services and treatments sought by Users; (d) Users' searches for providers and medical facilities; (e) Users' accessing and viewing the bill pay webpage; (f) the URLs visited by Users on the Web Properties; and (g) other information that qualifies as PII and/or PHI under federal and state laws,

process of adding the trackers to a webpage is a multi-step process that, as described in detail in Secs. B&C, *infra*, must be undertaken by the website owner, namely, Oswego.

⁶ See Oswego Privacy Policy, available at <https://www.oswegohealth.org/privacy-policy/> (last visited Jun. 5, 2026).

such as the User's name, email address, phone number, zip code, and city of residence entered on the Web Properties.

15. Worse, Oswego's tracking technologies linked this information to its Users' specific internet protocol ("IP") address, device identifiers, email addresses, and/or unique Google accounts – which often contain a User's first and last name, email address(s), phone number(s), and physical address – to create for each User a detailed "data packet" that is shared with Google for marketing and analytics purposes.⁷ These data packets containing the Users' PII and PHI are then used by Oswego and third parties, for example, to send targeted advertisements to Users based on their sensitive and protected Private Information, or to gain additional insights into how Users use certain websites.⁸

16. HIPAA sets forth certain requirements designed to protect the privacy and confidentiality of all individually identifiable health information, or PHI, that is held or transmitted by a medical provider. Specifically, the HIPAA privacy rule prevents a medical provider from disclosing a patient's PHI without the patient's express, written consent.

17. Additionally, HIPAA lists approximately eighteen (18) "identifiers" which either identify or can be used to identify, contact, or locate an individual, alone or in combination with other sources. These identifiers, which include names, dates related to an individual, email addresses, device identifiers, web URLs, and IP addresses,⁹ are considered PII but are not protected

⁷ These data packets may also include, *e.g.*, the buttons a User clicks and/or the words a User types into the search bar on the Oswego Web Properties.

⁸ Oswego unquestionably was required to inform its Users that it had deployed tracking technologies on its Web Properties so that those Users could make an informed decision as to whether they wanted their information to be collected, disclosed, and used in this manner. *See* OCR Bulletin, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (emphasis added), available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited Jun. 1, 2026) ("disclosures of PHI to tracking technology vendors for marketing purposes, ***without individuals' HIPAA-compliant authorizations***, would constitute impermissible disclosures.").

⁹ *Guidance Regarding Methods for De-identification of Protected Health Information in*

by HIPAA *unless* they are or can be linked an individual's health-related data.

18. Operating as designed and as implemented by Oswego, the tracking technologies that Oswego installed on its Web Properties intercept and share with Google both Users' protected *PHI* – information such as when and where a specific User was seeking confidential medical care, for what medical condition, and the precise care they sought or received – and their *PII* – the specific User's email address, IP address, and/or device identifier, which is then connected with the User's medical information and becomes protected. Google is then able to use this collection of Private Information to build incredibly fulsome and robust marketing profiles for individual Users and create targeted advertisements for each User based on their own Private Information.

19. By installing these tracking technologies on its Web Properties, Oswego effectively planted a bug on the web browsers of its Users, including Plaintiffs and the Class Members, and caused them to unknowingly disclose their private, sensitive, and confidential health-related communications to Google through Oswego, for Oswego's profit.

20. In so doing, Oswego put its desire for profit over its patients' privacy rights.

21. As described in detail below, covered healthcare providers such as Oswego are not permitted to use tracking technology tools like Google trackers in a way that exposes patients' Private Information to any third party without each patient's express and informed consent. And Oswego never sought or received such consent from either Plaintiffs or the Class Members.

22. As recognized by both the Federal Trade Commission ("FTC") and the Office for Civil Rights ("OCR") of the Department of Health and Human Services ("HHS"), healthcare companies' use of tracking technologies to collect and divulge their patients' sensitive and

Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, available at <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Jun. 5, 2026).

confidential information is an extremely serious data security and privacy issue:

In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. *But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.*¹⁰

23. Similarly, OCR is clear that “[r]egulated entities [*i.e.*, healthcare providers 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.”¹¹

24. As a healthcare provider, Oswego had certain duties and obligations to its patients and Users of its web properties, including Plaintiffs and Class Members. Oswego breached those duties and obligations in one or more of the following ways: (a) by failing to adequately review its marketing programs and web-based technology to ensure the Web Properties were safe and secure; (b) by installing, or by failing to remove or disengage, technology that was known and designed to share web Users' information; (c) by failing to obtain Users' consent to disclose their PII and PHI to Google or other third parties; (d) by failing to take steps to block the transmission of Users' PII and PHI through its tracking technologies; (e) by failing to warn Users; and (f) by otherwise failing to design and monitor its Web Properties to maintain the confidentiality and integrity of Users' PII and PHI.

25. Plaintiffs and Class Members have suffered injury because of Oswego's conduct;

¹⁰ See Elisa Jillison, *Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC Cases*, Program on Corporate Compliance and Enforcement at New York University School of Law (Sept. 4, 2023) (emphasis added), available at https://wp.nyu.edu/compliance_enforcement/2023/09/04/protecting-the-privacy-of-health-information-a-bakers-dozen-of-takeaways-from-ftc-cases/ (last visited Jun. 1, 2026).

¹¹ See OCR Bulletin, *supra* note 8.

these injuries include: (a) invasion of privacy, (b) loss of benefit of the bargain, (c) compromise and disclosure of their Private Information, (d) diminution of value of their Private Information, (e) statutory damages, and (f) the continued and ongoing risk to their Private Information.¹²

26. Plaintiffs seek to remedy these harms for themselves and a class of all others similarly situated and therefore assert causes of action for (a) Violations of the Electronic Communications Privacy Act (18 U.S.C. § 2510, *et seq.*); (b) Negligence; (c) Breach of Implied Contract; (d) Breach of Fiduciary Duty; (e) Unjust Enrichment; (f) Breach of Confidence; (g) Constructive Bailment; (h) Implied Covenant of Good Faith and Fair Dealing; and (i) Violation of New York's Deceptive Trade Practices Act (New York Gen. Bus. Law § 349).

PARTIES

27. Plaintiff Eva Perry is a natural person residing in Oswego County in the State of New York, where she intends to remain.

28. Plaintiff Jacqueline Fletcher is a natural person residing in Oswego County in the State of New York, where she intends to remain.

29. Plaintiff Debra L. Gilmore is a natural person residing in Oswego County in the State of New York, where she intends to remain.

30. As detailed herein, Plaintiffs accessed Oswego's Web Properties on their computers and/or mobile devices and used the Web Properties, *inter alia*, to look for providers, review conditions and treatments, make appointments, communicate with their providers, view test results, and/or pay medical bills.

31. Defendant Oswego Health, Inc. is a registered non-profit entity with its

¹² The exposed Private Information of Plaintiffs and Class Members can – and likely will – be further disseminated to additional third parties utilizing the data for retargeting or insurance companies utilizing the information to set insurance rates. Furthermore, third parties often offer for sale the unencrypted, unredacted Private Information to criminals on the dark web for use in fraud and cyber-crimes.

headquarters, principal place of business and main campus at 110 W. Sixth St., Oswego, New York 13126.

32. Defendant Oswego is a covered entity under HIPAA.

JURISDICTION & VENUE

33. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because it arises under the laws of the United States and under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

34. This Court has supplemental jurisdiction over Plaintiffs' state-law claims under 28 U.S.C. § 1367(a) because Plaintiffs' state-law claims are so related to the federal claims that they form part of the same case or controversy under Article III of the United States Constitution.

35. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and a substantial portion of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

36. Venue is proper in this judicial district under 28 U.S.C § 1391 (a) through (d) because: (a) a substantial part of the events giving rise to this action occurred in this judicial district, including decisions made by Oswego's governance and management personnel or inaction by those individuals that led to the unauthorized sharing of Plaintiffs' and Class members' Private Information; (b) Oswego's principal place of business is located in this judicial district; (c) Oswego collects and redistributes Class members' Private Information in this judicial district; and (d) Oswego caused harm to Class members residing in this judicial district.

COMMON FACTUAL ALLEGATIONS

A. Federal Regulators Make Clear That the Use of Tracking Technologies to Collect & Divulge Private Information Without Patients’ Informed Consent Is Illegal.

37. The surreptitious collection and divulgence of Private Information is an extremely serious data security and privacy issue. Both the Federal Trade Commission (“FTC”) and the Office for Civil Rights of the HHS have reiterated the importance of and necessity for data security and privacy concerning health information.

38. For instance, in 2023, the FTC’s Business Blog published a bulletin entitled *Protecting the Privacy of Health Information: A Baker’s Dozen of Takeaways from FTC Cases*, in which it noted that “[h]ealth information isn’t just about medications, procedures, and diagnoses. **Rather, it’s *anything that conveys information – or enables an inference – about a consumer’s health*.** Indeed, [recent FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx*, and *Flo Health* **make clear that the fact that a consumer is using a particular health-related app or website – one related to mental health or fertility, for example – or how they interact with that app (say, turning ‘pregnancy mode’ on or off) may itself be health information.**”¹³

39. Indeed, the FTC has unequivocally stated that healthcare companies should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without a patient’s informed consent:

Don’t use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.

In today’s surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers’ sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.*** [Recent FTC enforcement actions such as]

¹³ See Jillison, *Protecting the Privacy of Health Information*, *supra* note 10 (emphasis added).

*BetterHelp, GoodRx, Premom, and Flo make clear that practices like that **may run afoul [off] the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information.***¹⁴

40. The federal government is taking these violations of health data privacy and security seriously, as evidenced by past, high-profile FTC settlements with several telehealth companies.

41. For example, in 2023, the FTC imposed a \$1.5 million penalty on GoodRx for violating the FTC Act by sharing its customers' sensitive PHI with advertising companies and platforms, including Facebook, Google, and Criteo. The FTC also reached a \$7.8 million settlement with the online counseling service BetterHelp, resolving allegations that the company shared customer health data with Facebook and Snapchat for advertising purposes. Likewise, the FTC reached a settlement with Flo Health, Inc. regarding information about fertility and pregnancy that the Flo fertility-tracking app was improperly sharing with Facebook, Google, and other third parties. And Easy Healthcare was ordered to pay a \$100,000 civil penalty for violating the Health Breach Notification Rule when its ovulation tracking app Premom shared health data for advertising purposes.¹⁵

¹⁴ *Id.* (emphasis added) (further noting that *GoodRx & Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization).

¹⁵ See Jill Hughes, *How FTC Enforcement Actions Will Impact Telehealth Data Privacy*, available at <https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy> (last visited Jun. 3, 2026); see also Allison Grande, *FTC Targets GoodRx In 1st Action Under Health Breach Rule*, Law360 (Feb. 1, 2023), available at www.law360.com/articles/1571369/ftc-targets-goodrx-in-1st-action-under-health-breach-rule?copied=1 (last visited Jun. 3, 2026); *FTC Gives Final Approval to Order Banning BetterHelp from Sharing Sensitive Health Data for Advertising, Requiring It to Pay \$7.8 Million*, available at <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising> (last visited Jun. 3, 2026); *Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order*, available at <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc> (last visited Jun. 3, 2026); *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Data with Facebook, Google, and Others*, available at <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc->

42. And in July 2023, federal regulators sent a letter to approximately 130 healthcare providers warning them about using online tracking technologies that could result in unauthorized disclosures of Private Information to third parties. The letter highlighted the “risks and concerns about the use of technologies, such as the Meta/Facebook Pixel and Google Analytics, that can track a user’s online activities,” and warned about “[i]mpermissible disclosures of an individual’s personal health information to third parties” that could “result in a wide range of harms to an individual or others.” According to the letter, “[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more.”¹⁶

43. The Office for Civil Rights at HHS has made clear, in a 2024 bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the transmission of such protected information violates HIPAA’s Privacy Rule:

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.***¹⁷

44. The OCR Bulletin *reminds* healthcare organizations regulated under HIPAA that they may use third-party tracking tools such as Google Analytics or Pixels *only in a limited way*, to perform analysis on data key to operations. But they are **not** permitted to use these tools in a

[finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google](#) (last visited Jun. 3, 2026).

¹⁶ See FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies (Jul. 20, 2023), available at <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking> (last visited Jun. 10, 2023).

