ROPES & GRAY

ALERT

December 15, 2022

Use of Tracking Technology- Walking the Regulatory Line?

Background

Attorneys
Deborah L. Gersh
Jennifer L. Romig
Jamie E. Darch
Ryan Gorman

Across industries, organizations have deployed online tracking technologies, supplied by third-party vendors, on websites and mobile applications, to collect and analyze information about user behavior and enhance the user experience. Many organizations also rely on these technologies to ensure their websites and applications are functioning properly and to provide crash reports when users encounter issues, thereby playing an integral role in reducing downtime and timely addressing other website access and operational issues, as discussed further below. Tech giants such as Google[1] and Meta, the parent company of Facebook,[2] offer these technology services, which also include cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts, to organizations who may choose to embed them in the code of the organizations' websites and applications.

Despite widespread use by both government[3] and private organizations, health systems and hospitals have recently been scrutinized for their use of online tracking technologies, particularly with respect to their appointment scheduling pages, patient portals, and mobile applications. Beginning with a class action brought against Mass General Brigham and Dana-Farber in 2019, patients have alleged that hospitals' use of third-party tracking technology, without patient consent, violated their privacy rights, as well as state consumer protection statutes.[4] Following the Mass General and Dana Farber settlement in early 2022 for $18.4 million,[5] a tech-focused journalism outlet, The Markup, published an exposé in June 2022 claiming that, of the top 100 Newsweek-ranked U.S. hospitals, 33 had installed the Meta Pixel on appointment scheduling pages, and six had installed the Meta Pixel on patient portals, potentially violating patient privacy.[6]

Since the Markup article was published, class action lawsuits have been filed against a growing number of hospitals and health systems—including Dignity Health/University of California San Francisco,[7] MedStar,[8] Northwestern Memorial Hospital,[9] Rush System for Health,[10] UPMC,[11] and Advocate Aurora Health[12] —and have named tracking vendors, such as Google and Meta, as co-defendants or entities involved in unlawful tracking.[13] These lawsuits assert, among other things, that online tracking technologies were installed on hospital scheduling pages and/or patient portals, resulting in the transmission of sensitive patient information to third-party vendors without patient consent in violation of applicable state privacy and consumer protection laws.

In the six months following the release of the Markup article, the United States Department of Health and Human Services Office for Civil Rights ("OCR") did not issue guidance as to the implications of tracking technology for entities subject to HIPAA.[14] Even without such guidance, four health systems proactively reported breaches involving protected health information ("PHI") stemming from their use of online tracking technologies, including Novant Health (August 12, 2022),[15] WakeMed (October 14, 2022),[16] Advocate Aurora Health (October 14, 2022),[17] and Community Health Network (November 18, 2022).[18]

OCR Guidance

On December 1, 2022, OCR broke its silence and issued a bulletin titled "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,"[19] which sets forth broad-reaching guidance for HIPAA covered entities and their business associates ("regulated entities") that utilize online tracking technologies on their webpages and applications. In the guidance, OCR takes the position that individuals may provide certain information (including IP address, geographic location, or other unique identifying code) when using a regulated entity's website or app, and that all such information is generally PHI required to be protected in accordance with HIPAA. This is the case even if (1) the information, such as IP address or geographic location, does not include health information, and (2) the individual does not have an existing patient relationship with the regulated entity. Seeming to anticipate objections to this broad interpretation of what constitutes PHI, OCR defends its position by asserting that "when a regulated entity collects the individual's [information] through its website or mobile app, the information connects the individual to the regulated

entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care."[20]

OCR then reviews three modalities in which online tracking technologies may be used by regulated entities: (1) *user-authenticated* webpages that require a user login (for example, a patient portal); (2) *unauthenticated* webpages that do not require a user login (for example, a health system home page); and (3) *mobile applications* ("apps").

