Privacy Alert

April 2024

OCR Issues Updated Guidance on Use of Online Tracking Technologies

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) issued updated guidance on the use of online tracking technologies by HIPAA-covered entities and business associates.

Here are some of the key aspects of the updated guidance:

Key Definitions

- Tracking technology—defined by the OCR as "a script or code on a website or mobile app used to gather information about users or their actions as they interact with a website or mobile app."
- Individually identifiable health information (IIHI)—a subset of health information, including demographic information collected from an individual, that is created or received by a covered entity (or its business associate) or employer; relates to the past, present or future health, health care or payment for health care of an individual; and identifies the individual (or there is a reasonable basis to believe the information can be used to identify the individual). When tracking technology collects IIHI, it will be considered protected health information (PHI).

Key Takeaways

1. The OCR views IIHI collected through tracking technologies on a regulated entity's mobile app or website as PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI does not include specific treatment or billing information like dates and types of health care services. The OCR notes that tying an IP address or device ID to a webpage addressing specific health conditions or listing health care providers is not a sufficient combination of information to constitute IIHI if the visit to the webpage is not related to an individual's past, present or future health, health care or payment for health care. Whether the information collected from a tracking technology is PHI depends in part on the intent of the individual visiting the site (based on one example, tracking technologies on an unauthenticated page of a hospital website that outlines health care services may be collecting PHI if the website visitor is looking for a health care provider but wouldn't be collecting PHI if the visitor is a student doing research). What the OCR overlooks, however, is that neither the hospital nor the tracking technology vendor will know the difference. Most tracking technologies aren't able to discern why someone has come to a website. Instead, they generate inferences from the visit. While vendors can control how they generate or label inferences, they can't control or discern the reason for a visit in each case. Companies will need to evaluate their risk based on the data collected, not the potential intent of the visitor, unless their website is structured in a way that makes it clear.

Attorney Advertising

2. The OCR views tracking technology vendors as business associates if they create, receive, maintain or transmit PHI on behalf of a regulated entity, which means they expect these companies to sign a business associate agreement (BAA), and HIPAA's Privacy Rule will apply. For example, if a tracking technology vendor receives information about a medical appointment tied to an IP address, it will be a business associate. A BAA is required or the regulated entity must get HIPAA authorization, which can't be obtained through a website banner. It is insufficient for a tracking technology vendor itself to de-identify PHI (in lieu of authorization or a BAA). The OCR does state, however, that an intermediary can be used to de-identify data before it is shared with the tracking technology provider; it's unclear how that will work from a technology perspective. **Practice point:** Consider how to configure these tools so that this information is not collected unless that is the purpose of the service being provided.
3. The OCR also clarifies that signing an agreement with BAA-like restrictions will not make a company a business associate (like the controller/processor distinction—you are what you are, and the contract doesn't change that).
4. The OCR distinguishes between authenticated and unauthenticated webpages, noting that many unauthenticated webpages do not have access to information that relates to any individual's past, present or future health, health care or payment for health care. It is the responsibility of the regulated entity to determine whether the tracking technologies on its website or mobile app collect PHI. However, the examples provided again stray from reality. Consider the example of the student writing a term paper, who visits a hospital's webpage listing its oncology services, in contrast to an individual visiting that same webpage seeking a second opinion on treatment options. The collection of IP address and webpage information is not PHI for the student but is for the patient. The challenge is that neither the hospital nor the tracking technology vendor would know the difference between the two. Unless an entity divides its site into sections for patients seeking care and everyone else, it will have to treat its website visitors as patients or face the inadvertent disclosure of PHI.
5. The same rules apply for mobile apps, but the OCR reiterates that HIPAA rules do not protect information on mobile apps that are not developed or offered by a regulated entity, even if the individual is providing information from their own medical records. (Heart rate trackers, fitness and weight-loss apps, period apps, etc., fall in this bucket.)

What Does This Mean?

Bottom line: This is an enforcement priority for the OCR. The best time to look at this was a few years ago, but the next-best time is now. Both sides (vendors and regulated entities) need to understand what information is being collected by tracking technologies and whether it is covered by HIPAA, and then act based on that analysis. Companies that fall outside of HIPAA aren't off the hook—the Federal Trade Commission (FTC) is also watching this area closely.

What should you do now? The OCR's guidance provides the following next steps:

- **Audit your website.** Determine what trackers are on the site and what information they are collecting. If that information could be PHI, the HIPAA rules will apply and you will need a BAA with that vendor. Note a privacy policy disclosure is not sufficient. You cannot disclose your way out of HIPAA obligations.
- **Determine whether BAAs should be in place.** If there is no BAA or no grounds for disclosure under HIPAA (because the disclosure is tied to payment or treatment), you must obtain HIPAA authorization. Website banners are not sufficient.
    - Notably, the OCR states that it is "insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place and requires that there is an applicable Privacy Rule permission for disclosure."
    - Also notable, the OCR clarifies that signing an agreement containing elements of a BAA does not make a tracking technology provider a business associate. This is important for

companies that feel they fall outside of this definition but are being forced to sign a BAA by their partners. An agreement that meets the BAA requirements but does not state that the vendor is a business associate may give both sides comfort (like the controller/processor distinction—you are what you are, the contract won't change that).

- **Consider de-identification.** While the OCR states that de-identification by the tracking technology vendor is insufficient, if a tracking technology vendor will not sign a BAA, the regulated entity can establish a BAA with a third party that will enter into a BAA with the regulated entity to de-identify online tracking information that includes PHI and subsequently disclose the de-identified information to tracking technology vendors that are unwilling to sign the BAA.
- **Include tracking technologies in your HIPAA risk assessments and analysis.** The information shared with these vendors should be considered when designing the administrative, physical and technical safeguards required by the Security Rule (and may require encrypting ePHI that is transmitted to the tracking technology vendor, and enabling and using appropriate authentication, access, encryption and audit controls when accessing ePHI maintained in the tracking technology vendor's infrastructure). Vendors should expect to have to demonstrate the security measures they have in place.
- **Remember that failure to comply may be a breach.** There is a presumption that when PHI is disclosed to a tracking technology vendor without a BAA, or there is no Privacy Rule permission or requirement to disclose, there has been a breach that must be reported unless the entity can demonstrate that there is a low probability that the PHI has been compromised.

Related Professional

Jessica B. Lee . . . . . jblee@loeb.com