¹⁷ See OCR Bulletin, *supra* note 8 (emphasis added).

way that may expose patients' PHI to these vendors.¹⁸

45. The OCR Bulletin specifically discusses the harms that disclosure may cause patients:

An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, *discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI*. Such disclosures can reveal incredibly sensitive information about an individual, *including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment*.

While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, *because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule*.¹⁹

46. Moreover, investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on the digital properties of hospitals, health care providers, and telehealth companies to monetize their Users' Private Information.

47. For instance, in 2022, THE MARKUP reported that 33 of *Newsweek's* top 100 hospitals in the America utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment.²⁰

48. And, in the aptly titled report "*Out of Control*": *Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, a joint investigation by STAT and THE

¹⁸ See *id.*

¹⁹ *Id.* (emphasis added).

²⁰ See Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (Jun. 16, 2022), available at <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> (last visited Jun. 3, 2026).

MARKUP of 50 direct-to-consumer telehealth companies reported that telehealth companies or virtual care websites were providing sensitive medical information they collect to the world's largest advertising platforms.²¹

49. Many healthcare sites had at least one tracker – from Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn and/or Pinterest – that collected patients' answers to medical intake questions.²²

B. The Tracking Technologies Used by Oswego on Its Web Properties.

50. Google operates multiple tracking technologies that collect and compile user data in order to enable website owners to enhance user experience, personalize content, and implement effective targeted advertising, among other things.

51. One such technology is DoubleClick, a digital advertising platform acquired by Google that has been fully integrated into Google's advertising ecosystem as part of the Google Marketing Platform. DoubleClick's technologies automate the ad buying process and rely on collected data to support targeted advertising initiatives.²³

52. Specifically, DoubleClick is an advertising tracking tool designed to collect information about user behavior on websites for the purpose of improving the targeting and effectiveness of advertising campaigns. It builds independent user profiles to optimize ad targeting

²¹ Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, "*Out Of Control*": *Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech's tracking tools* (Dec. 13, 2022), available at <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies> (last visited Jun. 3, 2026).

²² See *id.* (noting that "[t]rackers on 25 sites, including those run by industry leaders Hims & Hers, Ro, and Thirty Madison, told at least one big tech platform that the user had added an item like a prescription medication to their cart, or checked out with a subscription for a treatment plan").

²³ See <https://support.google.com/faqs/answer/2727482?hl=en> (last visited Jun. 8, 2026).

and does not rely on users having pre-existing Google accounts.²⁴

53. Stated otherwise, DoubleClick utilizes “cookies”²⁵ and other device identifiers to show users personalized ads based on their browsing behavior.

54. To accomplish this, DoubleClick collects and stores users’ IP addresses in server logs, and additionally creates two types of cookies, which are generated by a User’s web browser, are stored on the User’s computer, and can be used to uniquely identify the User.

55. The first such identifier is the IDE cookie. The IDE cookie is a persistent advertising identifier that is used to show personalized Google ads on non-Google sites. It builds user profiles for cross-site ad targeting and plays a central role in tracking users’ interactions across the web. The IDE cookie increases advertising effectiveness by tracking actions that users take after viewing or clicking on advertisements, such as visiting specific pages or completing transactions, and enables the delivery of personalized ads to users based on those actions.

56. The second is the DSID cookie. 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.

57. Both IDE and DSID cookies are unique to each user and may be used to identify or single out individuals; thus, they constitute PII.

58. Another Google tracking technology is Google Ads. Google Ads is an advertising platform that allows businesses, organizations, and advertisers to reach users across the Google

²⁴ *See id.*

²⁵ “Cookies are small files of information that a web server generates and sends to a web browser. ... Cookies help inform websites about the user, enabling the websites to personalize the user experience.” *See* <https://www.cloudflare.com/learning/privacy/what-are-cookies/> (last visited Jun. 3, 2026).

ecosystem. The platform supports various campaign types such as search ads, display ads, shopping ads, and video ads. Advertisers can define audiences, track conversions, and optimize campaigns based on user engagement signals and behavioral data.²⁶

59. Google Ads uses a set of third-party cookies (*e.g.*, 3PSID, 3PAPISID, 3PSIDCC, and NID) to track user behavior across websites and link it to advertising audiences and targeting signals. These cookies allow Google to create more comprehensive user profiles, enabling Google to associate web activity with authenticated accounts. Because these are third-party cookies, the data collected does not remain within the originating website but is transmitted directly to Google's advertising infrastructure for purposes such as ad personalization and measurement.

60. The 3PSID, 3PAPISID, and 3PSIDCC cookies are used to identify users by linking their browsing activity to their Google account when they are signed in.

61. In contrast, the NID cookie collects information from users even when they are not signed in or have never created a Google account. This cookie assigns a unique ID to the user's browser to store customized settings and manage targeted ads across Google services. Thus, the NID cookie enables Google to track user behavior across websites regardless of their account status, by using browser-level identifiers to support ad delivery and preference management even in anonymous sessions.

62. Consequently, these cookies are also used to identify or single out individuals and thus can constitute PII, particularly when linked to other account data.

63. In certain implementations, tracking and remarketing requests related to Google Ads are routed through the "www.google.com" domain. Despite being served from a seemingly general-purpose domain, these requests participate directly in audience building, ad targeting, and

²⁶ See <https://support.google.com/google-ads/answer/6319> (last visited Jun. 8, 2026).

conversion tracking.²⁷ As such, data transmitted to Google in this context is not simply passive or generic, but contributes to Google’s advertising infrastructure, even when no visible ad is rendered.²⁸

64. Oswego installed DoubleClick and Google Ads (and, upon information and good faith belief, other tracking technologies) on many – if not all – of the webpages within its Web Properties, including at least some pages in its member-only patient Portals, and it programmed or permitted those webpages to surreptitiously share patients’ Private Information with Google and potentially other third parties.

65. Moreover, Oswego used the data it collected from Plaintiffs and Class Members, without their consent, to improve its advertising and bolster its revenues.

C. Oswego’s Method of Collecting and Transmitting Plaintiffs’ & Class Members’ Private Information.

66. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the Internet. Each “client device” (computer, tablet or smartphone) accesses web content through a web browser (*e.g.*, Google’s Chrome, Mozilla’s Firefox, Apple’s Safari and/or Microsoft’s Edge browsers).

67. Every website is hosted by a computer “server” that holds the website’s contents. The entity(ies) in charge of the website exchange communications with users’ devices as their web browsers query the server through the internet.

68. Web communications consist of Hypertext Transfer Protocol (“HTTP”) or Hypertext Transfer Protocol Secure (“HTTPS”) requests and HTTP or HTTPS responses, and any given browsing session may consist of thousands of individual HTTP requests and HTTP

²⁷ See <https://support.google.com/google-ads/answer/2476688> (last visited Jun. 8, 2026).

²⁸ See <https://support.google.com/google-ads/answer/1722022> (last visited Jun. 8, 2026).

responses, along with corresponding cookies:

- a. **HTTP request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (*i.e.*, web address) and retrieving data from it, GET Requests can also send data to the host server embedded inside the URL and can include cookies. POST Requests, another common type of HTTP Requests, can send a large amount of data outside of the URL. (For instance, uploading a PDF to file a motion to a court.)
- b. **HTTP response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP request. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data.
- c. **Cookies**: a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Typically, cookies are initially sent by a host server along with a HTTP response, instructing the client browser to store data locally. Once stored, cookies then automatically attach to subsequent HTTP requests made to the same website, identifying the client and its preferences. "Third-party cookies" are tracking files that are created by an entirely different website than the one the client is visiting, yet still communicate with that website (*e.g.*, to suggest targeted advertisements).

69. When a User visits an Oswego Web Property, the User's web browser sends an HTTP request to Oswego's servers to load the requested web page – *e.g.*, a list of specified medical providers or information about a particular ailment.

70. In response, Oswego's servers send back to the User the requested webpage, which the User is able to view on his or her web browser.

71. This communication exchange also involves the transmission of cookies – first from Oswego's web page, instructing the User's browser to store specific data on the User's device; and then from the User's device, identifying the User by IP address, device, and/or other identifying information. This exchange of cookies enables Oswego's servers, *e.g.*, to identify the User, to recall the User's preferences and log-in status, and/or to auto-populate the User's log-in

information.

72. Unbeknownst to the User, however, his communication with Oswego's Web Properties also includes the invisible and imperceptible exchange of additional information through the operation of at least two tracking technologies installed and implemented by Oswego: DoubleClick and Google Ads.

73. These tracking technologies run silently in the background as a User browses Oswego's Web Properties, and surreptitiously collect information about the User. The tracking technologies instruct the User's web browser to send the User's IP address, along with other identifying data like device information, browser details, and specific cookies, to Google. This identifying information allows Google to monitor the User's activity and gather insights about the User's behavior, both on Oswego's Web Properties and on other websites.

74. In other words, when Users visit Oswego's Web Properties via an HTTP request to Oswego's servers, Oswego's servers send an HTTP response that not only displays the webpage visible to the User, but also contains the invisible tracking technologies which are surreptitiously collecting and transmitting the User's Private Information to Google and/or other third parties – much like a traditional wiretap.

75. Consequently, Oswego is, in essence, handing its patients a tapped phone and, once the webpage is loaded into the patient's browser, the software-based wiretaps are quietly intercepting the patients' communications and Private Information – which are intended only for Oswego – and transmitting those communications to Google and other third parties.

76. Moreover, as described above, Google's tracking technologies place third-party cookies in the web browsers of Users logged into their services. These cookies uniquely identify the User and are sent with each intercepted communication to ensure that the third party can

identify the specific User associated with the information intercepted (in this case, highly sensitive Private Information).

77. On a general, commercial website, such as Amazon, this tracking of users' activity would most likely amount to nothing more than a mere annoyance. On the website of a medical provider like Oswego, however, it is far more serious – and indeed, a violation of applicable law and Users' privacy rights. This is because, through its tracking technologies, Oswego collects its Users' medical information – including searches for and views of medical conditions, services, and providers – links that information with other information that can be used to identify the User, and provides the entire “data package” to third-party Google.

78. Stated otherwise, Oswego intentionally configured the tracking technologies installed on its Web Properties to capture both the “characteristics” of individual patients' communications with Oswego (*i.e.*, the Users' IP addresses, cookie identifiers, device identifiers, and account identifiers) and the “content” of these communications (the buttons, links, pages and tabs they clicked and viewed relating to their health conditions and services sought from Oswego).

79. Upon information and belief, Oswego intercepted and disclosed the following non-public, private information to Google:

- a. Plaintiffs' and Class Members' status as medical patients, via their access to the patient Portals and/or clicking to pay a bill online;²⁹
- b. Plaintiffs' and Class Members' searches for medical providers, medical services, and medical facilities and locations;
- c. Plaintiffs' and Class Members' communications with Oswego through its Web Properties, including specific text queries typed into the search bar;
- d. Plaintiffs' and Class Members' clicking on “ways to give”;

²⁹ Significantly, accessing the patient Portals and/or paying a bill online would only be performed by existing Oswego patients, which information is considered patient data.

- e. Every URL visited by Plaintiffs and Class Members on the Web Properties; and
- f. PII collected by its tracking technologies, including but not limited to patients' locations, accounts, IP addresses, and device identifiers.

80. Oswego also deposits the third-party Google cookies listed above (*e.g.*, IDE, DSID, 3PSID, 3PAPISID, 3PSIDCC, and NID) onto Plaintiffs' and Class Members' computing devices. And without any notice or authorization, Oswego commands Plaintiffs' and Class Members' computing devices to contemporaneously re-direct the Plaintiffs' and Class Members' identifiers and the content of their communications to Google.

81. The following examples detail how a User may interact with Oswego's Web Properties, and how Oswego intercepts and shares those interactions – including information and search results related to the Users' private medical conditions and treatment, as well as the Users' identities – with Google in real time.

82. For example, a User may visit the Oswego Website to search for a medical provider. Users can search for a provider based on the provider's specialty, name, or city, among other criteria.³⁰

83. If a User were to search, *e.g.*, for the "Breast Care" specialty, she would be shown three providers.³¹ Clicking on a specific provider (*e.g.*, Lisa Lai, MD) would lead the user to that provider's individual webpage.³²

84. Unbeknownst to the User, her view of the provider's webpage and specialty is transmitted in real time to Google via DoubleClick and Google Ads through the tracking

³⁰ See <https://www.oswegohealth.org/provider-directory/> (last visited Jun. 8, 2026).

