Exhibit A3

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

RONDAL COOPER, CORAL FRASER and GILBERT MANDA, *on behalf of themselves and all others similarly situated*, Plaintiffs, v. MOUNT SINAI HEALTH SYSTEM, INC., Defendant.	Case No. 1:23-cv-09485 **JURY TRIAL DEMANDED**

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiffs Rondal Cooper, Coral Fraser and Gilbert Manda, through their attorneys, bring this class action lawsuit in their individual capacities and on behalf of all others similarly situated against Mount Sinai Health System, Inc. ("Mount Sinai" 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. Mount Sinai owns and operates eight hospitals and over a dozen medical centers in the New York City area.[1] Mount Sinai's health care system is made up of more than 43,000 employees, including 7,400 primary and specialty care physicians providing medical services

[1] These hospitals are: Mount Sinai Beth Israel, Mount Sinai Brooklyn, The Mount Sinai Hospital, Mount Sinai Queens, Mount Sinai Morningside, Mount Sinai West (formerly Mount Sinai Roosevelt), New York Eye and Ear Infirmary of Mount Sinai and Mount Sinai South Nassau. *See* https://www.mountsinai.org/about (last visited Jan. 9, 2024).

ranging from primary and urgent care to cancer treatment, cardiology, geriatrics, orthopedics and orthopedic surgery and neurology.[2]

2. Mount Sinai generates approximately $11.3 billion dollars in annual revenue.

3. As part of the medical services it provides, Mount Sinai owns, controls and maintains a website, https://www.mountsinai.org/ (the "Website"). Mount Sinai also controls and maintains a web-based patient portal (the "Portal").[3] The Website and the Portal are referred to herein as the "Web Properties."

4. Mount Sinai actively encourages its patients to use their Web Properties to communicate with their healthcare providers, access lab and test results, manage prescriptions and request refills, manage medical appointments, search medical conditions and treatment options, sign up for events and classes and much more. The Website is set up to mimic the in-person visit and invites patients to share and search for personal medical information about their own physical and mental health. And patients, trusting that this information will be safeguarded, share their most intimate and personal medical information with Mount Sinai through the Web Properties.

5. Information concerning a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of such information can have serious consequences including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.[4]

---

[2] *See* https://www.mountsinai.org/about/facts (last visited Jan. 9, 2024).

[3] *See* https://mychart.msmc.com/MyChart/Authentication/Login? (last visited Jan. 9, 2024). The MyChart patient portal is a software system designed and licensed to healthcare entities such as Mount Sinai by Epic Software Systems. Epic is a privately owned healthcare software company that provides services to 250 million patients, including two-thirds of the U.S. population.

[4] *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*

6. Plaintiffs and Class Members who visited and used Mount Sinai's Web Properties (collectively, the "Users") understandably thought that they were communicating only with their trusted healthcare providers. At no point has Mount Sinai, despite intentionally incorporating the Pixel into its Website and servers, informed its Users that their personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "PII/PHI" or "Private Information") communicated via its Web Properties was intentionally disclosed to a third party—let alone Facebook, which has a sordid history of privacy violations.[5]

7. In recent months, and in stark contrast, to Mount Sinai, several medical providers that used the Facebook Pixel in a similar way have provided their patients with notices of data breaches caused by the Pixel transmitting their information to third parties.[6]

8. Simply put (and as detailed herein), covered entities such as Mount Sinai are ***not*** permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private

---

endangering users in a post-Roe world, WIRED (Nov. 16, 2022), https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited Jan. 9, 2024) ("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.").

[5] This Court will not have to look far to find evidence of Meta's violations of privacy laws. Just in May of last year, for instance, the European Union fined Meta "a record-breaking" $1.3 billion for violating EU privacy laws. *See* Hanna Ziady, *Meta slapped with record $1.3 billion EU fine over data privacy*, https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html (last visited Jan. 9, 2024).

[6] *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, available at https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Jan. 9, 2024); *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022), available at https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3 (last visited Jan. 9, 2024); *Novant Health notifies patients of potential data privacy incident* (Aug. 12, 2022), available at https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx (last visited Jan. 9, 2024).

Information to any third party without express and informed consent from each patient. Neither Plaintiffs nor any other Class Members were provided—much less signed—a written authorization permitting Mount Sinai to disclose their Private Information to Facebook or any other third-party data brokers.

9. 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 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.***[7]

10. Similarly, OCR is clear that "[r]egulated 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."[8]

11. However, unbeknownst to Plaintiffs and Class Members, Mount Sinai did exactly that as it installed tracking technologies on its Web Properties to collect and disclose to unauthorized third parties their Private Information for its own pecuniary gain. Specifically, Mount Sinai embedded an undetectable tracking pixel on its Web Properties (the "Pixel" or "Facebook

---

[7] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases,* the FTC Business Blog (July 25, 2023) (emphasis added), *available at* https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Jan. 9, 2024).

[8] OCR Bulletin, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (emphasis added) (last visited Jan. 9, 2024).

Pixel") which transmits to Meta Platforms, Inc., d/b/a Meta ("Facebook") an incredible amount of personal and protected data about its Users. The collection and transmission of this information is instantaneous, invisible and occurs without any notice to—and certainly no consent from—the Users.[9]

12. Together with the patients' Private Information, the data sent to Facebook also discloses Users' unique and persistent Facebook ID ("Facebook ID" or "FID") which allows Facebook and other third parties to personally identify those Users and associates their Private Information with their Facebook profile.[10]

13. There is no anonymity in the information disclosed to Facebook for marketing and analytics purposes; that is, the Pixel collects and discloses a substantial "data packet" coupled with the FID so that Mount Sinai can, among other things, send targeted advertisements to Users based on their sensitive and protected Private Information. Mount Sinai also uses this impermissibly obtained data for analytics purposes to gain additional insights into how its patients use its Web Properties.[11]

---

[9] Hospitals that use analytics tools like the Facebook Pixel or Google Analytics on their websites may also have those tools embedded on the MyChart login page or even inside the MyChart patient portal.

[10] The Facebook ID is a string of numbers Facebook uses to identify and connect to a User's Facebook profile. Facebook creates a Facebook ID automatically, whether or not you choose to create a username. *See* https://www.facebook.com/help/211813265517027 (last accessed January 10, 2024). Thus Facebook, which creates and maintains the Facebook ID directly connected to a User's Facebook account, utilizes the Facebook ID to personally identify each User whose Private Information is disclosed to it.

[11] While gaining additional insights into its User base is not a bad thing necessarily, Mount Sinai 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. The OCR Bulletin is, again, instructive: "disclosures of PHI to tracking technology vendors for marketing purposes, ***without individuals' HIPAA-compliant authorizations,*** would constitute impermissible disclosures." *See*

14. Operating as designed and as implemented by Mount Sinai, the Pixel disclosed information that allows a third party (*e.g.*, Facebook) to know when and where a specific patient was seeking confidential medical care, for what medical condition, and the precise care they sought or received. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who geo-target Plaintiffs' and Class Members' Meta accounts based on that Private Information.

15. The Facebook Pixel, installed and configured by Mount Sinai, is a piece of code that "tracks the people and [the] type of actions they take"[12] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box).

16. Invisible to the naked eye, pixels—which are configured by the website owner, here, Mount Sinai—collect and transmit information from Users' browsers to unauthorized third parties including, but not limited to, Facebook and Google, Inc. (collectively, "Pixel Information Recipients").[13]

17. Incredibly, even after the filing of this class action alleging the improper use of tracking technologies in violation of federal, state and common law, Mount Sinai not only continues to use Google Analytics (as alleged in Plaintiffs' complaint), but—somewhat unbelievably—***still embeds at least forty-five other tracking codes on its Website***,

---

OCR Bulletin, *supra* note 8.

[12] *Retargeting*, https://www.facebook.com/business/goals/retargeting (last visited Jan. 11, 2023).

[13] The Pixel itself is a small snippet of code placed on webpages by the website owner. The process of adding the Pixel to a webpage is a multi-step process that, as described in detail in *section E*, must be undertaken by the website owner, namely, Mount Sinai.

including Adobe Audience Manager, Akamai mPulse, Dun & Bradstreet, Google Tag Manager, LinkedIn, New Relic, SolarWinds Pingdom, Oracle BlueKai, Piwik, Salesforce Marketing Cloud (iGoDigital), Salesforce Marketing Personalization (Evergage), ShareThis, The Trade Desk, TVSquared, AdTheorent, DoubleClick ads, Microsoft Universal Events, medtargetsystem.com, eyeota, Yahoo, Deep Intent, Adnxs/AppNexus, Casale Media, trc.lhmos.com, Fifty, Inmar Intelligence (OwnerIQ), AtData (TowerData), LiveIntent, ROQAD, LiveRamp - Arbor.io (Pippio), P.rfihub.com Malware, Zync by Zeta Global, Lijit.com, id5-sync.com, Neustar, OnAudience, creative-serving.com, Lotame, Amobee, Zeotap, GroupM, MediaMath, Improve Digital (360 Polaris), Affectv, and Full Circle Studies (ScorecardResearch.com).

18. And, at least the following trackers on Mount Sinai's Website are disclosing the Users' search queries: DoubleClick ads, Google Analytics, Microsoft Universal Events, Share This, Salesforce Marketing Cloud (iGoDigital), and TVSquared.

19. Upon information and good faith belief, Mount Sinai also installed and implemented Facebook's Conversions Application Programming Interface ("Conversions API" or "CAPI") on its Web Properties servers. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to disclose information to third parties in addition to the website owner, CAPI does not cause the User's browser to transmit information directly to Facebook. Rather, CAPI tracks the User's website interactions, including Private Information, records and stores that information on the website owner's servers and then transmits the data to Facebook from the website owner's servers.[14]

[14] *See* https://revealbot.com/blog/facebook-conversions-api/ (last visited Jan. 9, 2024). Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising

20. Unlike the pixels, CAPI functions from Mount Sinai's servers, so it cannot be stymied by the use of anti-pixel software or other workarounds such as ad blockers.

