AMERICAN HEALTH LAW ASSOCIATION

April 06, 2023

OCR Guidance on Online Tracking Technologies

This Briefing is brought to you by AHLA's Health Information and Technology Practice Group.

April 06, 2023

Carolyn V. Metnick, McDermott Will & Emery LLP | **Ashley O. Ogedegbe**, McDermott Will & Emery LLP

On December 1, 2022, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) issued a bulletin on the use of online tracking technologies by covered entities and business associates subject to the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA).[1] The bulletin underscores that HIPAA regulated entities are not permitted to leverage tracking technologies in a manner that would result in an impermissible disclosure or any other violation of HIPAA. But most notably, OCR adopts an expansive interpretation of the definition of protected health information (PHI) under HIPAA that will impact how regulated entities interact with users accessing their webpages and mobile applications.

Definition of Individually Identifiable Health Information

HIPAA generally defines PHI as individually identifiable health information (IIHI). IIHI is "information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates 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 (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."[2]

The definition of IIHI includes information that relates to future health care services or payment for such services and has remained unchanged since 2003. In the bulletin, however, OCR states that "[a]ll such IIHI collected on a regulated entity's website or mobile app generally is [PHI], *even if the*

individual does not have an existing relationship with the regulated entity and even if the IIHI, such as an IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services."[3] While OCR distinguishes between the collection of data on authenticated and unauthenticated websites (acknowledging that there may be situations where information collected on unauthenticated sites is not PHI), it asserts that the information collected qualifies as PHI because it "is indicative that the individual has received or will receive health care services or benefits" from the regulated entity.[4] The bulletin does not clearly exempt tracking technology scenarios where individuals use a regulated entity's website or mobile application without intending to seek future health care services or without having been a past patient of a regulated entity. Instead, OCR appears to take an expansive interpretation of IIHI and argue that nearly all information collected through tracking technologies will be PHI when the website or mobile application belongs to a regulated entity. This view seems to ignore that individuals may access a regulated entity's website with no intention of seeking care, e.g., attorneys or third-party consultants may review websites as part of due diligence or when confirming clients have posted necessary disclaimers or privacy notices.

Fundamentals of Tracking Technologies

A tracking technology is a script or code used to collect information about a user's interaction with a website or mobile application. The information is then analyzed to learn about a user's online presence. Websites commonly use third-party tracking technologies such as cookies, web beacons or pixels, and scripts. Cookies are small text files used by web servers and websites that can customize an individual's browsing experience but can also be used to collect data about that individual. Pixels (also called web beacons) are small image files that permit website owners to collect information from an individual when an individual opens an email or visits a website. Session replay scripts record how a user interacts with the website or app (e.g., mouse movements and typing). Mobile applications generally embed tracking codes and technologies into the algorithm of the application itself. For example, the application may collect a user's unique mobile device identification number, which is unique to each individual.

While some companies use their own tracking technologies, the bulletin primarily addresses the use of third-party tracking technologies. Through tracking technologies, regulated entities can collect a variety of IIHI, which may include an individual's IP address or geographic location. As discussed above, OCR states that all IIHI collected on a regulated entity's website or application is generally considered to be PHI, even if the individual does not have an existing relationship with the regulated entity. That is, OCR assumes that when an individual accesses a regulated entity's website or mobile application, the individual has received or will receive health care services from the covered entity, and therefore, such access relates to past, present, or future health care or payment.

Tracking on Unauthenticated and Authenticated Webpages

The bulletin distinguishes between the safeguards required when regulated entities use tracking technologies on user-authenticated webpages versus unauthenticated webpages. Unauthenticated webpages do not require users to enter login credentials to access the webpage. An example of an unauthenticated webpage includes a webpage that lists the locations for a medical practice or the mission statement of a regulated entity. Authenticated webpages require users to enter login

credentials. Patient portals and telehealth portals where patients can access their medical records are examples of authenticated webpages. OCR notes that user-authenticated webpages that are operated or developed by regulated entities generally have access to PHI due to the assumed past or future relationship between the user and regulated entity. Therefore, a regulated entity must ensure that such technologies only use and disclose PHI in accordance with HIPAA. OCR further provides that third-party tracking technology vendors are business associates when creating, receiving, maintaining, or transmitting PHI on behalf of a regulated entity. Therefore, if a tracking technology collects PHI (which may include an IP address) about a data subject through an authenticated webpage, the regulated entity should have a business associate agreement in place with the third party providing tracking technology services or data analytics.

OCR notes that while tracking technologies on unauthenticated websites do not typically have access to PHI, there are situations where they may. For example, when an individual enters login credentials on a regulated entity's patient portal page, the information entered by the individual is PHI and protected by HIPAA. The bulletin also clarifies that when individuals search for or schedule appointments with available health care providers, any identifying information collected in connection with the individual will be PHI. Ultimately, the bulletin makes it clear that in any situation where an individual accesses a regulated entity's website or mobile application, the regulated entity should tread carefully in its consideration of deploying tracking technologies since the information will be deemed PHI.