³¹ See <https://www.oswegohealth.org/provider-directory/?specialty=Breast%20Care> (last visited Jun. 8, 2026).

³² See <https://www.oswegohealth.org/provider-directory/providers/lisa-lai-md/> (last visited Jun. 8, 2026).

Dr. Lisa Lai's Name and Specialty Shared with DoubleClick, Along with IDE Cookie



Host

Method

URL

Params

Edited

Status code

Length

MIME type

Extension

Title

Notes

TLS

IP

Cookies

Time

Listener port

1962

https://www.google.com

GET

/pagead/js/user-list/1719069534...

200

843

GF

142.250.68.38

Secure-SPSID

10.38.23.9

6080

Request

Pretty

Raw

Hex

Analysis

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

Response

Pretty

Raw

Hex

Render

Analysis

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

Inspector

Request attributes

2

Request query parameters

37

Request cookies

5

Request headers

27

Response headers

15

Request

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

22

identifiable by her cookies, searched for Breast Care services and selected Dr. Lai.

86. Alternatively, a User may visit the Oswego Website to search for a medical service in a specific field. A User can click on the “Services” tab, and then on a particular specialty, such as Urology.³³

87. The User can then click on a specific provider (e.g., Eyal Kord, MD, MPH), which takes the User to that provider’s individual webpage.³⁴

88. Unbeknownst to the User, his search for a specific medical service and his view of the provider’s webpage is transmitted in real time to Google via DoubleClick and Google Ads through the tracking technologies Oswego has imbedded in its Web Properties’ code, along with unique identifying third-party cookies. See Figures 3 and 4, below.

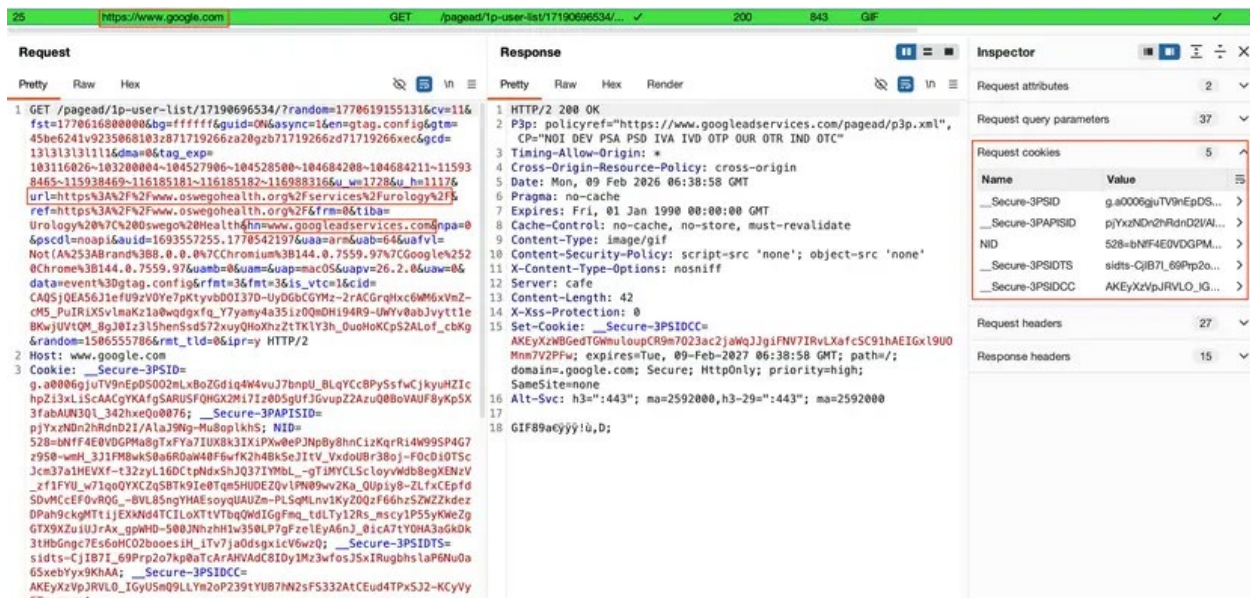
Figure 3

User’s View of Urology Specialty Shared with DoubleClick, Along with IDE Cookie

The screenshot displays the Chrome DevTools network panel. The top bar shows a GET request to `https://googleads.g.doubleclick.net` with a status of 200 and a size of 4876 bytes. The 'Request' tab is active, showing the full URL and a list of headers including 'Host', 'User-Agent', 'Accept', 'X-Client-Data', 'Sec-Fetch-Site', 'Sec-Fetch-Mode', 'Sec-Fetch-Dest', 'Sec-Fetch-Storage-Access', and 'Referer'. The 'Response' tab shows the server's reply, including status 200 OK, 'P3p' policy, 'Cross-Origin-Resource-Policy', 'Date', 'Expires', 'Cache-Control', 'Content-Type', 'X-Content-Type-Options', 'Content-Disposition', 'Server', 'Content-Length', 'X-XSS-Protection', 'Alt-Svc', and a JavaScript function. The 'Inspector' tab on the right shows the 'Request cookies' section, which contains a single cookie named 'IDE' with the value 'AHWqTukip9_SLKcY...'.

³³ See <https://www.oswegohealth.org/services/urology/> (last visited Jun. 8, 2026).

³⁴ See <https://www.oswegohealth.org/provider-directory/providers/eyal-kord-md-mp/> (last visited Jun. 8, 2026).

Figure 4**User's View of Urology Specialty Shared with Google Ads, Along with Cookies**

89. Thus, Oswego's tracking technologies inform Google that this individual User, identifiable by his cookies, searched for Urology services and selected Dr. Kord.

90. Additionally, anytime a User clicks the Patient Portal or Bill Pay tab on the Oswego Website – tabs that only active Oswego patients would use – the User's click is transmitted in real time to Google via DoubleClick and Google Ads through Oswego's tracking technologies, along with unique identifying third-party cookies. Thus, the tracking technologies inform Google that the User is an Oswego patient. *See, e.g.,* Figures 5 and 6, below.

Figure 5

User's Click on "Bill Pay" Shared with Google through DoubleClick, with IDE Cookie

The screenshot shows a network request to `https://googleads.g.doubleclick.net` with a GET method. The response is a JavaScript file. The 'Request cookies' section in the Inspector is highlighted in red, showing a cookie named 'IDE' with a value starting with 'ANWqTukd...'. The 'Response' pane shows the JavaScript code, which includes a function definition for 'function(a,b){...}'.

Figure 6

User's Click on "Bill Pay" Shared with Google through Google Ads, with Cookies

The screenshot shows a network request to `https://www.google.com` with a GET method. The response is a JavaScript file. The 'Request cookies' section in the Inspector is highlighted in red, showing a cookie named 'Secure-SPSID' with a value starting with 'g.a0005gu...'. The 'Response' pane shows the JavaScript code, which includes a function definition for 'function(a,b){...}'.

91. Similarly, if a User uses the Oswego Website's general, free-text search bar, the terms and phrases that the User types – such as “cancer” – along with any search results and subsequent “clicks” by the User are transmitted to Google, as well as third-party cookies

identifying the User, even if those terms, phrases, and search results contain a User's personal and private medical conditions, treatment or procedures, and/or any queries related thereto. *See, e.g.,* Figures 7 and 8, below.

Figure 7

User's "Cancer" Query Shared with Google through DoubleClick, with IDE Cookie

The screenshot displays the Chrome DevTools network and inspector panels. The network panel shows a request to `https://googleads.g.doubleclick.net/pagead/viewthroughconversion`. The response is a 200 OK with a JSON body. The 'Request cookies' section in the Inspector shows a single cookie named 'IDE' with a value starting with 'AHqTukdRnyebn6BYZLwHsg...'. The 'Request headers' section shows various headers including 'User-Agent', 'Accept', and 'Accept-Encoding'.

Figure 8

User's "Cancer" Query Shared with Google through Google Ads, with Cookies

The screenshot displays the Chrome DevTools network and inspector panels. The network panel shows a request to `https://www.google.com/pagead/ip-user-list`. The response is a 200 OK with a JSON body. The 'Request cookies' section in the Inspector shows multiple cookies, including '_Secure-3PSSID', '_Secure-3PSSID', and '_Secure-3PSSDTS'. The 'Request headers' section shows various headers including 'User-Agent', 'Accept', and 'Accept-Encoding'.

92. Consequently, the information transmitted to Google by the tracking technologies installed on Oswego's Web Properties includes both information about its Users' medical conditions and treatment and their personally identifying information (such as their physical location, IP addresses, and device information), which together constitute PII/PHI that is protected from disclosure by HIPAA.

93. Upon information and belief, the tracking technologies on Oswego's Web Properties collect and share with Google *every page a User visits on the Website*, as well as *every character typed and button or link "clicked" thereon*. Thus, Oswego is also tracking when Users search for the location of medical facilities, when they click on "Ways to Give" monetary donations, when they click for information about "Retirement Living," and even when they search for specific "Wellness Resources" such as cancer screenings.

94. Each time a User shares this information with Oswego, Oswego in turn shares it with Google – along with information that can be used to identify said User – which constitutes an unlawful disclosure of the User's PII/PHI.

95. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise permitted Oswego to disclose their PII/PHI; nor did they authorize any assistance with intercepting their communications. Plaintiffs and Class Members were never provided with any written notice that Oswego disclosed its Web Properties' Users' PII/PHI, nor were they provided any means of opting out of such disclosures. Despite this, Oswego knowingly disclosed Plaintiffs' and Class Members' PII/PHI to Google.

96. By law, Plaintiffs and Class Members are entitled to privacy in their PII/PHI and confidential communications. Oswego deprived Plaintiffs and Class Members of their privacy rights when it: (a) implemented a system that surreptitiously tracked, recorded, and disclosed

Plaintiffs' and Class Members' confidential communications, PII, and PHI to a third party; (b) disclosed patients' Protected Information to Google – an unauthorized third-party eavesdropper; and (c) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent. Plaintiffs and Class Members did not discover that Oswego disclosed their PII and PHI to Google, and assisted Google with intercepting their communications, until at least June 2026 for Plaintiffs Perry, Fletcher, and Gilmore.

D. Oswego's Use of the Tracking Technologies Violated Its Own Privacy Policies.

97. Oswego publishes several privacy policies that represent to Users of its Web Properties that it will keep their Private Information private and secure, and that it will only disclose PII and PHI provided to it under certain circumstances, ***none of which apply here.***

98. When Users first open the Oswego Website, they are shown a cookie banner at the bottom of the webpage which states:

This website uses cookies: We use cookies on this site to enhance your experience and improve our marketing efforts. By continuing to browse without changing your browsing settings to block or delete cookies, you agree to our website's cookie use as described in our privacy policy.

99. By presenting this banner, the Oswego Website conveys to Users that cookies are used primarily to enhance user experience and support the Website's own marketing efforts. The banner does ***not*** disclose that Users' interactions and communications – including searches for medical services and providers and personal identifying information – are transmitted to third-party advertising and analytics companies like Google. Nor does it inform Users that these third parties independently receive, process, and utilize this data for tracking and marketing purposes. Instead, the banner describes Oswego's cookie usage as merely internal and routine, without clarifying that Users' Private Information is being shared outside the Oswego system.

100. The banner further states that, by continuing to browse without changing their

browser settings, Users agree to the Website’s cookie use “as described in [Oswego’s] privacy policy.” Because the banner does not disclose that third-party tracking technologies intercept and transmit users’ activity and Private Information to external entities, however, any implied “consent” obtained through continued browsing, or even clicking “OK,” is not informed and thus cannot reasonably be construed as adequate consent to such tracking and disclosure. At most, the cookie banner suggests consent to the Website’s general internal cookie usage – *not* to the disclosure of Users’ sensitive medical and health-related Private Information to third-party advertising vendors like Google.

101. And even if a user were to click through and review Oswego’s formal Privacy Policy, that document likewise fails to provide clear and accurate notice of these third-party disclosures and, in several respects, **affirmatively contradicts** the Website’s actual tracking practices.