User-authenticated webpages. With respect to user-authenticated webpages, such as patient portals, OCR concludes that "[t]racking technologies on a regulated entity's user-authenticated webpages "***generally have access to PHI***,"[21] including the individual's IP address, email address, and appointment dates, as well as more sensitive information related to the individual's diagnosis, treatment, or insurance. As a result, OCR concludes that regulated entities must ensure that the disclosures made to such vendors are permitted by HIPAA and enter into a business associate agreement ("BAA") with tracking technology vendors who may receive such information.

Unauthenticated webpages. OCR notes that tracking technologies on unauthenticated webpages, in contrast, "generally do not have access to individuals' PHI" and are therefore not regulated by HIPAA.[22] However, OCR provides two categories where HIPAA would apply:

- If a patient enters credential information (e.g., name, email address) on the login or registration page of a regulated entity's patient portal, "such information is PHI"[23] and is protected by HIPAA.

- If a regulated entity's unauthenticated webpage "addresses specific symptoms or health conditions, such as pregnancy or miscarriage"[24] or "permits individuals to search for doctors or schedule appointments without entering credentials," tracking technologies installed on such pages also "may have access to PHI in certain circumstances."[25] OCR specifically contemplates that if a regulated entity's use of tracking technology "collect[s] an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider," such regulated entity "***is disclosing PHI*** to the tracking technology vendor, and thus the HIPAA Rules apply."[26]

Mobile apps. With respect to mobile apps, OCR asserts that user information, including device fingerprints, network location, geolocation, device ID, advertising ID, and health medical information, "collected by a regulated entity's mobile app ***is PHI***,"[27] such that disclosure of such information to tracking technology vendors is subject to HIPAA. OCR distinguishes those mobile apps that "are not developed or offered by or on behalf of regulated entities"[28] as not subject to HIPAA.

OCR concludes its guidance by reviewing compliance obligations of regulated entities that utilize tracking technologies. First, OCR notes that HIPAA regulated entities cannot simply inform users of potential third-party disclosures of an individual's PHI to a third party (whether via a privacy policy, notice, or website terms and conditions) if such consent does not qualify as a valid HIPAA authorization, thus foreclosing any argument that acceptance of such terms and conditions is sufficient (e.g., website banners asking users simply to accept or reject a website's use of tracking technologies, such as cookies). Second, OCR explains that the disclosure of PHI to a tracking vendor (without a patient HIPAA authorization) necessitates a BAA, regardless of whether such vendors otherwise agree to remove or de-identify PHI upon receipt. Third, OCR recommends "[a]ddressing the use of tracking technologies in the regulated entity's Risk Analysis and Risk Management processes" and also implementing Security Rule safeguards (e.g., "encrypting ePHI transmitted to the tracking technology vendor")[29]. Finally, OCR requires regulated entities to report "an impermissible disclosure of PHI to a tracking technology vendor [with whom the regulated entity has no BAA in place] that compromises the security or privacy of PHI" as a HIPAA breach.[30]

Practical Implications

Everything the Light Touches is PHI? In promulgating this guidance, OCR appears to take an expansive view of the information that constitutes PHI. In making these assumptions, OCR appears to dismiss the threshold question of whether information collected by tracking technology is being collected from patients of the regulated entity and relates to the past, present, or future health, health care, or payment for health care for that patient.

When looking at how individuals use the internet and mobile apps, however, we can imagine multiple scenarios where an individual accesses a regulated entity's unauthenticated webpage or mobile app without being a patient of that entity, and/or without providing health-related information to that entity. OCR does not suggest that evaluating the answers to these threshold questions is a necessary part of the analysis that should be undertaken by regulated entities and does not provide any framework for such evaluation.