21. While the information captured and disclosed without permission may vary depending on the pixel(s) embedded, these "data packets" can be extensive, sending, for example, the User's first name, last name, email address, phone number, zip code and city of residence entered on the Web Properties. The data packets also include the buttons a User clicks and the words the User types into a search bar.

22. For instance, when a User uses Mount Sinai's Web Properties where tracking technologies, such as the Facebook Pixel are present, the Pixel transmits the contents of their communications to Facebook including, but not limited to: (i) accessing the patient portal; (ii) the exact text of the User's search queries; (iii) medical services and treatments sought; (iv) scheduling of appointments; (v) accessing and viewing the bill page; (vi) the text of URLs visited by the User and (vii) other information that qualifies as PII and PHI under federal and state laws. The data in the "data packets" is then linked to a specific internet protocol ("IP") address, which is itself protected information under the Health Insurance Portability and Accountability Act ("HIPAA").

23. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered PII. This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual.

---

impacts both online and offline results." *See* https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Jan. 9, 2024).

24. These HIPAA Identifiers, as relevant here, include names, dates related to an individual, email addresses, device identifiers, web URLs and IP addresses.[15]

25. By installing the Facebook Pixel, CAPI and other tracking technologies, Mount Sinai effectively planted a bug on Plaintiffs' and Class Members' web browsers and caused them to unknowingly disclose their private, sensitive and confidential health-related communications to Facebook.[16]

26. The information intercepted by the Pixels and third-party tracking technologies is used to build incredibly fulsome and robust marketing profiles for individual Users and create targeted advertisements based on the medical conditions and other Private Information disclosed. Despite the clear and unequivocal prohibition on the disclosure of PHI without consent, Mount Sinai chose to use the Pixel and CAPI data for marketing purposes to bolster its revenue.

27. Simply put, Mount Sinai put its desire for profit over its patients' privacy rights.

28. As a healthcare provider, Mount Sinai had certain duties and obligations to its patients. Mount Sinai breached those duties and obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure the Web Properties was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web Users' information; (iii) failing to obtain the consent of Plaintiffs and

[15] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Jan. 11, 2024).

[16] While this Amended Complaint primarily focuses on how Mount Sinai embedded the Meta Pixel on its Web Properties to collect and disclose Users' Private Information, other secret tracking technologies embedded by Mount Sinai—such as Google Analytics, LinkedIn Ads, New Relic and Oracle BlueKai tracking codes—also collect such Private Information, and the respective tech companies have the capability to link it to specific user profiles they have built.

Class Members to disclose their PII and PHI to Facebook or other third parties; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' PII and PHI through the Pixels; (v) failing to warn Plaintiffs and Class Members; and (vi) otherwise failing to design and monitor its Web Properties to maintain the confidentiality and integrity of patient PII and PHI.

29. Plaintiffs and Class Members have suffered injury because of Defendant's conduct; these injuries include: (i) invasion of privacy, (ii) loss of benefit of the bargain, (iii) compromise and disclosure of Private Information, (iv) diminution of value of their Private Information, (iv) statutory damages and (v) the continued and ongoing risk to their Private Information.[17]

30. Plaintiffs seek to remedy these harms for themselves and a class of all others similarly situated and therefore assert causes of action for (i) Violations of the Electronic Communications Privacy Act (18 U.S.C. § 2510, *et seq.*); (ii) Negligence; (iii) Invasion of Privacy; (iv) Breach of Implied Contract; (v) Breach of Fiduciary Duty; (vi) Unjust Enrichment; (vii) Breach of Confidence; (viii) Constructive Bailment; (ix) Implied Covenant of Good Faith and Fair Dealing and (x) Violation of New York's Deceptive Trade Practices Act (New York Gen. Bus. Law § 349).

PARTIES

31. Plaintiff Rondal Cooper is a natural person residing in Queens County in the State of New York, where he intends to remain.

32. Plaintiff Coral Fraser is a natural person residing in New York County in the State of New York, where she intends to remain.

[17] 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.

33. Plaintiff Gilbert Manda is a natural person residing in New York County in the State of New York, where he intends to remain.

34. As detailed herein, Plaintiffs accessed Mount Sinai's Web Properties on their computers and mobile devices and used the Web Properties to look for providers, review conditions and treatments, make appointments and communicate with their providers. Plaintiffs have used and continue to use the same devices to maintain and access active Facebook accounts throughout the relevant period in this case.

35. Defendant Mount Sinai is a registered non-profit entity with its headquarters, principal place of business and main campus at One Gustave L. Levy Place in New York, New York 10029.

36. Defendant Mount Sinai is one of the oldest and largest teaching hospitals in the United States, with eight hospital campuses and thirteen free-standing joint venture centers.[18]

37. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

JURISDICTION & VENUE

38. 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.

[18] *See* https://www.mountsinai.org/about/facts (last visited Jan. 9, 2024).

39. 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.

40. Venue is proper in this judicial district under 28 U.S.C § 1391 (a) through (d) because: (i) a substantial part of the events giving rise to this action occurred in this judicial district, including decisions made by Mount Sinai's governance and management personnel or inaction by those individuals that led to the unauthorized sharing of Plaintiffs' and Class members' Private Information; (ii) Mount Sinai's principal place of business is located in this judicial district; (iii) Mount Sinai collects and redistributes Class members' Private Information in this judicial district and (iv) Mount Sinai 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 Informed Consent is Illegal.

41. This 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—in recent months—reiterated the importance of and necessity for data security and privacy concerning health information.

42. For instance, the FTC recently published a bulletin entitled *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, in which it noted that "[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is 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."[19]

43. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without 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] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that ***may run afoul of 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***.[20]

44. The federal government is taking these violations of health data privacy and security seriously as recent high-profile FTC settlements against several telehealth companies evidence.

---

[19] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases,* the FTC Business Blog (July 25, 2023) (emphasis added), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Jan. 9, 2024).

[20] *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.

45. For example, earlier this year, 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. related to information about fertility and pregnancy that 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 Premon shared health data for advertising purposes.[21]

46. Even more recently, 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

[21] *See* How FTC Enforcement Actions Will Impact Telehealth Data Privacy, https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy (last visited Jan. 9, 2024); *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-in1st-action-under-health-breach-rule?copied=1 ("The Federal Trade Commission signaled it won't hesitate to wield its full range of enforcement powers when it dinged GoodRx for allegedly sharing sensitive health data with advertisers, teeing up a big year for the agency and boosting efforts to regulate data privacy on a larger scale."); https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising; 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 Jan. 9, 2024); https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google (last visited Jan. 9, 2024).

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."[22]

47. The Office for Civil Rights at HHS has made clear, in a recent bulletin titled *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.***[23]

48. The OCR Bulletin *reminds* healthcare organizations regulated under the 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. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[24]

49. The OCR Bulletin 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***

[22] *See* OCR Bulletin, *supra* note 8.

[23] *Id*.

[24] *See id*.

> ***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.***[25]

50. 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.

51. For instance, THE MARKUP reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment.[26]

52. 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 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.[27]

---

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

[26] *See* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Jan. 9, 2024).

[27] 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), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies (last

53. 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.[28]

B. The Tracking Pixels.

54. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting, for example, serving online advertisements to people who have previously engaged with a business's website—and other marketing.

55. Here, a User's web browser executes the Pixels via instructions within each webpage of Mount Sinai's Website (and, upon information and good faith belief, within Mount Sinai's MyChart) to communicate certain information (within parameters set by Mount Sinai) directly to the corresponding Pixel Information Recipients—at the same time as the User's browser is sending this information to Mount Sinai.

56. The Pixels can also share the Users' identifying information for easy tracking via "cookies"[29] stored on their computer by any of the Pixel Information Recipients with whom they have an account. For example, Facebook stores or updates a Facebook-specific cookie every time a person accesses their Facebook account from the same web browser.

57. The Meta Pixel can access this cookie and send certain identifying information like the User's Facebook ID to Facebook along with the other data relating to the User's Website

---

visited Jan. 9, 2024).

[28] *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").

[29] "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 Jan. 9, 2024).

inputs. The same is true for the other Pixel Information Recipients, which also create cookies that are stored in the User's computer and accessed by the Pixels to identify the User.

58. The Pixels are programmable, meaning that Mount Sinai controls which of the webpages on the Website contain the Pixels and which events are tracked and transmitted to the Pixel Information Recipients.

59. Mount Sinai has utilized Facebook Pixels (and, upon information and good faith belief, other tracking technologies) since at least August 2017.

60. Mount Sinai used the data it collected from Plaintiffs and Class Members, without their consent, to improve its advertising and bolster its revenues.

C. Conversions API.

61. Facebook Conversions API and similar tracking technologies allow businesses to send web events, such as clicks, form submissions, keystroke events and other user actions performed by the user on the Website, from their own servers to Facebook and other third parties.[30]

62. Conversions API creates a direct and reliable connection between marketing data (such as website events and offline conversations) from Mount Sinai's server to Facebook.[31] In doing so, Mount Sinai stores Plaintiffs' and Class Members' Private Information on its own server and then transmits it to unauthorized third parties, *i.e.*, Facebook.

63. Conversions API is an alternative method of tracking versus the Meta Pixel because no privacy protections on the user's end can defeat it. This is because it is "server-side"

[30] *See* https://revealbot.com/blog/facebook-conversions-api/ (last visited Jan. 9, 2024).

[31] *See* https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Jan. 9, 2024).

implementation of tracking technology, whereas the Pixels are "client-side"—executed on users' computers in their web browsers.

64. Because Conversions API is server-side, it cannot access the Facebook c_user cookie to retrieve the Facebook ID.[32] Therefore, other roundabout methods of linking the user to their Facebook account are employed.[33] For example, Facebook has an entire page within its developers' website about how to de-duplicate data received when both the Facebook Pixel and Conversions API are executed.[34]

65. Conversions API tracks the user's website interactions, including Private Information being shared, and then transmits this data to Facebook and other third parties. Facebook markets Conversions API as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[35]

66. Mount Sinai installed the Meta Pixels and, upon information and good faith belief, Conversions API, as well as other tracking technologies, on many (if not all) of the webpages

---

[32] "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses and phone numbers, that we use for matching purposes only." *See* https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/ (last visited Jan. 9, 2024).