102. Specifically, when Users click on Oswego’s Privacy Policy link, either in the cookie banner or at the bottom of the Website page, they are directed to a relatively brief text that emphasizes anonymity and moreover **expressly denies the use of identifiable data**.³⁵

103. Indeed, the Privacy Policy asserts:

We will not distribute information that identifies you individually or reveals your identity (personally identifiable information) to any organization outside of the Oswego Health system. We will not make identifying information available publicly without the prior written or electronic consent of the individual identified. We may collect and use information about you and your use of the Oswego Health site, including identifying information, for our own internal purposes such as analyzing usage of the website for improvement purposes.³⁶

104. Oswego’s Privacy Policy further states:

³⁵ See <https://www.oswegohealth.org/privacy-policy/> (emphasis added) (last visited Jun. 9, 2026).

³⁶ *Id.* (emphasis added).

Oswego Health may use other companies or outside agencies to perform certain functions. For example, functions might include credit card payment processing or email services. **These companies or outside agencies may be given access to certain personally identifiable information as needed to perform their services, but are not authorized to use this information for any other purposes.** From time to time Oswego Health may share certain customer information with affiliates, but we also ask those companies to honor the standards of our Privacy Policy.³⁷

105. Finally, with respect to cookies, the Privacy Policy represents: “The Oswego Health site may store files called ‘cookies’ on the user’s computer that contain usernames, passwords and other user preferences **solely for the convenience of the user.**”³⁸

106. Accordingly, Oswego’s Privacy Policy expressly promises **not** to share Users’ PII with third parties without the Users’ express consent (except for certain, limited purposes).

107. Despite these assurances, Oswego’s Web Properties incorporate third-party tracking tools that enable user profiling (*i.e.*, PII) and transmit patients’ medical data (PHI) to Google through DoubleClick’s uniquely identifying IDE cookies and Google Ads’ cookies, as described above. This practice directly contradicts the Privacy Policy’s repeated assertions that Oswego will not distribute PII to third parties.

108. Indeed, Oswego’s Privacy Policy does **not** permit it to use or disclose Plaintiffs’ and Class Members’ PII/PHI for marketing purposes.

109. Nor does Oswego ever request – must less obtain – consent for the transfer or sale of this Private Information to third parties such as Google.

110. HHS HIPAA Guidance clarifies that any deployment of pixels, cookies, session-replay scripts, or similar technologies on a healthcare website is subject to HIPAA. Even if a provider were to disclose in its privacy policy that it uses such tracking tool – which Oswego does,

³⁷ *Id.* (emphasis added).

³⁸ *Id.* (emphasis added).

albeit routine cookies for internal purposes only – such disclosure alone would not render the disclosure of PHI lawful. Rather, to comply with HIPAA, the provider must: (a) execute a HIPAA-compliant Business Associate Agreement (“BAA”) with the tracking vendor, and (b) ensure that any disclosure of PHI is based on a permissible purpose under HIPAA (*e.g.*, for treatment, payment, or healthcare operations) or otherwise obtain the patient’s written authorization therefor. Absent both a BAA and an appropriate legal basis, transmitting PHI to a tracking vendor constitutes a HIPAA violation.³⁹

111. Oswego does not meet these requirements. In fact, Oswego operates in a **directly contradictory manner**. Although its Privacy Policy discloses the use of (routine, internal) cookies, Oswego neither (a) notifies Users that their PHI is being disclosed to third parties such as Google, nor (b) obtains the required authorizations from the Users.

112. Instead, Oswego makes categorical assurances that no personal identifiable information is being distributed to third parties without consent, which commitments Oswego plainly does not honor.

113. Oswego’s failure to disclose its actual practices to its Users, coupled with the express denials in its Privacy Policy, further exacerbates Oswego’s failure to comply with HIPAA, as Oswego not only withholds essential information from its Users (*i.e.*, Oswego patients), but also affirmatively misleads them into believing that no such disclosures to third parties exist. Indeed, there is no indication that Oswego has executed a BAA with Google, nor has it obtained HIPAA-compliant authorizations from its Users – and specifically not from Plaintiffs – to permit such disclosures for non-treatment purposes. In effect, Oswego creates the impression that no such

³⁹ See <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html#:~:text=BAA%20is%20required,-,Tracking%20on%20unauthenticated%20webpages,a%20disclosure%20of%20PHI%20and%20is%20subject%20to%20the%20HIPAA%20Rules,-Tracking%20within%20mobile> (last visited Jun. 9, 2026).

authorizations are necessary.

114. Accordingly, Oswego breached its own Privacy Policies by unlawfully intercepting and disclosing Users' Private Information to Google (and likely to other third parties) without obtaining the Users' consent or authorization. These practices amount to a clear violation of HIPAA's requirements governing the use, disclosure, and consent related to PII and PHI, and constitute, *inter alia*, deceptive trade practices and a breach of its contracts with and duties to Plaintiffs and the Class.

E. Oswego Violated HIPAA.

115. Oswego's disclosure of Plaintiffs' and Class Members' Private Information to third party entities like Google violated HIPAA.

116. Under federal law, a healthcare provider may not disclose PHI or related PII about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.⁴⁰

117. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (a) "created or received by a health care provider;" (b) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

118. The Privacy Rule broadly defines protected health information as individually identifiable health information that is "transmitted by electronic media; maintained in electronic

⁴⁰ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

119. Under the HIPAA de-identification rule, “health information is not individually identifiable only if”: (a) 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 (b) “the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

A. Names;

...

H. Medical record numbers;

...

J. Account numbers;

...

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

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

P. Any other unique identifying number, characteristic, or code... and” the covered entity must not “have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”⁴¹

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

121. Even the fact that an individual is receiving a medical service or is a patient of a particular entity can be PHI.

122. HHS has instructed health care providers that, while identifying information alone is not necessarily protected PHI if it were part of a public source such as a phonebook because it

⁴¹ See 45 C.F.R. § 160.514.

is not related to health data, “[i]f such information was listed with health condition, health care provision or payment data, **such as an indication that the individual was treated at a certain clinic**, then this information would be PHI.”⁴²

123. Consistent with this restriction, HHS has issued marketing guidance that provides, “With limited exceptions, **the [Privacy] Rule requires an individual’s written authorization before a use or disclosure of his or her protected health information can be made for marketing.** ... Simply put, **a covered entity may not sell protected health information to a business associate or any other third party for that party’s own purposes.** Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list.”⁴³

124. As detailed above, Oswego provided PII/PHI to third parties in violation of the Privacy Rule, as well as in violation of its own Privacy Policy. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.”

125. The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information ... if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320(d)(6).

126. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where “the offense is committed with intent to sell, transfer, or use individually identifiable health information

⁴² See *Guidance Regarding Methods for De-Identification of Protected Health Information*, *supra* note 9.

⁴³ *Marketing*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html> (last visited Jun. 9, 2026).

for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains individually identifiable health information relating to an individual “shall be fined not more than \$250,000, imprisoned not more than 10 years, or both.” 42 U.S.C. § 1320(d)(6)(b)(1).

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

128. Oswego violated HIPAA by disclosing the PII/PHI of its patients to Google for marketing purposes without the patients’ express written authorization. *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

129. When Users visit Oswego’s Web Properties, they may, *e.g.*, search for medical services, select care centers and providers, request appointments, enter the patient Portals, and pay medical bills, among other things. This information, when combined with identifiers and cookies collected by the DoubleClick and Google Ads tracking technologies installed by Oswego on its Web Properties – which collect device identifiers, IP addresses, and URLs and associate them with the User’s medical information – qualifies as protected PII/PHI because it is (1) individually identifiable and (2) relates to the patient’s health status. By sharing this information with third parties like Google without adequately informing Users or obtaining their consent to do so, Oswego has violated HIPAA.

130. For example, when a User visits Oswego’s Web Properties, DoubleClick’s cookies

and the associated script embed persistent, unique identifiers in the User's browser and transmit them to Google with page-level data. Under 45 CFR §§ 160.103 and 164.514, such "unique identifying number[s], characteristic[s], or code[s]" (including cookies and device IDs) qualify as identifiers. When those identifiers travel in the same payload as the Users' medical service needs, care center selections, or status as a patient of Oswego (as evidenced by the User entering the patient Portal or attempting to pay a bill), the combined dataset becomes protected PII/PHI because the identifiers can be used by third parties to single out the specific User whose health data is implicated. When Oswego allows such information to be transmitted to Google via DoubleClick, it results in a HIPAA violation.⁴⁴

131. Oswego further failed to comply with other HIPAA safeguard regulations as follows:

- a) Failing to ensure the confidentiality and integrity of electronic PII/PHI that Oswego created, received, maintained and transmitted in violation of 45 C.F.R. § 164.306(a)(1);
- b) Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- c) Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Oswego in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- d) Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- e) Failing to protect against reasonably anticipated uses or disclosures of electronic PII/PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3), and
- f) Failing to design, implement and enforce policies and procedures that

⁴⁴ See *Kane v. University of Rochester*, 2024 WL 1178340, 2024 U.S. Dist. LEXIS 48515 (W.D.N.Y. Mar. 19, 2024) (possibility of matching of health data with personal identifiers can effect a HIPAA violation and satisfy the ECPA crime-tort exception).

would establish physical and administrative safeguards to reasonably safeguard PII/PHI in violation of 45 C.F.R. § 164.530(c).

132. In disclosing the content of Plaintiffs and the Class Members' communications, Oswego's conduct was tortious, criminal, and designed to violate federal and state constitutional and statutory provisions.

133. Commenting on a June 2022 report discussing the use of tracking technology by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it ... It is quite likely a HIPAA violation."⁴⁵

134. Oswego's placing third-party tracking codes on its Web Properties is a violation of Plaintiffs' and Class Members' privacy rights under federal and state law. While Plaintiffs do not bring a claim under HIPAA itself, Oswego's HIPAA violations demonstrate Oswego's wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

F. Oswego's Use of Tracking Technologies Violates OCR Guidance.

135. The federal government has issued guidance warning that tracking technologies like those used by Oswego may violate federal privacy law when installed on healthcare websites.

136. Healthcare organizations regulated under HIPAA may use third-party tracking tools *only in a limited way*, to perform analysis on data key to their own operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to third parties.⁴⁶

137. According to the OCR Bulletin, Oswego has violated HIPAA rules by

⁴⁵ ADVISORY BOARD, 'Deeply Troubled': Security experts worry about Facebook trackers on hospital sites, <https://www.advisory.com/daily-briefing/2022/06/17/data-trackers> (last visited Jun. 9, 2026).

⁴⁶ See OCR Bulletin, *supra*, note 8.

implementing the tracking technologies detailed herein.⁴⁷

138. Oswego has shared Plaintiffs’ and Class Members’ Private Information, including their health conditions, medical providers, treatments and/or medications sought, the frequency with whom they take steps to obtain healthcare for certain conditions, and their unique personal identifiers. This information is, as described in the OCR Bulletin, “highly sensitive.”

139. The OCR Bulletin makes clear how broad the government’s view of protected information is, as it explains:

This information might include an individual’s medical record number, home or email address, or dates of appointments, as well as an individual’s IP address or geographic location, medical device IDs, *or any unique identifying code*.⁴⁸

140. And when a User’s PHI is or can be connected with information that can identify the User, the OCR Bulletin makes clear that any and all such information is protected by HIPAA and *cannot* be disclosed without the User’s consent:

If an individual were looking at a hospital’s webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, **the collection and transmission of the individual’s IP address, geographic location, or other identifying information showing their visit to that web page is a disclosure of PHI** to the extent that the information is both identifiable and related to the individual’s health or future health care.⁴⁹

141. As detailed herein, this is exactly what Oswego is doing with its Users’ data.

142. Oswego’s sharing of Users’ Private Information – which included both their PII and PHI – with third parties such as Google violated Plaintiffs’ and Class Members’ rights under applicable law.

⁴⁷ See *id.* (“disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures”).

⁴⁸ *Id.* (emphasis added).

⁴⁹ *Id.* (emphasis added).

G. Oswego Violated Industry Standards.

143. A medical provider’s duty of confidentiality is embedded in the physician-patient and hospital-patient relationship – indeed, it is a cardinal rule.

144. The American Medical Association’s (“AMA”) Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

145. 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)[.]⁵⁰

146. 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-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.⁵¹

147. AMA Code of Medical Ethics Opinion 3.3.2 provides:

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically ... must: (c) Release patient information only in keeping with ethics guidelines for confidentiality and privacy.⁵²

⁵⁰ See <https://code-medical-ethics.ama-assn.org/ethics-opinions/privacy-health-care> (emphasis added) (last visited Jun. 9, 2026).

