Now & Next
Healthcare Alert

March 20, 2024

OCR updates guidance on the risks of using online tracking technologies

By Valerie Breslin Montague and Laurie T. Cohen[1]

The guidance clarifies compliant use of online tracking technologies by HIPAA-regulated entities but reiterates OCR's broad interpretation of what is considered PHI.

What's the impact?

- Faced with widespread industry criticism and AHA legal action, OCR attempted to clarify prior guidance related to the scope of HIPAA-regulated information.
- The updated guidance does not, however, provide a HIPAA-regulated entity with a workable solution to identify when users' interactions with the entity's website or app result in the provision of PHI.
- The updated guidance reminds health plans, healthcare providers, and other HIPAA-regulated entities to evaluate how their organizations capture and share data through tracking technologies.

[1] Grace Connelly, a legal intern in Nixon Peabody's Healthcare practice and a 2024 J.D. candidate at Loyola University Chicago School of Law, assisted with the preparation of this alert.

On March 18, 2024, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) updated its guidance regarding the use of online tracking technologies by Health Insurance Portability and Accountability Act (HIPAA) covered entities and business associates. OCR's previous guidance, issued in December 2022, advised HIPAA-regulated entities not to share protected health information (PHI) with vendors of online tracking technologies, taking the expansive view that Internet protocol (IP) addresses and other information provided by their website (following user login) or mobile application (mobile app) users "generally is PHI," even if the individual is not a patient of the organization. In November 2023, the American Hospital Association (AHA), supported by several health systems and state hospital associations, filed a lawsuit against HHS to bar enforcement of its tracking technologies guidance, arguing that the guidance seeks to regulate more than PHI.

As we previously described, online tracking technologies are of concern for HIPAA-regulated organizations because these technologies could collect and disclose PHI to third-party tracking technology vendors. Often, the tracking technology vendors are not business associates of the HIPAA-regulated entities, and even if they are business associates, the vendors may collect and share data for marketing purposes, which would require written patient authorization. In addition to reemphasizing the risks of these arrangements, the updated guidance continues to take a broad view of what PHI is in relation to users interacting with the websites and apps of HIPAA-regulated entities.

Clarifications in OCR's updated guidance

In the wake of the AHA lawsuit and other industry pushback, OCR's updated guidance seeks to provide more clarity for HIPAA-regulated organizations regarding the data captured on websites and mobile apps. For entities with user-authenticated websites (those that require a user to log in), OCR states that any associated tracking technology will "generally have access to PHI," referencing an example of an individual making an appointment for clinical care. If this user-authenticated site is using tracking technologies, the website might automatically transmit information regarding the appointment and the individual's IP address to the tracking technologies vendor, which requires a business associate agreement (BAA) or HIPAA-compliant authorization. OCR also views information collected by a HIPAA-regulated entity's mobile app "generally" as PHI.

For entities using unauthenticated websites (those that do not require a user to log in), OCR acknowledges that some identifying information captured by tracking technologies may not be PHI. However, OCR continues to caution that PHI captured on an unauthenticated website triggers HIPAA compliance obligations. OCR describes how the purpose of the user's visit to the entity's website is relevant in determining whether HIPAA applies, providing example scenarios where it applies and where it does not. OCR describes a user's visit to a webpage providing visiting hour information, clarifying that information captured on the user related to that interaction would not be deemed PHI. The guidance also discusses two scenarios involving users

interacting with a site's oncology services information. In the first example, OCR describes a student using a hospital website to research a term paper, stating that the data captured on the student in this scenario would not be PHI, even if it could be used to identify the student. However, if an individual visits a hospital's website to research its oncology services when seeking a second opinion on treatment options for a brain tumor, OCR explains that the individual's IP address, location, or other identifying information would constitute PHI to the extent it is related to the individual's health or healthcare. It is unclear how a HIPAA-regulated entity would determine, from available data, whether visits to its site were made by a student for educational purposes or by a patient seeking treatment.

What is the impact?

While OCR outlines certain scenarios describing when user website activity falls outside of the transmission of PHI based on the purpose of the user's interaction with the site, it ignores the fact that the majority, if not all, HIPAA-regulated entities do not have the means to determine a user's intent in navigating their websites. Healthcare providers, health plans, and HIPAA business associates remain subject to OCR's broad interpretation of PHI related to a user navigating their websites absent a concrete way to capture and document the user's intent. HIPAA-regulated entities must continue to evaluate existing and any new uses of tracking technologies to confirm that PHI disclosures comply with HIPAA. Disclosures to tracking technology vendors that fall outside HIPAA compliance should be analyzed as potential breaches.

OCR's guidance describes its intent to prioritize HIPAA Security Rule compliance when investigating tracking technology issues. In this regard, a HIPAA-regulated entity needs to ensure that its website teams are trained and clearly understand the privacy and security requirements governing the entity's use of tracking technologies. In addition to executing BAAs with the tracking technology vendors (to the extent they are willing to do so) or seeking patient authorization for the transfer of PHI to a tracking technology vendor (which may not be practical), the guidance suggests that HIPAA-regulated entities engage a vendor/business associate to de-identify data before it is transmitted to a tracking technology vendor. HIPAA-regulated entities should explore all avenues that allow for the compliant use of tracking technologies with their vendors if they continue to use these tools.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Valerie Breslin Montague
312.977.4485
vbmontague@nixonpeabody.com

Laurie T. Cohen
518.427.2708
lauriecohen@nixonpeabody.com

Lindsay Maleson
516.832.7627
lmaleson@nixonpeabody.com

Rebecca Simone
516.832.7524
rsimone@nixonpeabody.com