[33] "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req- rec-params (last visited Jan. 9, 2024).

[34] *See* https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events (last visited Jan. 9, 2024).

[35] *About Conversions API*, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Jan. 9, 2024).

within its Web Properties (including the member-only patient portal) and programmed or permitted those webpages to surreptitiously share patients' private and protected communications with the Pixel Information Recipients—communications that included Plaintiffs' and Class Members' Private Information.

D. Mount Sinai's Method of Transmitting Plaintiffs' & Class Members' Private Information via Pixels & Conversions API.

67. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (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).

68. 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.

69. 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 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), GET Requests can also send data to the host server embedded inside the URL and can include cookies. POST 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. **Cookies**: a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Cookies are sent with HTTP requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely

different website.

c. **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.

70. A patient's HTTP request essentially asks Mount Sinai's Website to retrieve certain information (such as a set of health screening questions). The HTTP response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons and other features that appear on the participants' screens as they navigate Mount Sinai's Website.

71. Every website is comprised of Markup and "Source Code." Source Code is a simple set of instructions that commands the website user's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

72. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP requests quietly executed in the background without notifying the web browser's user.

73. The Pixels are Source Code that do just that—they surreptitiously transmit a Website User's communications and inputs to the corresponding Pixel Information Recipient, much like a traditional wiretap. When individuals visit Mount Sinai's Website via an HTTP request to Mount Sinai's server, Mount Sinai's server sends an HTTP response (including the Markup) that displays the webpage visible to the User, along with Source Code (including the Pixels).

74. Thus, Mount Sinai 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 waiting for private communications on the webpage to trigger the Pixels, which then intercept those communications—intended only for Mount Sinai—and transmit those communications to the corresponding Pixel Information Recipient.

75. Third parties like the Pixel Information Recipients place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third party can identify the specific user associated with the information intercepted (in this case, highly sensitive Private Information).

76. Mount Sinai intentionally configured Pixels installed on its Website to capture both the "characteristics" of individual patients' communications with Mount Sinai's Website (their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (the buttons, links, pages and tabs they click and view related to their health conditions and services sought from Defendant).

77. Epic's MyChart software system was also designed to permit licensees—such as Mount Sinai—to deploy "custom analytics scripts" within the Portal. For example, this would allow the website owner to deploy the Facebook Pixel or Google Analytics to capture the transmission of Private Information, including medical and health-related information and communications to third parties.[36]

78. Upon information and belief, Defendant intercepted and disclosed the following non-public private information to Facebook:

a. Plaintiffs' and Class Members' status as medical patients;

b. Plaintiffs' and Class Members' communications with Defendant through its Web Properties, including specific text queries typed into the search bar, medical conditions for which they sought treatments and treatments sought;

c. Plaintiffs' and Class Members' searches for appointments, appointment details, location of treatments, medical providers'

[36] *See* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Jan. 9, 2024).

names and their specialties, medical conditions and treatments;

d. PII, including but not limited to patients' locations, IP addresses, device identifiers and an individual's unique Facebook ID.

79. Mount Sinai also deposits cookies named _fbp, _ga_ and _gid onto Plaintiffs' and Class Members' computing devices. These are cookies associated with the third-parties Facebook and Google but which Mount Sinai deposits on Plaintiffs' and Class Members' computing devices by disguising them as first-party cookies. And without any action or authorization, Mount Sinai commands Plaintiffs' and Class Members' computing devices to contemporaneously re-direct the Plaintiffs' and Class Members' identifiers and the content of their communications to Facebook and Google.

80. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Mount Sinai's use of the Meta Pixel.[37] The fbp cookie emanates from Mount Sinai's Website as a putative first-party cookie, but is transmitted to Facebook through cookie-synching technology that hacks around the same-origin policy.

81. A user who accesses Defendant's Web Properties while logged (or having recently logged) into Facebook will transmit the c_user cookie to Facebook, which contains that user's unencrypted FID.

82. When accessing Mount Sinai's Website, for example, Facebook receives at least seven cookies[38]:

[37] The letters fbp are an acronym for Facebook Pixel.

[38] Not pictured here is the _fbp cookie, which is transmitted as a first-party cookie.

Name	Value	Domain	P...	Expires / Max-Age	S...
presence	C%7B%22t3%...	.facebook.com	/	Session	75
sb	GrxtY1jj9lKWn...	.facebook.com	/	2024-04-06T23:4...	26
datr	QtI1Y1lVd2UW...	.facebook.com	/	2024-04-05T23:1...	28
xs	7%3A_7bqKp6...	.facebook.com	/	2024-10-23T20:4...	99
wd	1664x993	.facebook.com	/	2023-10-31T20:4...	10
fr	1BhquGXZpTh...	.facebook.com	/	2024-01-22T20:4...	84
c_user	54(	.facebook.com	/	2024-10-23T20:4...	15

83. The fr cookie contains, at least, an encrypted FID and browser identifier.[39] Facebook, at a minimum, uses the fr cookie to identify users.[40]

84. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies.

85. The Facebook Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—i.e., Defendant.[41] A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook.[42]

86. At each stage, Defendant also utilized the _fbp cookie, which attaches to a browser as a first-party cookie, and Facebook uses to identify a browser and a user:[43]

Name	Value	Domain	P...	Expires / Max-Age
_fbp	fb.1.1696430267150.1195488401	.mountsinai.org	/	2024-01-24T15:15...

[39] Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* (Sept. 21, 2012), at 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited Jan. 9, 2024).

[40] COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/ (last visited Jan. 9, 2024).

[41] *First-Party Cookie*, https://www.pcmag.com/encyclopedia/term/first-party-cookie (last visited Jan. 9, 2024). This is confirmable by using developer tools to inspect a website's cookies and track network activity.

[42] *Third-Party Cookie*, https://www.pcmag.com/encyclopedia/term/third-party-cookie (last visited Jan. 9, 2024). This is also confirmable by tracking network activity.

[43] *Id*.

87. The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.[44] If that happens, the time resets, and another 90 days begins to accrue.

88. The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website.[45] If that happens, the time resets and another 90 days begins to accrue.

89. The __ga and _gid cookies operate similarly as to Google.

90. Furthermore, if the patient is also a Facebook user, the information Facebook receives is linked to the patient's Facebook profile (via their Facebook ID or "c_user id" cookie), which includes other identifying information.[46]

91. For example, when patients visit https://www.mountsinai.org/ to search for a doctor, they may select the "Find a Doctor" tab, which takes them to the "Find a Doctor" page.

92. Upon information and good faith belief, Defendant's webpages for its various hospitals operate in the same way as Defendant's general Website, and share their patients' identities and online activity including information and search results related to their private medical conditions and treatment.

---

[44] *Id*.

[45] COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/ (last visited Jan. 9, 2024).

[46] Facebook uses several cookies to identify users, including cookies named c_user, datr, fr, and _fbp. The c_user cookie identifies Facebook users. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one—and only one—unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications. The Facebook datr cookie identifies the web browser the patient is using. It is an identifier unique to each patient's specific web browser and is another way Meta can identify Facebook users (Facebook keeps a record of every datr cookie identifier associated with each of its users). The Facebook fr cookie is an encrypted combination of the c_user and datr cookies.

93. If a patient selects filters or enters keywords into the search bar on the "Find a Doctor" webpage, the filters and search terms, including the doctor's specialty, are transmitted via the Facebook Pixel.

94. Similarly, if a patient uses the Website's general search bar, the terms and phrases the patient types are transmitted to Facebook, even if they contain a patient's treatment, procedures, medical conditions or related queries. This information is automatically sent from the patient's device to Facebook, revealing the patient's FID (c_user field) along with each search filter the patient selected.

95. After taking any of these actions on the "Find a Doctor" page, patients are subsequently directed to the page with "search results," and their selections or search parameters are automatically transmitted to Facebook. The information transmitted to Facebook includes: (i) the patient's unique and persistent FID (c_user ID), (ii) the fact that the patient clicked on a specific provider's profile page, (iii) the patient's search parameters (demonstrating they specifically searched for a doctor's specialty) and (iv) the patient's location.

96. Defendant installed at least two Facebook Pixels on its Web Properties, including a Pixel with ID number "940133619402530" which identified and categorized which actions the User took on the webpage at issue (including "PageView" which identifies the User as having viewed the particular webpage, "Microdata" which contains page metadata, and "SubscribedButtonClick," which tracks each click on the webpage and shares the metadata of buttons clicked by the User, such the "inner text" of the button, with Facebook). Defendant also installed a Pixel with ID number "194331831908198" which also collected "PageView" events.

97. Defendant's Website also includes a feature that allows patients to book appointments through a particular doctor's profile page. If a patient clicks on the "Request

Appointment" button, this action is communicated and shared with Facebook, including, upon information and good faith belief, provider's name and/or specialty.

98. If a patient finishes the process for making an appointment, this action is also communicated and shared with Facebook.

99. Similarly, each doctor's profile page includes a direct link that allows a patient to call the doctor's office, and upon clicking the telephone number button, the patient's click is shared with Facebook.

100. Each time Defendant sends this activity data, it discloses a patient's PII and PHI.

101. Finally, Defendant also notifies Facebook of its patients' patient status. For example, when a user accesses Defendant's page to utilize Defendant's patient portal, Defendant notifies Facebook of that as well.

102. Mount Sinai's Website also provides a link to MyMountSinai (MyChart) on each page of its Website. When a patient clicks on this link, that information (*i.e.*, that the patient is accessing MyChart, and thus, presumptively, a patient of Mount Sinai), is sent to Facebook.

103. Defendant has re-configured the Pixels on many of its webpages. As a result, Plaintiffs are unable to determine whether the Pixels were embedded inside the MyChart portal. However, given Defendant's use of the Pixels on other pages of the Website (including the "book appointment" page, which tells Facebook that a patient booked an appointment with a specific doctor, and the log-in page for the MyChart portal), Plaintiffs reasonably believe and, therefore, aver that Defendant used the Pixels to track information on its entire digital platform, including inside its MyChart portal.

104. Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link to FIDs and corresponding Facebook profiles.