⁵¹ See <https://code-medical-ethics.ama-assn.org/ethics-opinions/access-medical-records-data-collection-companies> (emphasis added) (last visited Jun. 9, 2026).

⁵² See <https://code-medical-ethics.ama-assn.org/ethics-opinions/confidentiality-electronic-medical-records> (last visited Jun. 9, 2026).

148. Oswego's use of the tracking technologies also violates FTC data security guidelines. The FTC has promulgated numerous guides for businesses, which highlight the importance of implementing reasonable data security practices.

149. The FTC's October 2016 publication *Protecting Personal Information: A Guide for Business*⁵³ established cyber-security guidelines for businesses. These guidelines provide, *inter alia*, that businesses should protect the personal patient information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network vulnerabilities, and implement policies to correct any security problems.

150. In fact, in past years the FTC has brought enforcement actions against several healthcare companies, including Premom, BetterHelp, GoodRx, and Flow Health, for conveying information – or enabling an inference – about their consumers' health to unauthorized third parties without the consumers' consent.

151. Like the health care companies fined by the FTC in recent years, Oswego failed to implement these basic, industry-wide data security practices, and in doing so violated applicable law and the rights of Plaintiffs and Class Members.

H. Oswego Violated New York Standards.

152. New York State has long been a national leader in protecting the confidentiality of personal medical information, and it has established strict privacy standards for medical records.

153. Specifically, New York requires patient consent before a physician can disclose an individual's medical information to another treating physician, and it limits such disclosure to

⁵³ See https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jun. 9, 2026).

immediately relevant information. *See* N.Y. Public Health Law § 18(6).

154. Even stronger protections restrict the release of certain particularly sensitive information regarding genetic tests, mental health, medical treatment of adolescents, sexually transmitted infections, and HIV.⁵⁴

155. Moreover, New York Department of Health regulations governing hospitals impose significant privacy and security standards relating to medical records, patient rights, and medical staff by-laws.

156. With respect to medical records, a hospital must ensure the confidentiality of patient records and release records or information from records “only to hospital staff involved in treating the patient and individuals as permitted by Federal and State laws.” 10 NYCRR § 405.10 (a)(6).

157. This provision has been interpreted to require hospitals to obtain consent from the patient before disclosing medical records to an outside entity, even for treatment or reimbursement purposes.⁵⁵

158. A hospital must also institute safeguards to protect the security of medical records, including a system “to ensure the integrity of the authentication and protect the security of all transmissions, records and record entries” as well as implement policies to ensure the security of electronic or computer equipment from unwarranted access. 10 NYCRR § 405.10 (a)(2).

159. Accordingly, Oswego’s decision to utilize tracking technologies which disclose

⁵⁴ *See, e.g.*, N.Y. Civil Rights Law § 79-l (genetic health); N.Y. Civil Rights Law § 79-j (mental health); New York Public Health Law § 18(1)(e) (mental health); Mental Hygiene Law § 33.13 (mental health); NY eHealth Collaborative Privacy & Security Minor Consent Tiger Team, *Barriers to the Exchange of Pediatric Health Information*, pp. 7-8 (July 2, 2010) (describing numerous state law provisions and state and federal case law that create confidentiality rights for minors seeking health care on their own); N.Y. Public Health Law Chap. 45, § 2306 (sexually transmitted infections); N.Y. Public Health Law Chap. 45, Art. 27-F (HIV).

⁵⁵ *See Williams v. Roosevelt Hospital*, 66 N.Y.2d 391 (1985).

Users' Private Information without their consent violated New York standards as well.

I. Users' Reasonable Expectation of Privacy.

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

161. Indeed, when Plaintiffs and Class Members provided their PII/PHI to Oswego, they each had a reasonable expectation that the information would remain private, and that Oswego would not share their Private Information with third parties for a commercial purpose unrelated to patient care.

162. Had Plaintiffs and Class Members known that Oswego would share their Private Information with third parties such as Google, they never would have used Oswego's Web Properties nor shared their Private Information thereon.

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

164. For example, a Consumer Reports study shows that 92% of Americans believe that Internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.⁵⁶

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

166. Plaintiffs' and Class Members' reasonable expectations of privacy in their PII/PHI

⁵⁶ Consumer Reports, *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds* (May 11, 2017), available at <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/> (last visited Jun. 9, 2026).

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

167. Oswego's used of tracking technologies on its Web Properties, which led to the unauthorized disclosure of Users' Private Information without their consent, violated the Users' expectation of privacy.

J. Unique Personal Identifiers Are Protected Health Information.

168. As described above, HIPAA sets forth policies designed to protect the privacy and confidentiality of all individually identifiable health information that is held or transmitted by a covered entity.

169. While not all health or personal data is covered under HIPAA, the law specifically applies to health information that is or can be directly associated with an individual (PHI) and that is held by healthcare providers, health insurance providers, and healthcare data clearinghouses.⁵⁷

170. Additionally, HIPAA lists approximately eighteen (18) "identifiers" which either identify or can be used to identify, contact, or locate an individual, alone or in combination with other sources. These identifiers, which include names, geographic information (street address, city, county, and zip code), dates related to an individual, email addresses, device identifiers, web

⁵⁷ See Alfred Ng & Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids' Information to Facebook* (June 21, 2022), <https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook> (stating that "[w]hen you are going to a covered entity's website, and you're entering information related to scheduling an appointment, including your actual name, and potentially other identifying characteristics related to your medical condition, there's a strong possibility that HIPAA is going to apply in those situations") (last visited Jun. 9, 2026).

URLs, and IP addresses, are considered PII and are protected by HIPAA if they are or can be linked to an individual's health-related data.⁵⁸

171. As described above, the information disclosed to Google (and potentially other third parties) by Oswego included not only its Users' generic medical information – *i.e.*, the medical services and providers they sought and selected, their status as an Oswego patient, the medical conditions they researched, and the medical advice they sought, among other things – but also a number of HIPAA identifiers connected therewith – *i.e.*, their names, geographic information, email addresses, dates they sought treatment, telephone numbers, computer IP addresses, device identifiers, and web URLs visited.

172. Because this information was produced together and connects (or can be used to connect), for example, the treatment sought with the individual User who sought the treatment, it is all protected by HIPAA and cannot be disclosed without the Users' consent. *See* 45 C.F.R. § 164.514(2)(ii) (information is protected as personally identifiable when it “could be used alone or in combination with other information to identify an individual who is a subject of the information”).

173. Consequently, Oswego's disclosure of Plaintiffs' and Class Members' PII in connection with their PHI also violated HIPAA and industry-wide privacy standards.

K. Oswego Was Enriched & Benefitted from Its Use of Tracking Technologies.

174. One of the primary reasons that Oswego decided to embed tracking technologies on its Web Properties was to improve marketing by creating targeted advertising campaigns that maximize conversions and thereby decrease costs to Oswego and boost its revenues.

175. This process works as follows. The tracking technologies installed by Oswego on

⁵⁸ *Guidance Regarding Methods for De-identification of Protected Health Information*, *supra* note 8.

its Web Properties, specifically Double Click and Google Ads, collect and share with Google information communicated to Oswego by Users via Oswego's Web Properties, including the Users' PII/PHI. Google analyzes this information for specific data points, such as how Users interact with the Web Properties and which Website and Portal features are most frequently used. Google then shares its analysis with Oswego, which provides Oswego with a commercial benefit (e.g., permitting Oswego to optimize the functionality of its Web Properties).

176. Oswego also receives additional commercial benefits from using Google's tracking technologies, such as being able to serve targeted advertisements to existing and prospective patients through a process known as "retargeting."

177. Retargeting is a form of online marketing that targets Users with ads based on their previous Internet communications and interactions. Retargeting operates by tracking Users' web activity via tracking code and cookies and placing targeted ads on other websites which Users may visit later.⁵⁹

178. Here, for example, if a User were to search for and click on a specific doctor or medical condition on Oswego's Web Properties, that information is sent to Google, who can then target that User with ads about that doctor or condition for Oswego's benefit. Google can also target the User with ads about another doctor or medication that can treat the condition, who potentially has paid Google to place such a targeted ad. Google can also use its data on the User to find more individuals with traits similar to the User, and who are thus more likely to use Oswego – or another sponsored facility, doctor, or medication – in a similar manner, and target those new

⁵⁹ Medico Digital Insights, *The complex world of healthcare retargeting*, available at <https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/> (last visited Jun. 9, 2026).

individuals with customized, targeted ads.⁶⁰

179. Through this process, the tracking technologies used by Oswego load and capture as much data as possible whenever a User loads the Oswego Web Properties. The information the tracking technologies capture “includes URL names of pages visited, and actions taken – all of which could be potential examples of health information.”⁶¹

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

181. In exchange for disclosing the Private Information of their account holders and patients, Oswego is compensated by Google in the form of enhanced advertising services and more cost-efficient marketing on its platform.

182. But companies have started to warn about the potential HIPAA violations associated with using tracking technologies because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.⁶²

183. For example, Medico Digital warns that “retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences.”⁶³

184. Oswego retargeted patients and potential patients, including Plaintiffs and Class

⁶⁰ See, e.g., *How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023), <https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking> (last visited Jun. 9, 2026).

⁶¹ *Id.*

⁶² See *The guide to HIPAA compliance in analytics*, <https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf> (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Jun. 9, 2026).

⁶³ *The complex world of healthcare retargeting*, *supra* note 59.

Members.

185. Thus, utilizing the tracking technologies commercially benefitted Oswego by, among other things, helping it to optimize its Web Properties and reducing its cost of advertising via retargeting.

L. Plaintiffs’ and Class Members’ Private Information is Extremely Valuable.

186. Plaintiffs’ and Class Members’ Private Information had value, and Oswego’s unlawful interception and disclosure thereof harmed Plaintiffs and the Class by not compensating them for the value of their Private Information and, in turn, decreasing the value of their Private Information.

187. Tech companies are under particular scrutiny because they already have access to a massive trove of information about people, which information they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

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

189. The market for Internet user data has been analogized to the “oil” of the tech industry.⁶⁴ A 2015 article from TechCrunch accurately noted that “data has become a strategic asset that allows companies to acquire or maintain a competitive edge.”⁶⁵ That article noted that the value of a single Internet user – or really, a single user’s data – varied from about \$15 to more than \$40.

190. Conservative estimates suggest that in 2018, Internet companies earned \$202 per

⁶⁴ See <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (last visited Jun. 9, 2026).

⁶⁵ See <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/> (last visited Jun. 9, 2026).

American user from mining and selling data (after costs).⁶⁶ 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.

191. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: “Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.”⁶⁷

192. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize their own data. Indeed, numerous companies, such as PermissionResearch and Smart Panel, **will pay Internet users cash money for their data.**⁶⁸

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

194. Courts have recognized the value of personal information and the harm when it is disclosed without consent. *See, e.g., In re Facebook Privacy Litig.*, 572 F. App’x 494, 494 (9th Cir. 2014) (holding that plaintiffs’ allegations that they were harmed by the dissemination of their

⁶⁶ See Robert J. Shapiro, *What Your Data is Really Worth to Facebook* (Jul. 12, 2019), <https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/> (last visited Jun. 9, 2026).

⁶⁷ Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

⁶⁸ See Kevin Mercandante, *10 Apps for Selling Your Data for Cash*, <https://wallethacks.com/apps-for-selling-your-data/> (last visited Jun. 9, 2026).

personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing “the value that personal identifying information has in our increasingly digital economy”).

195. Healthcare data is particularly valuable on the black market because it often contains both an individual’s PII and medical conditions, as opposed to a single piece of information that may be found in a financial breach.

196. Moreover, unlike a stolen credit card that can be canceled, most people are unaware that their medical information has been stolen and sold. Even once detected, it can take years to undo the damage caused.

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

198. Specifically, in 2023, the Value Examiner published a report entitled *Valuing Healthcare Data*. The report focused on the rise in providers, software firms, and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of “such data should ensure it is priced at fair market value to mitigate any regulatory risk.”⁶⁹

199. Trustwave Global Security published a report entitled *The Value of Data*. With respect to healthcare data records, the report found that they may be valued at up to \$250 per record on the black market, compared to \$5.40 for the next highest value record (a payment card).⁷⁰

⁶⁹ See <https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf> (last visited Jun. 9, 2026).

