AMERICAN HEALTH LAW ASSOCIATION

HEALTH LAW WEEKLY
April 12, 2024

OCR's Updated Tracking Technology Guidance

Carolyn V. Metnick, Sheppard Mullin Richter & Hampton LLP

On March 18 2024, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) updated its guidance on the use of tracking technologies.[1] Unfortunately, the updated guidance provides little clarity to Health Insurance Portability and Accountability Act (HIPAA)-regulated entities, many of which continue to grapple with the questions of whether their third-party tracking technologies on websites, portals, and applications receive protected health information (PHI) and whether the deployment of the technologies resulted in an impermissible use or disclosure of PHI to a third-party tracking technology vendor in violation of HIPAA.

In December 2022, the OCR published its initial guidance (Bulletin), which forced many HIPAA-regulated entities to investigate their use of tracking technologies (e.g., pixels, web beacons, and cookies) and to analyze whether their use complies with the Bulletin. The complexity of these questions, the Bulletin's lack of clarity (which upended prior thinking), and the evolving litigation landscape, including a lawsuit brought by the American Hospital Association (AHA), has fueled frustration and confusion among HIPAA-regulated entities. The potential for Federal Trade Commission or OCR enforcement action[2] and class action litigation also raises the stakes. Hospitals and health systems, among others, continue to

spend significant resources on investigation, analysis, and remediation, with the hope of complying with the Bulletin without a bright-line rule or clear direction.

When AHA, along with the Texas Hospital Association, Texas Health Resources, and United Regional Health Care System, filed a lawsuit against the Secretary of HHS and the Director of OCR on November 2, 2023[3] in response to the Bulletin, HIPAA-regulated entities may have thought enforcement risk as lower while the lawsuit played out. The AHA lawsuit challenges the suggestion that the use of tracking technologies on unauthenticated sites may be subject to HIPAA, alleging that HHS exceeded its authority and created a rule without following the rulemaking process outlined in the Administrative Procedure Act. AHA and other plaintiffs asked the court to prevent enforcement of the Bulletin and to declare that IP addresses are not individually identifiable health information (IIHI), among other relief. In the event that the court finds in favor of the plaintiffs, HIPAA-regulated entities would have more of a bright-line rule to follow. Although the litigation continues (albeit slowly), OCR makes it clear through the updated guidance that tracking technology enforcement remains a priority.

The updates to the guidance include:

- An example of how insights gleaned from tracking technologies may be beneficial to HIPAA-regulated entities.

- Clarification that a tracking technology connecting "the IP address of a user's device with a visit to a website addressing specific health conditions or listing health care providers" is insufficient in and of itself to constitute IIHI if the visit to the site is not related to the individual's health, health care, or payment for health care.[4]

- Specific examples of when visits to unauthenticated webpages may or may not involve the disclosure of PHI, including:
    - Where a user visits pages about job postings or visiting hours on a hospital website, the information that shows the visit, along with the user's IP address, geographic location, or other identifying information, would not involve a disclosure of PHI (even if the user could reasonably be identified) because the technology did not have access to the individual's health, health care, or payment information.
    - A student writing a paper about oncology services and visiting a hospital webpage about oncology services would not collect PHI because it does not relate to the user's health, health care, or payment for health care. On the other hand, if the user was researching oncology options for a second opinion, the information collected and transmitted would be PHI to the extent that it is identifiable and related to the user's health or future health care.

- An individual's email address or reason for seeking health care where the individual visits an unauthenticated site and makes an appointment or enters symptoms in a tool for a health analysis would constitute PHI because the information collected is IIHI and relates to past, present, or future health care.

The examples illustrate how the guidance places HIPAA-regulated entities in the position of having their obligations with respect to the information collected on unauthenticated pages turn on the intent and purpose of the user's visit. A HIPAA-regulated entity cannot know whether an individual is visiting an unauthenticated website to research oncology services for a paper or to obtain information for the individual's own health care.

The updated guidance also suggests that HIPAA-regulated entities may choose to work with Customer Data Platform vendors (CDPs) to de-identify online tracking information before disclosing the information to the tracking technology vendor. The updated guidance also states that CDP arrangements require the use of a business associate agreement with the CDP and that if a vendor will not enter into a business associate agreement then authorization is required from the users.

The updated guidance concludes with a statement that OCR is prioritizing compliance with the Security Rule in its investigations of tracking technology uses. Accordingly, HIPAA-regulated entities should continue to investigate and analyze their use of tracking technologies with legal counsel. HIPAA-regulated entities that have not started this process should not wait. Questions about tracking technology use are becoming common place in diligence and increasingly frequent in seller representations and warranties. Further, the use of tracking technologies can easily be gleaned by plaintiffs' counsel, regulators, and other interested parties. Through the updated guidance, the OCR has made it clear that enforcement remains a top priority.

---

[1] U.S. Dep't of Health and Human Servs. Office for Civil Rights, *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.
[2] The FTC and OCR sent a joint letter to approximately 130 hospitals and telehealth providers. *See* Model Letter: Use of Online Tracking Technologies, https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.
[3] *American Hosp. Ass'n v. Rainer,* Case No. 4:23-cv-011110-P (compl. filed Nov. 2, 2023 N.D. Tex.).
[4] U.S. Dep't of Health and Human Servs. Office for Civil Rights, *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.