105. As described *infra*, Defendant sent these identifiers with the event data.

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

107. By law, Plaintiffs are entitled to privacy in their PHI and confidential communications. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (i) implemented a system that surreptitiously tracked, recorded and disclosed Plaintiffs' and Class Members' confidential communications, PII and PHI to a third party; (ii) disclosed patients' protected information to Facebook—an unauthorized third-party eavesdropper; and (iii) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent. Plaintiffs did not discover that Defendant disclosed their PII and PHI to Facebook, and assisted Facebook with intercepting their communications, until at least August 2023 for Plaintiffs Cooper, Fraser and Manda.

E. Facebook's Platform & its Business Tools.

108. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021.[47] Roughly 97% of that came from selling advertising space.[48]

[47] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Jan. 9, 2024).

[48] *Id.*

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

110. Facebook's Business Tools, including the Meta Pixel, are bits of code that advertisers can integrate into their webpages, mobile applications and servers, thereby enabling the interception and collection of user activity on those platforms.

111. In particular, the Meta Pixel "tracks the people and type of actions they take."[49]

112. The User's web browser (software applications that allow consumers to exchange electronic communications over the Internet) executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner.

113. The Pixel is thus customizable and programmable, meaning that the website owner controls which of its web pages contain the Pixel and which events are tracked and transmitted to Facebook.

114. The process of adding the Pixel to webpages is a multi-step process that must be undertaken *by the website owner*.[50]

115. Facebook guides the website owner through setting up the Pixel during the setup process. Specifically, Facebook explains that there are two steps to set up a pixel:

> 1. Create your pixel and set up the pixel base code on your website. You can use a partner integration if one is available to you or you can manually add code to your website.

[49] *Retargeting*, *supra* note 12.

[50] *Business Help Center: How to set up and install a Meta Pixel*, https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited Jan. 9, 2024); *see* Ivan Mana, *How to Set Up & Install the Facebook Pixel (in 2022)*, https://www.youtube.com/watch?v=ynTNs5FAUm8 (last visited Jan. 9, 2024).

> 2. Set up events on your website to measure the actions you care about, like making a purchase. You can use a partner integration, the point-and-click event setup tool, or you can manually add code to your website.[51]

116. Aside from the various steps to embed and activate the Pixel, website owners, like Mount Sinai, must also agree to Facebook's Business Tools Terms by which Facebook requires website owners using the Meta Pixel to "represent and warrant" that they have adequately and prominently notified users about the collection, sharing and usage of data through Facebook's Business Tools (including the Pixel and Conversions API)[52] and that websites "will not share Business Tool Data . . . that [websites] know or reasonably should know . . . includes health, financial information or other categories of sensitive information . . . ."[53]

117. Once fully loaded and operational, the Pixel prompts the Users' web browser to transmit specific information based on parameters set by the website owner. This customizable nature of the Meta Pixel allows the website owner to determine which webpages contain the Pixel, which events are tracked and shared with Facebook and whether the tracked events are standard (chosen from the list of 18 provided by Facebook) or custom (defined by the website owner). For example, the Pixel can be set to capture the URLs visited by website visitors via a "PageView"

---

[51] *Id*.

[52] *Meta Business Tools Terms*, https://www.facebook.com/legal/businesstech?paipv=0&eav=AfbOvnb7E0sZ-wzgCW6xNLFKEOEVH_fr6JjkMINTJNqN7i1R-3MPh5caFgmdgAOxbL8&_rdr (last visited Jan. 9, 2024) ("When you use any of the Meta Business Tools to send us or otherwise enable the collection of Business Tool Data . . ., these Business Tools Terms govern the use of that data").

[53] *Id.*; *see also* Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report* (June 16, 2022) https://www.newsbytesapp.com/news/science/facebook-collects-personal-data-on-abortion-seekers/story (quoting Facebook spokesman Dale Hogan as saying that it is "against [Facebook's] policies for websites and apps to send sensitive health data about people through [its] Business Tools") (last visited Jan. 9, 2024).

event, or to capture the exact inner text of buttons clicked by a visitor, via a "SubscribedButtonClick" event.

118. The Business Tools are automatically configured to capture "Standard Events," such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[54]

119. Advertisers, such as Mount Sinai, can track other User actions and can create their own tracking parameters by building a "custom event."[55]

120. When a user accesses a webpage that is hosting the Meta Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers—traveling from the user's browser to Facebook's server.

121. This additional, simultaneous secret transmission contains the original GET request sent to the host website, along with additional data that the Meta Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Mount Sinai's Website—Mount Sinai's own code and Facebook's embedded code.

---

[54] *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Jan. 9, 2024); *see also* META PIXEL, GUIDES, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/ (last visited Jan. 9, 2024); BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited Jan. 9, 2024); APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 9, 2024).

[55] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (last visited Jan. 9, 2024).

122. Mount Sinai tracked users through "PageView," "Microdata," and "SubscribedButtonClick" events as well as custom events such as a "MyChart" event. These events disclosed at least the following:

- Users' search queries;
- When Users clicked to use the MyChart app;
- When Users clicked to access and viewed the bill page;
- When Users clicked to request an appointment; and
- What care and treatment options Users viewed.

123. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients' Facebook IDs, IP addresses and/or device IDs and the other information they input into Mount Sinai's Website, including not only their medical searches, treatment requests and the webpages they view, but, upon information and good faith belief, also their name, email address and/or phone number.

124. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[56] Plaintiffs' and Class Members identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

125. Instead of taking proactive steps to verify that businesses using the Pixel obtain the required consent, Meta uses an "honor system" under which Meta assumes these businesses have "provided robust and sufficient prominent notice to users regarding the Business Tool Data collection, sharing, and usage."[57]

[56] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Jan. 9, 2024).

[57] *See* Facebook Business Tools Terms, https://www.facebook.com/legal/terms/businesstools.

126. After intercepting and collecting this information, Facebook processes it, analyzes it and assimilates it into datasets like Core Audiences and Custom Audiences. When the website visitor is also a Facebook user, the information collected via the Meta Pixel is associated with the user's Facebook ID that identifies their name and Facebook profile—their real-world identity.

127. The pixel collects data regardless of whether the visitor has an account. Facebook maintains "shadow profiles" on users without Facebook accounts, and links the information collected via the Meta Pixel to the user's real-world identity using their shadow profile.[58]

128. A user's Facebook ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access and view the user's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

129. The Private Information disclosed via the Pixel allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought. Facebook then uses that information to sell advertising to Mount Sinai and other advertisers and/or sells that information to marketers who use it to online target Plaintiffs and Class Members.

130. With substantial work and technical know-how, internet users can sometimes circumvent the browser-based wiretap technology of the Pixels. This is why third parties bent on

[58] *See* Russell Brandom, *Shadow Profiles Are the Biggest Flaw In Facebook's Privacy Defense*, (Apr 11, 2018), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (last visited Jan. 9, 2024).

gathering Private Information, like Facebook, implement workarounds that even savvy users cannot evade. Facebook's workaround is Conversions API.

131. Conversions API is effective because it transmits directly from the host server and does not rely on the user's web browser.

132. Thus, the communications between patients and Mount Sinai, which are necessary to achieve the purpose of Mount Sinai's Website, are received by Mount Sinai and stored on their server before Conversions API collects and sends the Private Information contained in those communications directly from Mount Sinai to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.[59]

133. The Pixel Information Recipients track user data and communications for their own marketing purposes and for the marketing purposes of the website owner. Ultimately, the purpose of collecting user data is to make money.

134. Thus, without any knowledge, authorization or action by a user, website owners like Mount Sinai use source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

135. In this case, Mount Sinai employed the Pixels and Conversions API, among other tracking technologies, to intercept, duplicate and re-direct Plaintiffs' and Class Members' Private Information to Facebook and the other Pixel Information Recipients.

[59] Although prior to discovery there is no way to confirm that Mount Sinai has implemented Conversions API or another workaround (as that would require accessing the host server), Facebook instructs website owners like Mount Sinai to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Mount Sinai "to share website events [with Facebook] that the pixel may lose." *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Jan. 9, 2024). Thus, it is reasonable to infer that Mount Sinai is utilizing the Conversions API workaround.

136. In sum, the Pixels and other tracking technologies on the Website transmitted Plaintiffs' and Class Members' highly sensitive communications and Private Information to the corresponding Pixel Information Recipient, which communications contained private and confidential medical information.

137. These transmissions were performed without Plaintiffs' or Class Members' knowledge, consent or express written authorization.

F. Meta Encourages Healthcare Partners, Including Mount Sinai, to Upload Patient Lists for Ad Targeting.

138. Meta operates the world's largest social media company. Meta's revenue is derived almost entirely from selling targeted advertising. Meta's Health division is dedicated to marketing to and servicing Meta's healthcare partners. Meta defines its Partners to include businesses that use Meta's products, including the Meta Pixel or Meta Audience Network tools to advertise, market or support their products and services.

139. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

140. Meta offers an ad targeting option called "Custom Audiences."

141. When a patient takes an action on a Meta healthcare partner's website embedded with the Pixel, the Pixel will be triggered to send Meta "Event" data that Meta matches to its users.