⁷⁰ See <https://www.imprivata.com/blog/healthcare-data-new-prize-hackers> (last visited Jun. 9, 2026) (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

200. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled “How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry,” in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.⁷¹

201. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-identified patient data has become its own small economy: There’s a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers.”⁷²

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

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

204. In short, there is a quantifiable economic value to Internet users’ data, including Plaintiffs’ and Class Members’, that is greater than zero. The exact value of that information in this case will be a matter for experts to determine in the course of discovery.

205. Here, however, Oswego simply gave away Plaintiffs’ and Class Members’ communications and transactions via its Web Properties to a third-party advertiser, without their permission.

206. The unauthorized access to Plaintiffs’ and Class Members’ personal and Private Information has diminished the value of that information, resulting in harm to Users of Oswego’s Web Properties, including Plaintiffs and Class Members.

⁷¹ See <https://time.com/4588104/medical-data-industry/> (last visited Jun. 9, 2026).

⁷² See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited Jun. 9, 2026).

207. Plaintiffs have a continuing interest in ensuring that their future communications with Oswego are protected and safeguarded from future unauthorized disclosure.

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

A. Plaintiff Eva Perry

208. Plaintiff Eva Perry has been an Oswego patient for approximately four years.

209. Beginning in or around 2022, Plaintiff Perry began utilizing Oswego's Web Properties – both the Website and the patient Portals – via her Android phone and personal computer, *inter alia*, to search for and receive healthcare services from Oswego, at Oswego's direction.

210. As a condition of receiving Oswego's services, Plaintiff Perry disclosed her Private Information to Oswego beginning in 2022 and as recently as May 2026.

211. Plaintiff Perry logged onto the Oswego patient Portals; viewed appointments with her providers via the Portals; viewed her medical records, test results, and bills; and communicated with her providers via the Portals.

212. Plaintiff Perry also searched for medical providers and office locations/addresses on the Oswego Website, and she searched for information and treatment options for medical conditions from which she suffers.⁷³

213. In so doing, Plaintiff Perry disclosed to Oswego information about her specific medical conditions, providers, location, patient status, and the treatments she sought via Oswego's Web Properties.

214. Plaintiff Perry has used and continues to use the same devices throughout the

⁷³ The names of Plaintiffs' medical providers, as well as their specific medical conditions and treatments, have been withheld in an effort to protect Plaintiffs' privacy and the additional disclosure of their Private Information.

relevant time period in this case. Plaintiff Perry also has used, and continues to use, these devices to access her active Google account.

215. Plaintiff Perry reasonably expected that her communications with Oswego via its Website and Portals were confidential, solely between herself and Oswego, and that such communications would not be transmitted to or intercepted by a third party.

216. Plaintiff Perry provided her Private Information to Oswego and trusted that the information would be safeguarded according to Oswego's policies and state and federal law.

217. As described herein, Oswego worked along with Google to intercept Plaintiff Perry's communications with Oswego's Web Properties, including those that contained and/or constituted Private and confidential information.

218. Oswego willfully facilitated these interceptions without Plaintiff Perry's knowledge, consent, or express written authorization.

219. Oswego transmitted to Google Plaintiff Perry's computer IP address, device identifiers, physical location, and patient status, in conjunction with information such as her medical services, treatments, providers, and office locations sought and selected, appointment types, and various searches and button/menu selections.

220. By doing so without her consent, Oswego breached Plaintiff Perry's right to privacy and unlawfully disclosed her Private Information.

221. Oswego did not inform Plaintiff Perry that it had shared her Private Information with Google.

222. After disclosing her private medical information to Oswego, Plaintiff Perry began receiving targeted ads on her web browser relating to Oswego and/or her medical conditions, providers, and treatment.

223. Plaintiff Perry suffered damages in the form of, *inter alia*, (a) invasion of privacy; (b) violation of confidentiality of her Private Information; (c) loss of benefit of the bargain; (d) diminution of value of the Private Information; (e) statutory damages; and (f) the continued and ongoing risk to her Private Information.

224. Plaintiff Perry has a continuing interest in ensuring that her Private Information is protected and safeguarded from future unauthorized disclosure.

225. In connection with her ongoing medical care, Plaintiff Perry continues to use Oswego's Website and patient Portal, and she will need to do so in the future. Plaintiff Perry has an interest in ensuring that her Private Information communicated to Oswego's Web Properties in the future is also protected and safeguarded from unauthorized disclosure.

B. Plaintiff Jacqueline Fletcher

226. Plaintiff Jacqueline Fletcher has been an Oswego patient since at least 2019.

227. Beginning in or around 2019, Plaintiff Fletcher began utilizing Oswego's Web Properties – both the Website and the patient Portals – via her Android phone, *inter alia*, to search for and receive healthcare services from Oswego, at Oswego's direction.

228. As a condition of receiving Oswego's medical services, Plaintiff Fletcher disclosed her Private Information to Oswego via its Web Properties as recently as May 2026.

229. Plaintiff Fletcher logged onto the Oswego patient Portals; scheduled and viewed appointments with her providers via the Portals; looked up her medical records, test results, and bills; and communicated with her providers via the Portals.

230. Plaintiff Fletcher searched for medical providers and office locations/addresses on the Oswego Website, and she searched for information and treatment options for medical conditions from which she suffers.

231. In so doing, Plaintiff Fletcher disclosed to Oswego information about her specific medical conditions, providers, location, patient status, and the treatments she sought via Oswego's Web Properties.

232. Plaintiff Fletcher has used and continues to use the same device throughout the relevant time period in this case.

233. Plaintiff Fletcher reasonably expected that her communications with Oswego via the Website and Portals were confidential, solely between herself and Oswego, and that such communications would not be transmitted to or intercepted by a third party.

234. Plaintiff Fletcher provided her Private Information to Oswego and trusted that the information would be safeguarded according to Oswego's policies and state and federal law.

235. As described herein, Oswego worked along with Google to intercept Plaintiff Fletcher's communications with Oswego's Web Properties, including those that contained Private and confidential information.

236. Oswego willfully facilitated these interceptions without Plaintiff Fletcher's knowledge, consent, or express written authorization.

237. Oswego transmitted to Google Plaintiff Fletcher's computer IP address, device identifiers, physical location, and patient status, in conjunction with information such as her medical services, treatments, providers, and office locations sought and selected, appointment types, and various searches and button/menu selections.

238. By doing so without her consent, Oswego breached Plaintiff Fletcher's right to privacy and unlawfully disclosed her Private Information.

239. Oswego never informed Plaintiff Fletcher that it had shared her Private Information with Google.

240. After disclosing her private medical information to Oswego, Plaintiff Fletcher began receiving targeted ads on her web browser relating to Oswego and/or her medical conditions, providers, and treatment.

241. Plaintiff Fletcher suffered damages in the form of, *inter alia*, (a) invasion of privacy; (b) violation of confidentiality of her Private Information; (c) loss of benefit of the bargain; (d) diminution of value of her Private Information; (e) statutory damages; and (f) the continued and ongoing risk to her Private Information.

242. Plaintiff Fletcher has a continuing interest in ensuring that her Private Information is protected and safeguarded from future unauthorized disclosure.

243. In connection with her ongoing medical care, Plaintiff Fletcher continues to use Oswego's Website and patient Portal, and she will need to do so in the future. Plaintiff Fletcher has an interest in ensuring that her Private Information communicated to Oswego's Web Properties in the future is also protected and safeguarded from unauthorized disclosure.

C. Plaintiff Debra L. Gilmore

244. Plaintiff Debra L. Gilmore has been an Oswego patient for many years.

245. Beginning in or around 2021, Plaintiff Gilmore began utilizing Oswego's Web Properties – both the Website and the patient Portals – via her Android phone, *inter alia*, to search for and receive healthcare services from Oswego, at Oswego's direction.

246. As a condition of receiving Oswego's medical services, Plaintiff Gilmore disclosed her Private Information to Oswego via its Web Properties as recently as June 2026.

247. Plaintiff Gilmore logged onto the Oswego patient Portals; viewed appointments with her providers via the Portals; looked up her medical records, test results, and bills; and communicated with her providers via the Portals.

248. Plaintiff Gilmore searched for medical providers and office locations/addresses on

the Oswego Website, and she searched for information and treatment options for medical conditions from which she suffers.

249. In so doing, Plaintiff Gilmore disclosed to Oswego information about her specific medical conditions, providers, location, patient status, and the treatments she sought via Oswego's Web Properties.

250. Plaintiff Gilmore has used and continues to use the same device throughout the relevant time period in this case.

251. Plaintiff Gilmore reasonably expected that her communications with Oswego via the Website and Portals were confidential, solely between herself and Oswego, and that such communications would not be transmitted to or intercepted by a third party.

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

253. As described herein, Oswego worked along with Google to intercept Plaintiff Gilmore's communications with Oswego's Web Properties, including those that contained Private and confidential information.

254. Oswego willfully facilitated these interceptions without Plaintiff Gilmore's knowledge, consent, or express written authorization.

255. Oswego transmitted to Google Plaintiff Gilmore's computer IP address, device identifiers, physical location, and patient status, in conjunction with information such as her medical services, treatments, providers, and office locations sought and selected, appointment types, and various searches and button/menu selections.

256. By doing so without her consent, Oswego breached Plaintiff Gilmore's right to privacy and unlawfully disclosed her Private Information.

257. Oswego never informed Plaintiff Gilmore that it had shared her Private Information with Google.

258. After disclosing her private medical information to Oswego, Plaintiff Gilmore began receiving targeted ads on her web browser relating to Oswego and/or her medical conditions, providers, and treatment.

259. Plaintiff Gilmore suffered damages in the form of, *inter alia*, (a) invasion of privacy; (b) violation of confidentiality of her Private Information; (c) loss of benefit of the bargain; (d) diminution of value of her Private Information; (e) statutory damages; and (f) the continued and ongoing risk to her Private Information.

260. Plaintiff Gilmore has a continuing interest in ensuring that her Private Information is protected and safeguarded from future unauthorized disclosure.

261. In connection with her ongoing medical care, Plaintiff Gilmore continues to use Oswego's Website and patient Portal, and she will need to do so in the future. Plaintiff Gilmore has an interest in ensuring that her Private Information communicated to Oswego's Web Properties in the future is also protected and safeguarded from unauthorized disclosure.

TOLLING

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

CLASS ACTION ALLEGATIONS

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

264. Plaintiffs seek certification of a class (the "Class" and each member thereof, a

“Class Member”) defined as follows:

All Oswego patients who visited Oswego’s Web Properties and whose Private Information was disclosed to a third party without their authorization or consent.

265. Plaintiffs also seek certification of a subclass defined as follows:

All Oswego patients who visited Oswego’s Web Properties and performed one of the following actions thereon:

- **Searched for medical providers;**
- **Searched for medical facilities or locations;**
- **Searched for medical services;**
- **Accessed the patient Portals;**
- **Clicked to pay a bill online;**
- **Clicked the “Ways to Give” link;**
- **Clicked the “Wellness Resources” link; and/or**
- **Typed a search query into the Website’s search bar.**

266. The class and subclass are collectively referred to herein as the “Classes.” Excluded from the Classes are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign and any Judge who adjudicates this case, including their staff and immediate family.

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

268. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are over 50,000 individuals whose PII and PHI were improperly disclosed to third parties by Defendant, and the Class is identifiable within Defendant’s records. The vast majority of the Class Members are believed to be New York residents.

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

include:

- a. Whether and to what extent Defendant had a duty to protect Plaintiffs' and Class Members' Private Information;
- b. Whether Defendant had a duty not to disclose Plaintiffs' and Class Members' Private Information to unauthorized third parties;
- c. Whether Defendant violated legal standards by disclosing Plaintiffs' and Class Members' Private Information to Google or other third parties;
- d. Whether Defendant violated its privacy policy by disclosing Plaintiffs' and Class Members' Private Information to Google or other third parties;
- e. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;
- f. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been disclosed and/or compromised;
- g. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;
- h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Private Information;
- i. Whether Defendant violated the consumer protection statutes invoked herein;
- j. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;
- k. Whether Defendant knowingly omitted material facts with respect to its data security and/or privacy policy practices;
- l. Whether Defendant's acts and practices violated Plaintiffs' and Class Members' privacy rights;
- m. Whether Plaintiffs and Class Members are entitled to actual, consequential, statutory, or nominal damages as a result of Defendant's wrongful conduct;
- n. Whether Defendant knowingly made false representations as to its data

security and/or privacy policy practices; and

- o. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their Private Information.

270. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised and disclosed to third parties as a result of Defendant's use of the tracking technologies, due to Defendant's misfeasance.

271. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class, and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

272. **Superiority and Manageability.** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a defendant with significant resources like Oswego. 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.

273. **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 Plaintiffs' 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 Plaintiffs.

274. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class member with its 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 Plaintiffs 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.

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

276. **Ascertainability & Notice.** Membership in the Class can be determined by objective records maintained by Defendant, and adequate notice can be given to Class Members directly using information maintained in Defendant's records.

277. **Class-wide Injunctive Relief.** Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth herein.

278. 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.

279. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information;
- b. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information with respect to Defendant's privacy policy;
- c. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using and safeguarding their Private Information;
- d. Whether Defendant failed to comply with its own policies, applicable laws, regulations and industry standards relating to data security;
- e. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;
- f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties; and
- g. Whether Class Members are entitled to actual, consequential, statutory, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

NEW YORK LAW SHOULD APPLY TO PLAINTIFFS & THE CLASS AS A WHOLE

280. The State of New York has a significant interest in regulating the conduct of businesses operating within its borders.

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

282. The principal place of business and headquarters of Oswego, located at 110 W. Sixth St. in Oswego, New York 13126, is the “nerve center” of its business activities – the place where its high-level officers direct, control, and coordinate Defendant’s activities, including major policy decisions.

283. Defendant’s actions and corporate decisions surrounding the allegations made herein were made from and in New York.

284. Defendant’s breaches of duty to Plaintiffs and Class Members emanated from New York.

285. Application of New York law to the Class with respect to Plaintiffs’ and Class Members’ claims is neither arbitrary nor fundamentally unfair because New York has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Class.

286. Under New York’s choice of law principles, which are applicable to this action, the common law of New York applies to the nationwide common law claims of all Class Members.

287. New York has a significant interest in regulating the conduct of businesses operating within its borders. New York also has the most significant relationship to Defendant, as

it is headquartered in New York, its executives and officers are located in New York and the decisions giving rise to the allegations and claims asserted herein were made in New York. Thus, there is no conflict in applying New York law to non-resident consumers such as some of the potential Class Members.

CAUSES OF ACTION

COUNT I

Violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.* Unauthorized Interception, Use and Disclosure

288. Plaintiffs and Class Members repeat and re-allege the allegations in paragraphs 1-287 as if fully set forth herein.

289. The Electronic Communications Privacy Act (“ECPA”) prohibits the intentional interception, or the attempted or procured interception, of any wire, oral, or electronic communication. 18 U.S.C. § 2511(1)(a).

290. The ECPA protects both sent and received communications.

291. The ECPA, specifically 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.

292. Under the ECPA, a court may award as damages whichever is the greater of (a) the actual damages suffered by the plaintiff and any profits made by the defendant as a result of the violation, or (b) statutory damages of whichever is the greater of \$100 a day for each day of the violation or \$10,000. 18 U.S.C. § 2520(c)(2).

293. The transmissions of Plaintiffs’ and Class Members’ communications and information, which included Private Information, to Oswego via Oswego’s Web Properties is a “communication” under the ECPA’s definition under 18 U.S.C. § 2510(12).

294. Moreover, such transmissions constitute “transfer[s] of signs, signals, writing, ... data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce” and are therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(2).

295. 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).

296. The ECPA defines “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).

297. The ECPA defines “electronic, or other device” as “any device ... which can be used to intercept a[n] ... electronic communication[.]” 18 U.S.C. § 2510(5).

298. The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- a. The cookies Oswego and Google use to track Users’ communications;
- b. Users’ browsers;
- c. Users’ computing devices;
- d. Oswego’s servers for its Web Properties; and
- e. The tracking technologies, specifically DoubleClick and Google Ads, deployed by Oswego to effectuate the sending and acquisition of Users’ and patients’ sensitive and private communications.

299. Plaintiffs and Class Members’ interactions with Oswego’s Web Properties are electronic communications under the ECPA.

300. By utilizing and embedding tracking technologies such as DoubleClick and Google Ads on their Web Properties and/or servers, Oswego intentionally intercepted, endeavored to intercept, and/or procured another person to intercept the electronic communications of Plaintiffs

and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

301. Specifically, Oswego intercepted Plaintiffs' and Class Members' electronic communications via DoubleClick and Google Ads, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Private Information to Google and other third parties.

302. Oswego intercepted communications that included, but are not limited to, communications to/from Plaintiffs and Class Members regarding their PII and PHI, including first and last name, email address, IP address, and health information relevant to Plaintiffs' and Class Members' medical conditions and treatment.

303. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to Google and other 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), Oswego violated 18 U.S.C. § 2511(1)(c).

304. By intentionally using or endeavoring to use the contents of the electronic communications of Plaintiffs 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), Oswego violated 18 U.S.C. § 2511(1)(d).

305. Oswego is a "party to the communication" with respect to patient communications. However, the so-called "crime-tort exception" applies here because Oswego intercepted the contents of Plaintiffs' and Class Members' electronic communications for the independent purpose of committing criminal and tortious acts in violation of the Constitution or laws of the United States or of any State – namely, to violate HIPAA, to breach its contracts with and fiduciary and confidentiality duties owed to Plaintiffs and Class Members, and to invade their privacy, among

others. 18 U.S.C. § 2511(2)(d).

306. Specifically, by the acts alleged herein, Oswego knowingly and intentionally intercepted the contents of Plaintiffs’ and Class Members’ electronic communications, which included their Private Information, without their knowledge or consent, for the express purpose of sharing those communications and private information with Google, which is a crime in violation of HIPAA.

307. New York federal courts have generally held that the unauthorized disclosure of Private Information to third-party advertising platforms for profit is a criminal act under HIPAA, which invokes the ECPA crime-tort exception and overcomes the one-party consent rule. *See, e.g., Cooper v. Mount Sinai Health System*, 742 F. Supp. 3d 369 (S.D.N.Y. July 30, 2024) (transmitting PHI to Meta for advertising constituted “an independent criminal act under HIPAA,” satisfying the ECPA crime-tort exception); *Kane v. University of Rochester*, 2024 WL 1178340, 2024 U.S. Dist. LEXIS 48515 (W.D.N.Y. Mar. 19, 2024) (using Meta Pixel to transmit patients’ PHI and PII to Facebook for marketing profit plausibly alleged an ECPA interception); *Gay v. Garnet Health*, 2024 WL 4203263, 2024 U.S. Dist. LEXIS 168515 (S.D.N.Y. Sept. 16, 2024) (using tracking pixels to forward PHI and PII to Facebook and Google for profit sustained the ECPA claim); *Pattison v. Teladoc Health, Inc.*, 2025 WL 1756364, 2025 U.S. Dist. LEXIS 121044 (S.D.N.Y. June 25, 2025) (disclosure of PHI to Facebook and Google “for the purpose of violating HIPAA” independently triggered the crime-tort exception).

308. Moreover, Oswego intentionally used tracking technologies such as DoubleClick and Google Ads to intercept, track, and utilize Plaintiffs’ and Class Members’ wire and electronic communications, which included their Private Information, to increase its profit margins and for its own financial benefit.

309. Oswego was not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communications.

310. Plaintiffs and Class Members did not authorize Oswego to acquire the content of their communications for purposes of invading Plaintiffs' and Class Members' privacy via the tracking technologies such as DoubleClick and Google Ads.

311. Any purported consent that Oswego received from Plaintiffs and Class Members was not valid.

312. In intercepting and transmitting to third parties the content of Plaintiffs' and Class Members' communications relating to the browsing of Oswego's Web Properties, including researching providers, medical conditions, and treatment, accessing the patient Portals, and typing queries in the search bar, Oswego's purpose was criminal and tortious and designed to violate federal and state law, including as described above, a knowing intrusion into a private place, and conversation of matter that would be highly offensive to a reasonable person.

313. Oswego's acquisition of patient communications that were used and disclosed to Google and other third parties was also done for purposes of committing criminal and tortious acts in violation of the laws of the United States and New York (as described *infra*).

314. Consumers have the right to rely upon the promises that companies make to them. Oswego accomplished its tracking through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that caused Google tracking technologies and cookies (including but not limited to the IDE, DSID, 3PSID, 3PAPISID, 3PSIDCC, and NID cookies) to be deposited on Plaintiffs' and Class members' computing devices.

315. Oswego's scheme or artifice to defraud in this action consists of:

- a. the false and misleading statements and omissions in its privacy policies set forth above, including the statements and omissions recited in the

breach of contract and negligence claims below; and/or

- b. the placement of Google cookies on patient computing devices, which cookies were disguised as first-party cookies from Oswego so that they would not be blocked.

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

- a. property rights to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and
- b. property rights to determine who has access to their computing devices.

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

- a. with knowledge that (1) Oswego did not have the right to share such data without written authorization; (2) courts had determined that a healthcare providers' use of tracking technologies gave rise to claims for invasion of privacy and violations of state criminal statutes; (3) a reasonable user would not understand that Google was collecting their Private Information based on their activities on Oswego's Web Properties; and (4) the subsequent use of health information for advertising was a further invasion of such property rights in making their own exclusive use of their Private Information for any purpose not related to the provision of their healthcare; and
- b. with the intent to (1) acquire Plaintiffs and Class Members' Private Information without their authorization and without their healthcare providers or covered entities obtaining the right to share such information; (2) use Plaintiffs' and Class Members' Private Information without their authorization and (3) gain access to Plaintiffs' and Class Members' personal computing devices through hidden and disguised tracking technologies and cookies.

318. As a direct and proximate result of Oswego's violation of the ECPA, Plaintiffs and Class Members were damaged by Oswego's conduct.

319. Plaintiffs, individually, on behalf of the Class Members, seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages, punitive damages,

preliminary and other equitable or declaratory relief, and attorneys' fees and costs.

COUNT II
Negligence

320. Plaintiffs and Class Members repeat and re-allege the allegations in paragraphs 1-287 as if fully set forth herein.

321. Upon accepting, storing, and controlling the Private Information of Plaintiffs and the Class, Oswego owed – and continues to owe – a duty to Plaintiffs and the Class to exercise reasonable care to secure, safeguard, and protect their highly sensitive Private Information.

322. Oswego breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

323. It was reasonably foreseeable that Oswego's failures to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information through their use of DoubleClick, Google Ads, and other tracking technologies would result in unauthorized third parties – such as the Google – gaining unlawful access to such Private Information.

324. Oswego's duty of care to use reasonable measures to secure and safeguard Plaintiffs' and Class Members' Private Information arose due to the special relationship that existed between Oswego and its patients, which is recognized by statute, regulations and the common law.

325. In addition, Oswego had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for but to any entity that may have access to healthcare information about a patient that – if it were to fall into the wrong hands – could present a risk of harm to the patient's finances or reputation.

326. Oswego's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Private Information. Oswego's misconduct included the failure to (a) secure Plaintiffs' and Class Members' Private Information; (b) comply with industry-standard data security practices; (c) implement adequate Web Properties and event monitoring; and (d) implement the systems, policies and procedures necessary to prevent unauthorized disclosures resulting from the use of DoubleClick, Google Ads, and other tracking technologies.

327. As a direct result of Oswego's breach of their duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class Members' Private Information, Plaintiffs and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

328. Oswego's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiffs' and Class Members' Private Information constituted (and continues to constitute) negligence at common law.

329. Plaintiffs and the Class are entitled to recover damages in an amount to be determined at trial.

COUNT III **Breach of Implied Contract**

330. Plaintiffs and Class Members repeat and re-allege the allegations in paragraphs 1-287 as if fully set forth herein.

331. Oswego required Plaintiffs and Class Members to provide their Private Information, including their names, email addresses, phone numbers, computer IP addresses, appointment information, and other content submitted to Oswego's Web Properties as a condition

of their using such Web Properties and receiving healthcare services from Oswego.

332. When Plaintiffs and Class Members provided their data to Oswego in exchange for these services, they entered into an implied contract pursuant to which Oswego agreed to safeguard and not disclose their Private Information without consent.