Has a breach occurred? In declaring that a breach notification should be provided in the event of an "impermissible disclosure" of PHI by a regulated entity to a tracking technology vendor without a BAA in place, OCR notes that "there is a presumption that there has been a breach of unsecured PHI unless the regulated entity can demonstrate that there is a low probability that the PHI has been compromised."[31] OCR declines, however, to provide practical guidance regarding how a regulated entity can assess the risk of compromise to PHI in the context of tracking technology. Importantly, OCR requires evaluation of the following factors in determining whether there has been a low risk of compromise:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.[32]

Conducting this assessment in the context of tracking technology can be practically difficult, as many regulated entities using tracking technology may not know the details of whether or how the tracking vendor uses PHI that may be collected, including whether the tracking vendor would be able to re-identify the individual based on the information provided. Further, the information obtained by the tracking vendor may vary depending on whether the user was logged in to his or her personal account with the tracking vendor (*e.g.*, a Google or Facebook account), and the type of device used to access the website or app. However, such factors may not be known by a regulated entity.

Without direction from OCR regarding how to conduct a breach risk assessment for disclosures involving tracking technology, regulated entities likely will be faced with evaluating the factors within their knowledge and control—namely, the sensitivity of the information disclosed, as well as steps taken to mitigate the disclosure, which could potentially include (a) obtaining assurances from vendors that such vendors have not misused patient information and have also deleted or returned any PHI, and (b) halting the use of tracking technologies on website and application platforms to limit future impermissible disclosures.

What about patient care? The OCR guidance implies several go-forward options for regulated entities that deploy tracking technologies on platforms that may access PHI: (1) obtain a HIPAA authorization from patients to share the information with tracking vendors, (2) use a tracking vendor that has executed a HIPAA-compliant BAA, (3) build internal tracking technology, within the regulated entity, or (4) remove tracking from platforms. Unfortunately, these options fail to address the practical considerations facing regulated entities that seek to provide patients with seamless, efficient access to websites and mobile apps. Regulated entities that currently use tracking technologies on the platforms OCR perceives as containing PHI may deem it logistically impossible or impractical to obtain a HIPAA authorization. Leading tracking technology vendors may also decline to execute BAAs, leaving regulated entities to scramble for replacement vendors or to build internal capabilities, both of which may be cost prohibitive for smaller organizations.

Moreover, removing tracking platforms—either temporarily or as stop-gap measure before identifying replacement vendors—may, as a practical matter, prohibit regulated entities from ensuring their platforms are functioning appropriately (as many entities use tracking technology to assess when websites or mobile apps malfunction), or may require regulated entities to terminate access to their platforms, irrespective of whether the website or mobile app is necessary to facilitate patient care. Tracking technologies provide valuable data to identify the efficacy of services provided on regulated entities' websites and mobile apps, and, without these technologies, regulated entities will be hampered in their ability to better understand patient needs and enhance access to care. In proscribing these go-forward options, OCR does not provide guidance for entities that are concerned that such options may negatively impact patients.

What now? OCR's guidance may implicate a number of regulated entities, given the proliferation of tracking technology throughout the health care industry. In determining next steps, we recommend:

- Evaluating whether your organization has tracking technologies deployed on websites or mobile apps that have access to PHI;
- Assessing whether information disclosed to tracking technology vendors constitutes a breach of PHI under a four-factor risk assessment; and
- Considering the pathways available to your organization to ensure tracking technology that is necessary for the operation of websites and mobile apps that are used for the provision of patient care can be deployed in a HIPAA-compliant manner.