142. A web developer can then create a "Custom Audience" based on Events to target ads to those patients.

143. The Pixel can then be used to measure the effectiveness of an advertising campaign.[60]

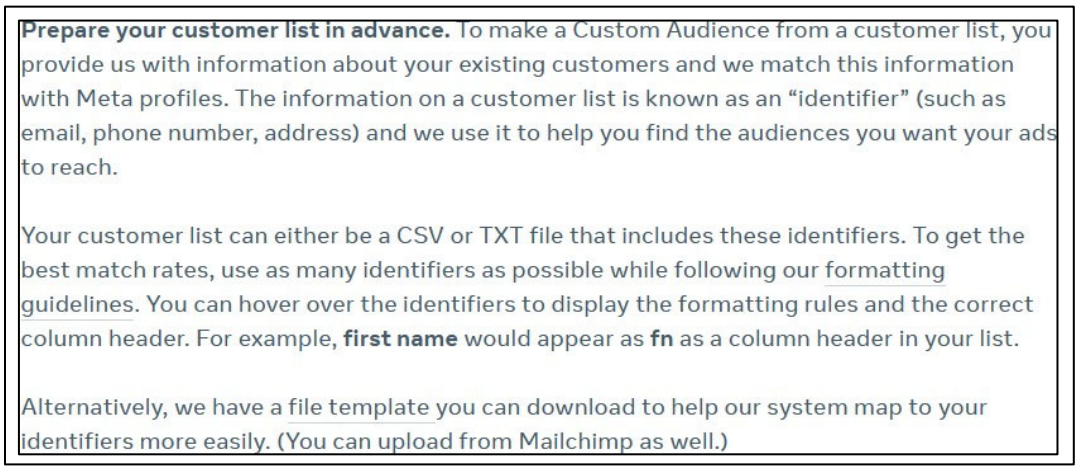
144. Meta also allows Meta healthcare partners to create a Custom Audience by uploading a patient list to Meta. As Meta describes it:[61]

> A Custom Audience made from a customer list is a type of audience you can create to connect with people who have already shown an interest in your business or product. It's made of information - called "identifiers" - you've collected about your customers (such as email, phone number and address) and provided to Meta. Prior to use, Meta hashes this information.
>
> Then, we use a process called matching to match the hashed information with Meta technologies profiles so that you can advertise to your customers on Facebook, Instagram and Meta Audience Network. The more information you can provide, the better the match rate (which means our ability to make the matches). Meta doesn't learn any new identifying information about your customers.

[60] Meta Business Help Center, *About Customer List Custom Audiences* (2023), https://www.facebook.com/business/help/341425252616329?id=2469097953376494; *see also,* Meta Blueprint, Connect your data with the Meta Pixel and Conversion API (2023), https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d_fnzRCUAhKGYsLqNA-VcLTMr3G_hxxFr3GZC_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9dff7fa.

[61] Meta Business Help Center, *About Customer List Custom Audiences* (2023), https://www.facebook.com/business/help/341425252616329?id=2469097953376494.

145. Meta provides detailed instructions for healthcare partners to send their patients' Private Information to Meta through the customer list upload. For example:[62]



Prepare your customer list in advance. To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Meta profiles. The information on a customer list is known as an "identifier" (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach.

Your customer list can either be a CSV or TXT file that includes these identifiers. To get the best match rates, use as many identifiers as possible while following our formatting guidelines. You can hover over the identifiers to display the formatting rules and the correct column header. For example, **first name** would appear as **fn** as a column header in your list.

Alternatively, we have a file template you can download to help our system map to your identifiers more easily. (You can upload from Mailchimp as well.)

146. Meta healthcare partners can then use the Custom Audiences derived from their patient list with the Pixel and Pixel Events for Meta marketing campaigns and to measure the success of those campaigns.

G. Mount Sinai's Use of the Pixels Violated Its Own Privacy Policies.

147. Defendant publishes several privacy policies that represent to patients and visitors to its Web Properties that it will keep 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***.

148. Defendant publishes Mount Sinai Privacy Policy, which tells patients: "MOUNT SINAI employs a variety of online security measures to safeguard and keep your information private."[63]

---

[62] Create a customer list custom audience, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited Jan. 9, 2024).

[63] https://www.mountsinai.org/privacy#:~:text=MOUNT%20SINAI%20reserves%20the%20right,ii)%20to%20release%20information%20in (last visited Jan. 9, 2024).

149. Defendant's Privacy Policy further states, "MOUNT SINAI ***does not*** share your personally identifiable information with third parties without your consent, except for third-party suppliers that perform essential business or administrative services for us (for example, our web hosting provider). MOUNT SINAI provides these suppliers only with the information they need to perform such services and asks that they either comply with this Privacy Policy or maintain comparable privacy policies that protect your personally identifiable information."[64]

150. Defendant's Notice of Privacy Practices explains Defendant's legal duties with respect to Private Information and the exceptions for when Defendant can lawfully use and disclose Plaintiffs' and Class Members' Private Information in the following ways:

- Treatment;
- Payment;
- Business operations;
- Appointment reminders, treatment alternatives, benefits and services;
- Fundraising ("We will not sell your PHI without your authorization.");
- Business associates ("we will have a written contract with them that requires the BA and any of its subcontractors to protect the privacy of your PHI. They and their subcontractors are independently required by federal law to protect your information.");
- In-Patient Directory;
- Family and friends involved in your care;
- As required by law;
- Public health activities;
- Victims of abuse, neglect or domestic violence;
- Health oversight activities,
- Product monitoring, repair and recall;
- Lawsuits and disputes;
- Law enforcement;
- To avert a serious and imminent threat to health or safety;
- National security and intelligence activities or protective services;
- Military and veterans;
- Inmates and correctional institutions;
- Workers' compensation;
- Coroners, medical examiners and funeral directors;
- Organ and tissue donation;

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

- Research;
- Completely de-identified of partially de-identified information;
  Incidental disclosures ("While we will take reasonable steps to safeguard the privacy of your PHI, certain disclosures of your PHI may occur during or as an unavoidable result of our otherwise permissible uses or disclosures of your PHI"). [65]

151. Defendant's Privacy Policy does ***not*** permit Defendant to use nor disclose Plaintiffs' and Class Members' PHI for marketing purposes.

152. Mount Sinai also acknowledges that it is "required by law to protect the privacy of your health information."[66]

153. Mount Sinai breached its own privacy policies by unlawfully intercepting and disclosing Users' Private Information to Facebook, Google and likely other third parties without obtaining patients' consent or authorization.

H. Mount Sinai Violated HIPAA.

154. Defendant's disclosure of Plaintiffs' and Class Members' Private Information to entities like Facebook also violated HIPAA.

155. Under federal law, a healthcare provider may not disclose PII, non-public medical information about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[67]

156. Guidance from HHS instructs healthcare providers that patient status alone is protected by HIPAA.

---

[65]https://www.mountsinai.org/files/MSHealth/Assets/HS/About/Compliance/Notice-of-Privacy-Practices-NOPP%20-English.pdf (last visited Jan. 9, 2024).

[66] *Id*.

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

157. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

158. The Privacy Rule broadly defines protected health information as individually identifiable health information that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

159. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (i) 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 (ii) "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."[68]

160. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—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.

161. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be PHI.

162. HHS has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, "[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."[69]

163. 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."[70]

---

[68] *See* 45 C.F.R. § 160.514.

[69] *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, (last visited Jan. 9, 2024).

[70] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (last visited

164. Here, as described *supra*, Mount Sinai provided patient information to third parties in violation of the Privacy Rule—and 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."

165. 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).

166. 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 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).

167. HIPAA also requires Mount Sinai 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)—which Mount Sinai failed to do.

168. Under HIPPA, Mount Sinai may not disclose PII about a patient, potential patient or household member of a patient for marketing purposes without the patient's express written

---

Jan. 9, 2024).

authorization. *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

169. Mount Sinai further failed to comply with other HIPAA safeguard regulations as follows:

a) Failing to ensure the confidentiality and integrity of electronic PHI that Mount Sinai created, received, maintained and transmitted in violation of 45 C.F.R. section 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. section 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 Mount Sinai in violation of 45 C.F.R. section 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. section 164.306(a)(2);

e) Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3), and

f) Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

170. In disclosing the content of Plaintiffs and the Class Members' communications, Mount Sinai had a purpose that was tortious, criminal and designed to violate state constitutional and statutory provisions.

171. Commenting on a June 2022 report discussing the use of Meta Pixels 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."[71]

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

I. Mount Sinai's Use of the Pixels Violates OCR Guidance.

173. The government has issued guidance warning that tracking technologies like the Pixels may come up against federal privacy law when installed on healthcare websites.

174. Healthcare organizations regulated under the HIPAA 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. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[72]

175. According to the Bulletin, Mount Sinai has violated HIPAA rules by implementing the Pixels.[73]

176. Mount Sinai has shared Plaintiffs' and Class Members' Private Information, including health conditions for which they seek treatments, treatments and/or medications sought, the frequency with whom they take steps to obtain healthcare for certain conditions and their

[71] 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 Jan. 9, 2024).

[72] *See* OCR Bulletin, *supra,* note 8.

[73] *See id*. ("disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures").

unique personal identifiers. This information is, as described in the OCR Bulletin, "highly sensitive."

177. The OCR Bulletin goes on to make clear how broad the government's view of protected information is as it explains:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code***.[74]

178. Mount Sinai's sharing of Private Information with the Pixel Information Recipients violated Plaintiffs' and Class Members' rights.

J. Mount Sinai Violated Industry Standards.

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

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

181. 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)[.] [75]

182. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent

[74] *Id.* (emphasis added).
[75] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (last visited Jan. 9, 2024).

> undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.[76]

183. 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.[77]

184. Mount Sinai's use of the Pixels also violates FTC data security guidelines. The FTC has promulgated numerous guides for businesses, which highlight the importance of implementing reasonable data security practices.

185. The FTC's October 2016 publication *Protecting Personal Information: A Guide for Business*[78] established cyber-security guidelines for businesses. These guidelines state 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.

186. In fact, the FTC has recently brought enforcement actions against several healthcare companies, including Premom, BetterHelp, GoodRx and Flow Health for conveying

---

[76] *Id*.

[77] *Id*.

[78] *See* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 9, 2024).

information—or enabling an inference—about their consumers' health to unauthorized third parties without the consumers' consent.

187. Like the health care companies fined by the FTC in recent years, Mount Sinai failed to implement these basic, industry-wide data security practices.

K. Defendant Violated New York Standards.

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

189. New York requires patient consent before a physician can disclose an individual's medical information to another treating physician and limits disclosure to immediately relevant information.[79]

190. Even stronger protections restrict the release of certain especially sensitive information regarding genetic tests,[80] mental health,[81] medical treatment of adolescents,[82] sexually transmitted infections[83] and HIV.[84]

[79] *See* New York Public Health Law § 18(6).
[80] *See* New York Civil Rights Law § 79-l.

[81] *Id*., § 79-j; New York Public Health Law § 18(1)(e); Mental Hygiene Law § 33.13.

[82] *See* 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).

[83] *See* New York Public Health Law Chapter 45, § 2306.