Tracking on Mobile Apps

Similar to authenticated webpages, mobile applications offered by HIPAA-regulated entities collect a wide range of information, including PHI. OCR distinguishes between applications that are not developed by or offered on behalf of regulated entities from those that are. It specifically notes that individuals often enter health-related information for their own use into applications that are developed by non-regulated entities. HIPAA will not apply in such situations. However, when a regulated entity offers or develops a mobile application for users to manage their health information, the information collected by the mobile application is PHI, and the regulated entity must comply with HIPAA.

HIPAA Requirements for Use of Tracking Technologies

OCR provides some important takeaways for regulated entities that deploy tracking technologies with access to PHI:

- Ensure disclosures are permitted by the Privacy Rule—disclosures and uses still need to comply with the Privacy Rule even with a business associate agreement in place and even where data subjects are on notice through a privacy policy;
- Ensure the minimum necessary amount of PHI is used to achieve the intended purpose unless an exception applies—this is an important HIPAA rule that requires covered entities to limit the amount of PHI to that which is necessary to satisfy the purpose of the disclosure or use.
- Ensure business associate agreements are in place with third-party tracking technology vendors that access PHI—agreeing to remove or de-identify PHI before the tracking technology vendor saves the

information is insufficient for HIPAA purposes.
- Factor the use of tracking technologies in a risk analysis and in risk management processes, including implementing safeguards in accordance with the Security Rule to protect electronic PHI used in the tracking technology's infrastructure.

OCR further states that a HIPAA compliant authorization is required before the tracking technology vendor may access PHI if the Privacy Rule does not permit the disclosure or if there is no business associate agreement in place. OCR clarifies that website banners that ask users to accept or reject a use of a tracking technology will not constitute a valid HIPAA authorization.

OCR also provides guidance on business associate arrangements, specifically noting that arrangements need to be analyzed to ensure they constitute business associate arrangements. The sole act of signing a business associate agreement does not create or validate a business associate or arrangement. Further, the bulletin reminds regulated entities that business associate agreements, at a minimum, must specify permitted and required uses of PHI, provide for safeguards, and require the reporting of security incidents and breaches to the regulated entity.

Breach Notification

The bulletin calls for regulated entities to notify data subjects (and the Secretary of HHS or media, where applicable) of improper disclosures to a tracking technology company that compromises the security or privacy of the PHI where there has not been a business associate agreement in place. OCR notes that there is a presumption that there has been a breach of unsecured PHI unless an entity can demonstrate a low probability of compromise.

A HIPAA breach risk assessment includes consideration of at least the following factors: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to PHI has been mitigated. [5]

Regulated entities should consider whether they need to notify data subjects and other entities as appropriate of situations where they have used a third-party tracking technology without having a business associate agreement in place. In conducting a HIPAA breach risk assessment, regulated entities should consider the sensitivity of the information (i.e., is it medical or is it demographic), whether the third-party tracking vendor is considered low or high risk in connection with safeguarding data and complying with HIPAA, and whether the collected information is deemed PHI under HIPAA.

Practical Business Practices for Regulated Entities to Ensure Compliance

Some may argue that the bulletin exacerbates preexisting challenges for regulated entities to comply with HIPAA, such as negotiating with third-party vendors who may be reluctant to or refuse to sign business associate agreements. Further, regulated entities, and smaller and/or less knowledgeable ones in particular, may not understand the data flow and relationships with tracking technology vendors, which is critical for describing the use and disclosure of PHI and obtaining appropriate authorization

from individuals. Also, many regulated entities may not have the resources to develop their own tracking technology to replace the third-party vendors who will not sign business associate agreements.

Although the bulletin takes an expansive interpretation of what information is considered PHI, regulated entities can begin implementing practical steps to ensure compliance under HIPAA:

- Evaluate current and future relationships with third-party tracking technology vendors to determine what information is collected, disclosed, and used through the tracking technologies and which information, if any, constitutes PHI;
- Ensure that any disclosures of PHI are the minimum necessary as permitted under HIPAA;
- Ensure that business associate agreements are in place with all third-party tracking technology vendors;
- In addition to updating privacy policies, obtain any necessary HIPAA-compliant authorizations prior to disclosing PHI to third parties;
- Implement appropriate security safeguards to secure any PHI collected, used, or disclosed in connection with the regulated entity's website or mobile application.

---

[1] 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).

[2] 45 C.F.R. § 160.103.

[3] OCR Dec. 2022 Bulletin (emphasis added).

[4] *Id.*

[5] 45 C.F.R. § 164.402.

ARTICLE TAGS

Health Information and Technology Practice Group Health Information

1099 14th Street NW, Suite 925, Washington, DC 20005 | P. 202-833-1100
For payments, please mail to P.O. Box 79340, Baltimore, MD 21279-0340