333. Plaintiffs and Class Members accepted Oswego's offers and provided their Private Information to Oswego.

334. Plaintiffs and Class Members fully performed their obligations under the contract with Oswego.

335. Oswego's relevant privacy policies and representations require it to take appropriate steps to safeguard the Private Information entrusted to it by the Plaintiffs and Class Members.

336. Oswego breached these agreements, which directly and/or proximately caused Plaintiffs and Class Members to suffer damages, including nominal damages.

337. Plaintiffs and Class Members would not have entrusted Oswego with their Private Information in the absence of an implied contract between them and Oswego obligating them not to disclose this Private Information without consent.

338. Oswego breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information to third parties, including Google.

339. As a direct and proximate result of Oswego's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members would not have used Oswego's Web Properties or services had they known their Private Information would be disclosed.

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

damages because of Oswego's breach of implied contract.

COUNT IV
Breach of Fiduciary Duty

341. Plaintiffs and Class Members repeat and re-allege the allegations in paragraphs 1-287 as if fully set forth herein.

342. A relationship existed between Plaintiffs and Class Members on the one hand and Oswego on the other, in which Plaintiffs and Class Members put their trust in Oswego to protect their Private Information, and Oswego accepted that trust.

343. Oswego breached the fiduciary duty that it owed to Plaintiffs and Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and instead intentionally disclosing, the Private Information of Plaintiffs and Class Members.

344. Oswego's breach of fiduciary duty was a legal cause of damage to Plaintiffs and Class Members.

345. But for Oswego's breach of fiduciary duty, the damage to Plaintiffs and Class Members would not have occurred.

346. Oswego's breach of fiduciary duty contributed substantially to producing the damage to Plaintiffs and Class Members.

347. As a direct and proximate result of Oswego's breach of fiduciary duty, Plaintiffs and Class Members are entitled to and do demand actual, consequential and/or nominal damages, injunctive relief, and all other relief allowed by law.

COUNT V
Unjust Enrichment

348. Plaintiffs and Class Members repeat and re-allege the allegations in paragraphs 1-

287 as if fully set forth herein.

349. Oswego benefited from Plaintiffs' and Class Members' Private Information and unjustly retained those benefits at Plaintiffs' and Class Members' expense.

350. Plaintiffs and Class Members conferred a benefit upon Oswego in the form of the monetizable Private Information that Oswego collected from them and disclosed to third parties, including Google, without authorization and proper compensation.

351. Oswego consciously collected and used this information for its own gain, providing Oswego with economic, intangible and other benefits, including substantial monetary compensation and increased advertising efficiencies.

352. Oswego unjustly retained those benefits at the expense of Plaintiffs and Class Members because Oswego's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiff or Class members.

353. The benefits that Oswego derived from Plaintiffs and Class Members were not offered by Plaintiff or Class members gratuitously and, thus, rightly belong to Plaintiffs and Class Members.

354. It would be inequitable under unjust enrichment principles and in New York for Oswego to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

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

COUNT VI
Breach of Confidence

356. Plaintiffs and Class Members repeat and re-allege the allegations in paragraphs 1-

287 as if fully set forth herein.

357. Medical providers, such as Oswego, have a duty to their patients to keep non-public medical information confidential.

358. Plaintiffs and Class Members had reasonable expectations of privacy in the responses and communications entrusted to Oswego through their Web Properties, which included highly sensitive Private Information.

359. Contrary to their duties as health care institutions and their express promises of confidentiality, Oswego installed the tracking technologies DoubleClick and Google Ads to collect, disclose, and transmit to third parties Plaintiffs' and Class Members' Private Information, including data relating to Plaintiffs' and Class Members' health.

360. These disclosures were made without Plaintiffs' or Class members' knowledge, consent, or authorization.

361. The third-party recipients included, but may not be limited to, Google.

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

363. As a direct and proximate cause of Oswego's unauthorized disclosures of Plaintiffs' and Class Members' Private Information, Plaintiffs and Class Members were damaged by Oswego's breach of confidentiality in that (a) sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private; (b) Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements; (c) Oswego eroded the essential confidential nature of health services that Plaintiffs and Class Members participated in; (d) general damages for invasion of their rights in an amount to be determined by a jury at trial; (e) nominal damages for each independent violation;

(f) the unauthorized use of something of value (the highly sensitive Private Information) that belonged to Plaintiffs and Class Members and the obtaining of a benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation to Plaintiff or Class members for the unauthorized use of such data; (g) diminishment of the value of Plaintiffs' and Class Members' Private Information; and (h) violation of property rights Plaintiffs and Class Members have in their Private Information.

COUNT VII
Constructive Bailment

364. Plaintiffs and Class Members repeat and re-allege the allegations in paragraphs 1-287 as if fully set forth herein.

365. Oswego acquired and was obligated to safeguard the Private Information of Plaintiffs and Class Members.

366. Oswego accepted possession and took control of Plaintiffs' and Class Members' Private Information under such circumstances that the law imposes an obligation to safeguard the property of another.

367. Specifically, a constructive bailment arises when Oswego, as is the case here, takes lawful possession of the property of another and has a duty to account for that property, without intending to appropriate it.

368. Constructive bailments do not require an express assumption of duties and may arise from the bare fact of the thing coming into the actual possession and control of a person fortuitously or by mistake as to the duty or ability of the recipient to affect the purpose contemplated by the absolute owner.

369. During the constructive bailment, Oswego owed a duty to Plaintiffs and Class Members to exercise reasonable care, diligence, and prudence in protecting their Private

Information.

370. Oswego breached its duty under the constructive bailment by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class Members' Private Information, resulting in the unlawful and unauthorized access to, disclosure, and misuse of such Information to third parties such as Google.

371. Oswego further breached its duty to safeguard Plaintiffs' and Class Members' Private Information by failing to notify them individually in a timely and accurate manner that their Private Information had been disclosed to third parties without Plaintiffs' and Class Members' knowledge, consent, or explicit authorization.

372. As a direct and proximate result of Oswego's breach of its constructive bailment, Plaintiffs and Class Members have suffered compensable damages that were reasonably foreseeable to Oswego, including but not limited to, the damages set forth herein.

COUNT VIII
Implied Covenant of Good Faith & Fair Dealing

373. Plaintiffs and Class Members repeat and re-allege the allegations in paragraphs 1-287 as if fully set forth herein.

374. Plaintiffs and Class Members entered into valid, binding, and enforceable implied contracts with Oswego, as alleged above.

375. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts.

376. These included the implied covenants that Oswego would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiffs'

and Class Members' Private Information and to comply with industry standards and federal and state laws and regulations.

377. A "special relationship" exists between Oswego and Plaintiffs and Class Members. Oswego entered into a "special relationship" with Plaintiffs and Class Members who sought healthcare services through Oswego and, in doing so, entrusted Oswego, pursuant to its requirements, with their Private Information.

378. Despite this special relationship with Plaintiffs, Oswego did not act in good faith and with fair dealing to protect Plaintiffs' and Class Members' Private Information.

379. Plaintiffs and Class Members performed all conditions, covenants, obligations and promises owed to Oswego.

380. Oswego's failure to act in good faith denied Plaintiffs and Class Members the full benefit of their bargain and also caused Plaintiff and Class Members to suffer actual damages resulting from the disclosure and interception of their Private Information and they remain at imminent risk of suffering additional damages in the future.

381. Accordingly, Plaintiffs and Class Members have been injured as a result of Oswego's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IX
Violation of the New York Deceptive Trade Practices Act
New York Gen. Bus. Law § 349, *et seq.*

382. Plaintiffs and Class Members repeat and re-allege the allegations in paragraphs 1-287 as if fully set forth herein.

383. By the acts and conduct alleged herein, Oswego committed unfair or deceptive acts and practices by:

- a. promising to maintain the privacy and security of Plaintiffs' and Class Members' PHI as required by law;
- b. installing the tracking technologies DoubleClick and Google Ads to operate as intended and transmit Plaintiffs' and Class Members' Private Information without their authorization to Google;
- c. failing to disclose or omitting material facts to Plaintiffs and Class Members regarding the disclosure of their Private Information to Google;
- d. failing to take proper action to ensure the tracking technologies were configured to prevent unlawful disclosure of Plaintiffs' and Class Members' Private Information; and
- e. unlawfully disclosing Plaintiffs' and Class Members' Private Information to Google.

384. These unfair acts and practices violated duties imposed by laws, including but not limited to, the Federal Trade Commission Act, HIPAA and NY GBL § 349.

385. Oswego's actions also constitute deceptive and unfair acts or practices because Oswego knew it failed to disclose to Plaintiffs and Class Members that their healthcare-related communications via the Web Properties would be disclosed to Google.

386. Oswego's actions also constitute deceptive and unfair acts or practices because Oswego intended that Plaintiffs and Class Members rely on its deceptive and unfair acts and practices, and the concealment and omission of material facts in connection with Oswego's offering of goods and services.

387. Specifically, Oswego was aware that Plaintiffs and Class Members depended and relied upon it to keep confidential their communications and Private Information, and Oswego instead disclosed that information to Google.

388. In addition, Oswego's material failure to disclose that Oswego collects Plaintiffs' and Class Members' Private Information for marketing purposes with Google, for Oswego's own benefit, constitutes an unfair act or practice prohibited by the NY GBL § 349. Oswego's actions

were immoral, unethical and unscrupulous.

389. Plaintiffs had reasonable expectations of privacy in their communications exchanged with Oswego, including communications exchanged on Oswego's Web Properties.

390. Plaintiffs' reasonable expectations of privacy in the communications exchanged with Oswego were further buttressed by Oswego's express promises in its Privacy Policy and HIPAA Privacy Notice.

391. Contrary to its duties as a medical provider and its express promises of confidentiality, Oswego deployed the tracking technologies, including DoubleClick and Google Ads, to disclose and transmit Plaintiffs' personally identifiable, non-public medical information and the contents of their communications exchanged with Oswego to third parties, *i.e.*, Google.

392. Oswego's disclosures of Plaintiffs' and Class Members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

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

394. Oswego willfully, knowingly, intentionally and voluntarily engaged in the aforementioned acts when it incorporated the tracking technologies with knowledge of their purpose and functionality.

395. The harm described herein could not have been avoided by Plaintiffs and Class Members through the exercise of ordinary diligence.

396. As a result of Oswego's wrongful conduct, Plaintiffs were injured in that they never would have provided their PII and PHI to Oswego, or purchased Oswego's services, had they known or been told that Oswego would share their confidential and sensitive Private Information with Google or any other third party.

397. As a direct and proximate result of Oswego's multiple, separate violations of NY GBL § 349, Plaintiffs and Class member have suffered harm, including financial losses related to the payments or services made to Oswego that Plaintiffs and Class Members would not have made had they known of Oswego's disclosure of their PII and PHI to Google; lost control over the value of their PII and PHI; and other harm resulting from the unauthorized use or threat of unauthorized use of their PII and PHI, including for unwanted solicitations or marketing, entitling them to damages in an amount to be proven at trial.

398. Oswego's acts, practices and omissions were done in the course of Oswego's business of furnishing healthcare-related services to consumers in the State of New York.

399. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed decisions and to protect Plaintiffs, Class Members, and the public from Oswego's unfair, deceptive and unlawful practices. Oswego's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

400. As a result, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Eva Perry, Jacqueline Fletcher, and Debra L. Gilmore respectfully pray for judgment in their favor and against Defendant Oswego as follows:

- A. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and Plaintiffs' counsel as Class Counsel;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class

Members;

- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to patient data collection, storage, and safety, and to disclose with specificity the type of PII and PHI disclosed to third parties;
- D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- F. For an award of punitive damages, as allowable by law;
- G. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- H. Pre- and post-judgment interest on any amounts awarded; and
- I. Such other and further relief as this Honorable Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs Eva Perry, Jacqueline Fletcher, and Debra L. Gilmore hereby demand that this matter be tried before a jury.

Date: June 25, 2026

Respectfully submitted,



Stephen DeNittis, Esq.
DENITTIS OSEFCHEN PRINCE, P.C.
315 Madison Ave., 3rd Floor
New York, New York 10017
Telephone: (646) 979-3642
Facsimile: (856) 797-9978
Email: sdenittis@denittislaw.com

Attorneys for Plaintiffs & Putative Classes