[84] *See* New York Public Health Law Chapter 45, Article 27-F.

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

192. 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."[85]

193. This provision has been interpreted to require hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes.[86]

194. 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.[87]

195. Accordingly, Mount Sinai's decision to embed the Pixels and disclose Users Private Information without consent violated New York standards.

L. Users' Reasonable Expectation of Privacy.

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

197. Indeed, when Plaintiffs and Class Members provided their PII/PHI to Defendant, they each had a reasonable expectation that the information would remain private, and that

[85] 10 NYCRR § 405.10 (a)(6).

[86] *See Williams v. Roosevelt Hospital*, 66 N.Y.2d 391 (1985).
[87] 10 NYCRR § 405.10 (a)(2).

Defendant would not share the Private Information with third parties for a commercial purpose unrelated to patient care.

198. 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.

199. For example, a recent 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.[88]

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

201. Plaintiffs' and Class Members' reasonable expectations of privacy in their PII/PHI are grounded in, among other things, Defendant's status as a healthcare provider, Defendant's 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 Defendant's express and implied promises of confidentiality.

M. Unique Personal Identifiers are Protected Health Information.

[88] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/ (last visited Jan. 9, 2024).

202. While not all health data is covered under HIPAA, the law specifically applies to healthcare providers, health insurance providers and healthcare data clearinghouses.[89]

203. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered PII. This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual.

204. These HIPAA Identifiers, as relevant here, include names, dates related to an individual, email addresses, device identifiers, web URLs and IP addresses.[90]

205. Mount Sinai improperly disclosed Plaintiffs' and Class Members' HIPAA identifiers, including their names, emails, dates they sought treatments, computer IP addresses, device identifiers and web URLs visited to the Pixel Information Recipients through their use of the Pixels *in addition to* services selected, patient statuses, medical conditions, treatments, provider information and appointment information.

206. An IP address is a number that identifies the address of a device connected to the Internet. IP addresses are used to identify and route communications on the Internet. IP addresses

---

[89] *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 Jan. 9, 2024).

[90] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Jan. 9, 2024).

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

207. Facebook tracks every IP address ever associated with a Facebook user (and with non-users through shadow profiles). Google also tracks IP addresses associated with Internet users.

208. Facebook, Google and other third-party marketing companies track IP addresses to target individual homes and their occupants with advertising.

209. Under HIPAA, an IP address is considered personally identifiable information, which is defined as including "any unique identifying number, characteristic or code" and specifically listing IP addresses among examples. *See* 45 C.F.R. § 164.514 (2).

210. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

211. Consequently, Mount Sinai's disclosure of Plaintiffs' and Class Members' IP addresses violated HIPAA and industry-wide privacy standards.

N. Mount Sinai was Enriched & Benefitted from the Use of the Pixel & Other Tracking Technologies.

212. One of the primary reasons that Mount Sinai decided to embed Pixels and other tracking technologies on its Web Properties was to improve marketing by creating campaigns that maximize conversions and thereby decrease costs to Mount Sinai and boost its revenues.

213. After receiving individually identifiable patient health information communicated on Mount Sinai's Web Properties, Facebook forwards this data, and its analysis of this data, to Mount Sinai.

214. Mount Sinai then uses this data and analysis for its own commercial purposes that include understanding how Users utilize its Web Properties.

215. Mount Sinai also receives an additional commercial benefit from using Facebook's tracking tools, such as the Meta Pixel and Conversions API, namely being able to serve more targeted advertisements to existing and prospective patients on their Meta accounts such as Facebook and Instagram.

216. Facebook advertises its Pixel as a piece of code "that can help you better understand the ***effectiveness of your advertising*** and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting. And when you use the Conversions API alongside the Pixel, it creates a more reliable connection that helps the delivery system ***decrease your costs***."[91]

217. Retargeting is a form of online marketing that targets users with ads based on previous internet communications and interactions. In particular, retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.[92]

218. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook via the tracking technologies and the Pixel embedded on, in this case, Mount Sinai's Web Properties. For example, when a User searches for doctors or medical conditions or treatment on Mount Sinai's Web

[91] *What is the Meta Pixel,* https://www.facebook.com/business/tools/meta-pixel (emphasis added) (last visited Jan. 9, 2024).
[92] *The complex world of healthcare retargeting,* https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/ (last visited Jan. 9, 2024).

Properties, that information is sent to Facebook. Facebook can then use its data on the User to find more users to click on a Mount Sinai ad and ensure that those users targeted are more likely to convert.[93]

219. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures, "includes URL names of pages visited, and actions taken—all of which could be potential examples of health information."[94]

220. 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.

221. In exchange for disclosing the Private Information of their account holders and patients, Mount Sinai is compensated by the Pixel Information Recipients in the form of enhanced advertising services and more cost-efficient marketing on their platform.

222. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.[95]

223. For example, Freshpaint, a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant. They don't sign BAAs, and the Meta Pixel acts like a giant personal user data

---

[93] *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 Jan. 9, 2024).

[94] *Id.*

[95] *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 Jan. 9, 2024).

vacuum sending PHI to Meta servers," and "[i]f you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[96]

224. Medico Digital also 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."[97]

225. Whether a user has a Facebook profile is not indicative of damages because Facebook creates shadow profiles, and at least one court has recognized that the pixels' ability to track comprehensive browsing history is also relevant. *See, e.g.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where Google combined the unique identifier of the user it collects from websites and Google Cookies that it collects across the internet on the same user).

226. Mount Sinai retargeted patients and potential patients, including Plaintiffs and Class Members.

227. Thus, utilizing the Pixels directly benefits Mount Sinai by, among other things, reducing the cost of advertising and retargeting.

O. Plaintiffs' Private Information is Extremely Valuable.

228. Plaintiffs' and Class Members' Private Information had value, and Mount Sinai's disclosure and interception 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.

---

[96] *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra* note 93.

[97] *The complex world of healthcare retargeting, supra* note 92.

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

230. 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.

231. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[98] A 2015 article from TechCrunch accurately noted that "[d]ata has become a strategic asset that allows companies to acquire or maintain a competitive edge."[99] 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.

232. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data (after costs).[100] 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.

233. 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.

---

[98] *See* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Jan. 9, 2024).

[99] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Jan. 9, 2024).

[100] *See 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 Jan. 9, 2024).

Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[101]

234. 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. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[102]

235. 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.

236. Courts recognize 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 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").

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

---

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

[102] *See 10 Apps for Selling Your Data for Cash*, https://wallethacks.com/apps-for-selling-your-data/ (last visited Jan. 9, 2024).

238. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

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

240. 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."[103]

241. 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).[104]

242. 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.[105]

---

[103] *See* https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Jan. 9, 2024).

[104] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (last visited Jan. 9, 2024) (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

[105] *See* https://time.com/4588104/medical-data-industry/ (last visited Jan. 9, 2024).

243. 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."[106]

244. 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.

245. 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.

246. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

247. Mount Sinai gave away Plaintiffs' and Class Members' communications and transactions on its Website without permission.

248. The unauthorized access to Plaintiffs' and Class Members' personal and Private Information has diminished the value of that information, resulting in harm to Website Users, including Plaintiffs and Class Members.

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

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

A. Plaintiff Rondal Cooper

[106] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Jan. 9, 2024).

250. Beginning in or around 2021, Plaintiff Cooper started to utilize Mount Sinai's Web Properties on his phone and computer to research conditions and treatments, research doctors and specialists and schedule appointments.

251. As a condition of receiving Defendant's services, Plaintiff Cooper disclosed his Private Information to Defendant as recently as May 2023.

252. Plaintiff Cooper communicated with his doctor and requested virtual appointments via Defendant's Website and Patient Portal.

253. Plaintiff Cooper also disclosed information about his specific medical conditions including, but not limited to, [redacted] and treatments sought, including [redacted] to Defendant by using the Website.

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

255. Plaintiff Cooper reasonably expected that his communications with Defendant via the Website and the Portal were confidential, solely between himself and Defendant and that such communications would not be transmitted to or intercepted by a third party.

256. Plaintiff Cooper provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

257. As described herein, Defendant worked along with Facebook to intercept Plaintiff Cooper's communications, including those that contained Private and confidential information.

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

259. Defendant transmitted to Facebook Plaintiff Cooper's FID, computer IP address, location and information such as treatment sought, appointment type, physician selected and button/menu selections.

260. By doing so without his consent, Defendant breached Plaintiff Cooper's right to privacy and unlawfully disclosed his Private Information.

261. After disclosing his private medical information to Defendant, Plaintiff Cooper began receiving targeted ads on his social media accounts such as Facebook, including those related to his medications, conditions, treatments and his specific medical diagnoses (including but not limited to, [redacted]).

262. For example, Plaintiff Cooper began receiving ads related to [redacted].

263. Defendant did not inform Plaintiff Cooper that it had shared his Private Information with Facebook.

264. Plaintiff Cooper suffered damages in, *inter alia*, the form of (i) invasion of privacy; (ii) violation of confidentiality of his Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages and (vi) the continued and ongoing risk to his Private Information.

265. Plaintiff Cooper has a continuing interest in ensuring that his Private Information is protected and safeguarded from future unauthorized disclosure.

B. Plaintiff Coral Fraser

266. Beginning in or around 2017, Plaintiff Fraser started to utilize Mount Sinai's Website on her phone to research conditions and treatments, research doctors and specialists and schedule appointments.

267. As a condition of receiving Defendant's services, Plaintiff Fraser disclosed her Private Information to Defendant as recently as May 2022.

268. Plaintiff Fraser disclosed information about her specific medical conditions including but not limited to [redacted], and treatments sought, including but not limited to, [redacted], to Defendant by using the Website.

269. Plaintiff Fraser further submitted information regarding her personal zip code when she was searching for doctors on the "Find a Doctor" page.

270. Plaintiff Fraser has used the same device to maintain and access an active Facebook account throughout the relevant period in this case.

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

272. Plaintiff Fraser provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

273. As described herein, Defendant worked along with Facebook to intercept Plaintiff Fraser's communications, including those that contained Private and confidential information.