1. See Google Analytics, https://analytics.google.com/analytics/web/provision/#/provision.
2. See Meta Pixel, https://developers.facebook.com/docs/meta-pixel/.
3. For example, the Centers for Medicare & Medicaid Services ("CMS") use pixel tracking on their website. *See* Centers for Medicare & Medicaid Services, "Privacy Policy" (last visited Dec. 6, 2022).
4. Doe v. Partners Healthcare System, Inc., No. 19-1657 (Suffolk Super Ct., May 23, 2019).
5. Suffolk Superior Court, Notice of Class Action Settlement, No. 1984CV01651-BLS1 (Sep 24, 2021).
6. T. Feathers et al., "Facebook Is Receiving Sensitive Medical Information from Hospital Websites," The Markup (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites
7. Doe v. Meta Platforms, Inc., No. 3:22-cv-04293 (N.D. Cal., July 25, 2022) (UCSF and Dignity Health named as co-defendants).
8. Doe v. Meta Platforms, Inc., No. 5:22-cv-03580 (N.D. Cal., June 17, 2022) (involving tracking on MedStar patient portal).
9. Krackenberger v. Northwestern Memorial Hospital, No. 1:22-cv-04203 (N.D. Ill., Aug. 10, 2022).
10. Kurowski v. Rush System for Health, No. 1:22-cv-05380 (N.D. Ill., Sep. 30, 2022).
11. Smidga v. Meta Platforms, Inc, No. 2:22-cv-1231 (W.D. Penn. Aug. 25, 2022) (UPMC named as co-defendant).
12. Stewart v. Advocate Aurora Health, Inc., No. 1:22-cv-05964 (E.D. Wis., Oct. 28, 2022); John v. Advocate Aurora Health, Inc., No. 2:22-cv-01253 (E.D. Wis., Oct. 24, 2022); Ajani v. Advocate Aurora Health, Inc.(Cook County Circuit Court, Oct. 24, 2022), *available at* https://unicourt.com/case/pc-db5-ajani-v-advocate-aurora-health-inc-1344164; Webster v. AAH, No. 2:22-cv-01278 (E.D. Wis., Oct. 27, 2022), *available at* https://unicourt.com/case/pc-db5-webster-v-advocate-aurora-health-inc-1326002; Danger v. AAH, No. 2:22-cv-01305 (E.D. Wis., Nov. 3, 2022), *available at* https://www.pacermonitor.com/public/case/46700954/Danger_v_Advocate_Aurora_Health,_Inc
13. *See, e.g.*, Krackenberger v. Northwestern Memorial Hospital, No. 1:22-cv-04203 (N.D. Ill., Aug. 10, 2022) (Meta, Facebook, and Instagram named as co-defendants); Stewart v. Advocate Aurora Health, Inc., No. 1:22-cv-05964 (E.D. Wis., Oct. 28, 2022) (Meta named as co-defendant); Kurowski v. Rush System for Health, No. 1:22-cv-05380 (N.D. Ill., Sep. 30, 2022) (Google named as vendor involved in unlawful tracking).
14. Health Insurance Portability and Accountability Act of 1996, as amended, together with its implementing regulations ("HIPAA").
15. Novant Health, "Your Medical Privacy Is Our Top Priority," (Aug. 12, 2022), https://www.novanthealth.org/home/privacy-statement/pixel.aspx
16. WakeMed, News Release, (Oct. 14, 2022), https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident (discussing WakeMed's use of pixel software on its websites).
17. Advocate Aurora Health, "Notice of Data Breach" (Oct. 14, 2022), https://www.advocateaurorahealth.org/pixel-notification/
18. Community Health Network, "Notice of Third-Party Tracking Technology Data Breach" (Nov. 16, 2022), https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach
19. OCR, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html ("OCR Dec. 2022 Bulletin").
20. OCR Dec. 2022 Bulletin (emphasis added).
21. *Id.* (emphasis added).
22. *Id.*
23. *Id.*
24. We note the specific discussion of pregnancy or miscarriage may relate to guidance HHS issued in response to the Supreme Court ruling in *Dobbs v. Jackson Women's Health Organization*, which demonstrates HHS's ongoing concern regarding how to ensure privacy for women who may seek abortion care. *See* U.S. Dept. Health & Human Services, "HHS Issues Guidance to Protect Patient Privacy in Wake of Supreme Court Decision on Roe," (June 29, 2022), https://www.hhs.gov/about/news/2022/06/29/hhs-issues-guidance-to-protect-patient-privacy-in-wake-of-supreme-court-decision-on-roe.html.
25. OCR Dec. 2022 Bulletin.
26. *Id.* (emphasis added).
27. *Id.* (emphasis added).
28. *Id.*
29. *Id.*
30. *Id.*
31. *Id.*
32. 45 C.F.R. 164 § 402(2).