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

275. Defendant transmitted to Facebook Plaintiff Fraser's FID, computer IP address, location, and information such as treatment sought, appointment type, physician selected and their specialty, and button/menu selections.

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

277. Defendant did not inform Plaintiff Fraser that it had shared her Private Information with Facebook.

278. After disclosing her private medical information to Defendant, Plaintiff Fraser began receiving targeted ads on her social media accounts such as Facebook and/or Instagram, including ads related to her specific conditions, treatments, and her medical diagnosis.

279. For example, Plaintiff Fraser began receiving ads related to [redacted].

280. Plaintiff Fraser suffered damages in, *inter alia*, the form of (i) invasion of privacy; (ii) violation of confidentiality of her Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

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

C. Plaintiff Gilbert Manda

282. Beginning in or around August 2022, Plaintiff Manda started to utilize Mount Sinai's Website on his phone and computer to receive healthcare services from Defendant and at Defendant's direction.

283. Beginning in or around April 2023, Plaintiff Manda started to utilize Mount Sinai's Patient Portal.

284. As a condition of receiving Defendant's services, Plaintiff Manda disclosed his Private Information to Defendant as recently as September 2023.

285. Plaintiff Manda scheduled doctor's appointments for himself via Defendant's Website and the Patient Portal, searched for specialists, looked up his records and bills, and communicated with his providers.

286. Plaintiff Manda also disclosed information about his specific medical conditions and the treatments he sought, including but not limited to [redacted], to Defendant by using the Web Properties.

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

288. Plaintiff Manda reasonably expected that his communications with Defendant via the Website and the Portal were confidential, solely between himself and Defendant and that such communications would not be transmitted to or intercepted by a third party.

289. Plaintiff Manda provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

290. As described herein, Defendant worked along with Facebook to intercept Plaintiff Manda's communications, including those that contained Private and confidential information.

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

292. Defendant transmitted to Facebook Plaintiff Manda's FID, computer IP address, location and information such as treatment sought, appointment type, physician selected, and button/menu selections.

293. By doing so without his consent, Defendant breached Plaintiff Manda's right to privacy and unlawfully disclosed his Private Information.

294. After disclosing his private medical information to Defendant, Plaintiff Manda began receiving targeted ads on his social media accounts such as Facebook, including those related to his medications, conditions, treatments and his specific medical diagnoses.

295. Defendant did not inform Plaintiff Manda that it had shared his Private Information with Facebook.

296. Plaintiff Manda suffered damages in, *inter alia*, the form of (i) invasion of privacy; (ii) violation of confidentiality of his Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages and (vi) the continued and ongoing risk to his Private Information.

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

TOLLING

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

CLASS ACTION ALLEGATIONS

299. Plaintiffs bring this action on behalf of themselves and on behalf of 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.

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

> All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the third-party tracking technologies on Defendant's Website or Web Properties.

301. The New York sub-class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the State of New York whose Private Information was disclosed to a third party without authorization or consent through the third-party tracking technologies on Defendant's Website or Web Properties.

302. The Nationwide Class and the New York sub-class 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.

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

304. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are over one million individuals whose PII and PHI may have been improperly accessed by Facebook, and the Class is identifiable within Defendant's records. The vast majority of those Class Members are believed to be New York residents.

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

a. Whether and to what extent Defendant had a duty to protect the Plaintiffs and Class Members' Private Information;

b. Whether Defendant had duties not to disclose the Plaintiffs and Class Members' Private Information to unauthorized third parties;

c. Whether Defendant violated its privacy policy by disclosing Plaintiffs and Class Members' Private Information to Facebook, Meta or additional third parties.

d. Whether Defendant adequately, promptly and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

g. Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Plaintiffs and Class Members' Private Information;

h. Whether Defendant violated the consumer protection statutes invoked herein;

i. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;

j. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices;

k. Whether Defendant's acts and practices violated Plaintiffs' and Class Members' privacy rights;

l. Whether Plaintiffs and Class Members are entitled to actual, consequential or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Defendant knowingly made false representations as to it data security and/or privacy policy practices;

n. Whether Defendant knowingly omitted material representations with respect 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.

306. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use of the Meta Pixel, due to Defendant's misfeasance.

307. **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.

308. **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, like Northwell, with significant resources. 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.

309. **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.

310. 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 they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which 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.

311. 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.

312. **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.

313. **Class-wide Injunctive Relief.** Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Amended Complaint as Defendant has acted or refused to act on grounds generally applicable to the Class

and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

314. 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;

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

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

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

316. 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.

317. The principal place of business and headquarters of Mount Sinai, located at One Gustave L. Levy Place in New York, New York 10029, 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.

318. Defendant's actions and corporate decisions surrounding the allegations made in the Amended Complaint were made from and in New York.

319. Defendant's breaches of duty to Plaintiffs and Class Members emanated from New York.

320. 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.

321. 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.

322. 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
(*On Behalf of Plaintiffs & the Nationwide Class*)

323. Plaintiffs and Class Members repeat and re-allege each and every allegation in the Amended Complaint as if fully set forth herein.

324. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

325. The ECPA protects both sent and received communications.

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

327. The transmissions of Plaintiffs' and Class Members' Private Information to Mount Sinai via Mount Sinai's Website is a "communication" under the ECPA's definition under 18 U.S.C. § 2510(12).

328. The transmission of Private Information between Plaintiffs and Class Members and Mount Sinai via their Website is "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).

329. 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).

330. 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).

331. 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).

332. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Mount Sinai and Meta use to track Plaintiffs' and the Class Members' communications;
b. Plaintiffs' and Class Members' browsers;
c. Plaintiffs' and Class Members' computing devices;
d. Mount Sinai's web-servers and
e. The Pixels deployed by Mount Sinai to effectuate the sending and acquisition of users' and patients' sensitive communications.

333. Plaintiffs and Class Members' interactions with Mount Sinai's Website are electronic communications under the ECPA.

334. By utilizing and embedding the Pixels and Conversions API on their Website and/or servers, Mount Sinai intentionally intercepted, endeavored to intercept and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

335. Specifically, Mount Sinai intercepted Plaintiffs' and Class Members' electronic communications via the Pixels and Conversions API, which tracked, stored and unlawfully disclosed Plaintiffs' and Class Members' Private Information to Facebook.

336. Mount Sinai intercepted communications that included, but are not limited to, communications to/from Plaintiffs and Class Members regarding PII and PHI, including first and last name, email address, IP address, Facebook ID and health information relevant Plaintiffs and Class Members medical conditions and treatment.

337. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to the Pixel Information Recipients and, potentially, 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), Mount Sinai violated 18 U.S.C. § 2511(1)(c).

338. 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), Mount Sinai violated 18 U.S.C. § 2511(1)(d).

339. Mount Sinai intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

340. Mount Sinai intentionally used wire or electronic communications to increase its profit margins. Mount Sinai specifically used the Pixels and Conversions API to track and utilize Plaintiffs' and Class Members' Private Information for its own financial benefit.

341. Mount Sinai was not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communications.

342. Plaintiffs and Class Members did not authorize Mount Sinai to acquire the content of their communications for purposes of invading Plaintiffs' and Class Members' privacy via the Pixels and Conversions API.

343. Any purported consent that Mount Sinai received from Plaintiffs and Class Members was not valid.

344. Mount Sinai is a "party to the communication" with respect to patient communications.

345. In sending and acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Mount Sinai' Website, researching medical conditions and treatment and scheduling appointments with doctors and specialists, Mount Sinai's purpose was tortious and designed to violate federal and state law, including as described above, a knowing intrusion into a private place, conversation or matter that would be highly offensive to a reasonable person.

346. Mount Sinai's acquisition of patient communications that were used and disclosed to Facebook 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*).

347. Consumers have the right to rely upon the promises that companies make to them. Mount Sinai accomplished its tracking through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that cause Facebook pixels and cookies (including but not limited to the fbp, ga and gid cookies) to be deposited on Plaintiffs' and Class members' computing devices as "first-party" cookies that are not blocked.

348. Mount Sinai'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;

b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie on Mount Sinai's Web Properties rather than a third-party cookie from Meta.

349. Mount Sinai 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.

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

a. with knowledge that (1) Mount Sinai did not have the right to share such data without written authorization; (2) courts had determined that a healthcare providers' use of the Meta Pixel gave rise to claims for invasion of privacy and violations of state criminal statutes; (3) a reasonable Facebook user would not understand that Meta was collecting their Private Information based on their activities on Mount Sinai's Web Properties; (4) "a reasonable Facebook user would be shocked to realize" the extent of Meta's collection of Private Information; (5) a Covered Incident had occurred which required a report to be made to the FTC pursuant to Meta's consent decrees with the FTC and (6) 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 the 'fbp' cookie disguised as a first-party cookie.

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

352. 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
(*On Behalf of Plaintiffs & the Nationwide Class*)

353. Plaintiffs and Class Members repeat and re-allege each and every allegation in the Amended Complaint as if fully set forth herein.

354. Upon accepting, storing and controlling the Private Information of Plaintiffs and the Class, Mount Sinai 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.

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

356. It was reasonably foreseeable that Mount Sinai's failures to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information through their use of the Pixels, Conversions API and other tracking technologies would result in unauthorized third parties—such as the Pixel Information Recipients—gaining unlawful access to such Private Information.

357. Mount Sinai'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 Mount Sinai and its patients, which is recognized by statute, regulations and the common law.

358. In addition, Mount Sinai 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.

359. Mount Sinai's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Private Information. Mount Sinai's misconduct included the failure to (i) secure Plaintiffs' and Class Members' Private Information; (ii) comply with industry-standard data security practices; (iii) implement adequate Website and event monitoring and (iv) implement the systems, policies and procedures necessary to prevent unauthorized disclosures resulting from the use of the Pixels, Conversions API and other tracking technologies.

360. As a direct result of Mount Sinai'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.

361. Mount Sinai'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.

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

COUNT III
INVASION OF PRIVACY
(*On Behalf of Plaintiffs & the Nationwide Class*)

363. Plaintiffs and Class Members repeat and re-allege each and every allegation in the Amended Complaint as if fully set forth herein.

364. The highly sensitive and personal Private Information of Plaintiffs and Class Members consists of private and confidential facts and information regarding Plaintiffs' and Class Members' health that were never intended to be shared beyond private communications on the Web Properties and the consideration of health professionals.

365. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this Information against disclosure to unauthorized third parties, including the Pixel Information Recipients.

366. Mount Sinai owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

367. Mount Sinai's unauthorized disclosure of Plaintiffs' and Class Members' Private Information to the Pixel Information Recipients, third-party technology and marketing giants, is highly offensive to a reasonable person.

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

369. Mount Sinai's conduct constitutes an intentional physical or sensory intrusion on Plaintiffs' and Class Members' privacy because Mount Sinai facilitated the Pixel Information Recipients' simultaneous eavesdropping and wiretapping of confidential communications.

370. Mount Sinai failed to protect Plaintiffs' and Class Members' Private Information and acted knowingly when they installed the Pixels onto the Website because the purpose of the Pixels is to track and disseminate Users' communications on the Website for marketing and advertising.

371. Because Mount Sinai intentionally and willfully incorporated the Pixels into the Website and encouraged individuals to use and interact with the Website and the health services thereon, Mount Sinai had notice and knew that their practices would cause injury to Plaintiffs and the Class.

372. As a proximate result of Mount Sinai's acts and omissions, the private and sensitive Private Information, including the PII and PHI of Plaintiffs and Class Members, was disclosed to unauthorized third parties, causing Plaintiffs and the Class to suffer damages.

373. Plaintiffs, on behalf of themselves and Class members, seeks compensatory damages for Mount Sinai's invasion of privacy, which includes the value of the privacy interest invaded by Mount Sinai, loss of time and opportunity costs, lost benefit of the bargain and pre-judgment interest and costs.

374. Mount Sinai's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Mount Sinai and still in the possession of the Pixel Information Recipients, and the wrongful disclosure of the Private Information cannot be undone.

375. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Mount Sinai's and unauthorized third parties' continued possession of their sensitive and confidential Private Information. A judgment for monetary damages will not undo Mount Sinai's disclosure of the Private Information to unauthorized third parties who, upon information and belief, continue to possess and utilize the Private Information.

376. Plaintiffs, on behalf of themselves and Class members, further seek injunctive relief to enjoin Mount Sinai from intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information and to adhere to its common law, contractual, statutory and regulatory duties.

COUNT IV
BREACH OF IMPLIED CONTRACT
(*On behalf of Plaintiffs & the Nationwide Class*)

377. Plaintiffs and Class Members repeat and re-allege each and every allegation in the Amended Complaint as if fully set forth herein.

378. Defendant required Plaintiffs and Class Members to provide their Private Information, including names, email addresses, phone numbers, computer IP addresses, appointment information and other content submitted to Defendant's Website as a condition of their receiving healthcare services.

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

380. Plaintiffs and Class Members accepted Mount Sinai's offers and provided their Private Information to Mount Sinai.

381. Plaintiffs and Class Members fully performed their obligations under the contract with Defendant.

382. Defendant'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.

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

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

385. Mount Sinai breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information to a third party like Facebook.

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

387. Plaintiffs and Class Members are entitled to compensatory and consequential damages because of Mount Sinai's breach of implied contract.

COUNT V
BREACH OF FIDUCIARY DUTY
(*On behalf of Plaintiffs & the Nationwide Class*)

388. Plaintiffs and Class Members repeat and re-allege each and every allegation in the Amended Complaint as if fully set forth herein.

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

390. Defendant 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 intentionally disclosing, the Private Information of Plaintiffs and Class Members.

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

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

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

394. As a direct and proximate result of Defendant'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 VI
UNJUST ENRICHMENT
(*On behalf of Plaintiffs & the Nationwide Class*)

395. Plaintiffs repeat and re-allege each and every allegation contained in the Amended Complaint as if fully set forth herein.

396. Mount Sinai benefited from Plaintiffs' and Class Members' Private Information and unjustly retained those benefits at Plaintiffs' and Class Members' expense.

397. Plaintiffs and Class Members conferred a benefit upon Mount Sinai in the form of the monetizable Private Information that Mount Sinai collected from them and disclosed to third parties, including the Pixel Information Recipients, without authorization and proper compensation.

398. Mount Sinai consciously collected and used this information for their own gain, providing Mount Sinai with economic, intangible and other benefits, including substantial monetary compensation.

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

400. The benefits that Mount Sinai derived from Plaintiffs and Class Members were not offered by Plaintiff or Class members gratuitously and, thus, rightly belongs to Plaintiffs and Class Members.

401. It would be inequitable under unjust enrichment principles and in New York for Mount Sinai 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 Amended Complaint.

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

COUNT VII
BREACH OF CONFIDENCE
(*On behalf of Plaintiffs & the Nationwide Class*)

403. Plaintiffs repeat and re-allege each and every allegation contained in the Amended Complaint as if fully set forth herein.

404. Medical providers, such as Mount Sinai, have a duty to their patients to keep non-public medical information confidential.

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

406. Contrary to their duties as health care institutions and their express promises of confidentiality, Mount Sinai installed the Pixels and Conversions API to disclose and transmit to third parties Plaintiffs' and Class Members' Private Information, including data relating to Plaintiffs' and Class Members' health.

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

408. The third-party recipients included, but may not be limited to, the Pixel Information Recipients.

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

410. As a direct and proximate cause of Mount Sinai's unauthorized disclosures of Plaintiffs' and Class Members' Private Information, Plaintiffs and Class Members were damaged by Mount Sinai'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) Mount Sinai 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 VIII
CONSTRUCTIVE BAILMENT
(*On behalf of Plaintiffs & the Nationwide Class*)

411. Plaintiffs repeat and re-allege each and every allegation contained in the Amended Complaint as if fully set forth herein.

412. Mount Sinai acquired and was obligated to safeguard the Private Information of Plaintiffs and Class Members.

413. Mount Sinai 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.

414. Specifically, a constructive bailment arises when Mount Sinai, 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.

415. 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.

416. During the bailment, Mount Sinai owed a duty to Plaintiffs and Class Members to exercise reasonable care, diligence and prudence in protecting their Private Information.

417. Mount Sinai 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 by third parties such as Facebook.

418. Mount Sinai 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.

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

COUNT IX
IMPLIED COVENANT OF GOOD FAITH & FAIR DEALING
(On Behalf of Plaintiffs & the Nationwide Class)

420. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Amended Complaint as if fully set forth herein.

421. Plaintiffs and Class Members entered into valid, binding, and enforceable implied contracts with Mount Sinai, as alleged above.

422. 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.

423. These included the implied covenants that Mount Sinai 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.

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

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

426. Plaintiffs and Class Members performed all conditions, covenants, obligations and promises owed to Mount Sinai.

427. Mount Sinai'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.

428. Accordingly, Plaintiffs and Class Members have been injured as a result of Mount Sinai'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 X

VIOLATION OF THE NEW YORK DECEPTIVE TRADE PRACTICES ACT

New York Gen. Bus. Law § 349, *et seq.*

(On Behalf of Plaintiffs & the Nationwide Class &
Alternatively on behalf of Plaintiffs & the New York sub-class)

429. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Amended Complaint as if fully set forth herein.

430. By the acts and conduct alleged herein, Defendant 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 Facebook Pixel to operate as intended and transmit Plaintiffs' and Class Members' Private Information without their authorization to Facebook;

c. failing to disclose or omitting material facts to Plaintiffs and Class Members regarding the disclosure of their Private Information to Facebook;

d. failing to take proper action to ensure the Pixel was configured to prevent unlawful disclosure of Plaintiffs' and Class Members' Private Information;

e. unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook.

431. 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.

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

433. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant 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 Defendant's offering of goods and services.

434. Specifically, Defendant was aware that Plaintiffs and Class Members depended and relied upon it to keep their communications confidential, and Defendant instead disclosed that information to Facebook.

435. In addition, Defendant's material failure to disclose that Defendant collects Plaintiffs' and Class Members' Private Information for marketing purposes with Facebook constitutes an unfair act or practice prohibited by the NY GBL § 349. Defendant's actions were immoral, unethical and unscrupulous.

436. Plaintiffs had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged at https://www.mountsinai.org and https://mychart.mountsinai.org/.

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

438. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Pixel to disclose and transmit Plaintiffs' personally identifiable, non-public medical information and the contents of her communications exchanged with Defendant to third parties, i.e., Facebook.

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

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

441. Defendant willfully, knowingly, intentionally and voluntarily engaged in the aforementioned acts when it incorporated the Facebook Pixel with knowledge of the Pixel's purpose and functionality.

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

443. As a result of Defendant's wrongful conduct, Plaintiffs were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's services, had they known or been told that Defendant shared their confidential and sensitive Private Information with Facebook.

444. As a direct and proximate result of Defendant's multiple, separate violations of the NY GBL § 349, Plaintiffs and Class member have suffered harm, including financial losses related to the payments or services made to Defendant that Plaintiffs and Class Members would not have made had they known of Defendant's disclosure of their PII and PHI to Facebook; 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.

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

446. Plaintiffs bring this action on behalf of herself 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 purchasing decisions and to protect Plaintiffs, Class Members and the public from Defendant's unfair, deceptive and unlawful

practices. Defendant's wrongful conduct as alleged in this Amended Complaint has had widespread impact on the public at large.

447. 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 Rondal Cooper, Coral Fraser and Gilbert Manda respectfully pray for judgment in their favor and against Defendant Mount Sinai 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 consumer 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 Rondal Cooper, Coral Fraser and Gilbert Manda hereby demand that this matter be tried before a jury.

Date: December 10, 2024

Respectfully submitted,

s/: David S. Almeida
David S. Almeida
New York Bar No. 3056520
Elena A. Belov
New York Bar No. 4080891
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
T: (708) 529-5418
david@almeidalawgroup.com
elena@almeidalawgroup.com

WEITZ & LUXENBERG, PC
James J. Bilsborrow
New York Bar No. 4702064
700 Broadway
New York, NY 10003
(212) 558-5500
jbilsborrow@weitzlux.com

Attorneys for Plaintiffs & Putative Classes