Now & Next
Healthcare Alert

July 3, 2024

Portions of OCR's bulletin on online tracking technologies deemed unlawful

By Julia E. Cassidy, Laurie T. Cohen, Valerie Breslin Montague, and Rebecca Simone

This new Texas federal court ruling limits OCR's guidance, but HIPAA regulated entities should continue to take care when using pixels and cookies.

What's the impact?

- OCR's guidance, widely viewed by the industry as overly-broad, is slightly narrowed in scope.
- Risks continue for HIPAA covered entities and business associates transmitting data to tracking technology vendors.
- HIPAA regulated entities should carefully analyze their use of tracking technologies on websites, portals, and apps.

On June 20, 2024, the US District Court for the Northern District of Texas ruled that key portions of the bulletin issued by the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR) regarding the use of online tracking technologies by Health Insurance Portability and Accountability Act (HIPAA) covered entities and business associates were unlawful. The court's ruling held that HHS exceeded its statutory authority with respect to certain aspects of

the bulletin and granted, in part, the request that the bulletin be vacated. The new ruling creates uncertainties around the use of tracking technologies and the enforcement of various aspects of OCR's bulletin which are still in effect.

History of OCR guidance

OCR issued a bulletin on December 1, 2022, which addressed the obligations of covered entities and business associates under HIPAA when using online tracking technologies, such as cookies and pixels, on their websites, patient portals, or mobile applications (apps). OCR expressed the view that information captured on a HIPAA regulated entity's website, portal, or app by a tracking technology and subsequently disclosed to a third-party tracking technology vendor may be an impermissible disclosure of protected health information (PHI). Subsequently, on July 20, 2023, OCR and the Federal Trade Commission (FTC) jointly issued a letter to approximately 130 hospitals and telehealth providers informing them that online tracking technologies may be operating on their websites or mobile apps and collecting health information in violation of HIPAA.

Following issuance of OCR's bulletin and letter from OCR and the FTC, in November 2023, the American Hospital Association (AHA), the Texas Hospital Association, and two Texas-based health systems filed a lawsuit against HHS to challenge enforcement of the bulletin and to obtain a declaratory judgment that IP addresses are not individually identifiable information under HIPAA. Both parties moved for summary judgment.

On March 18, 2024, OCR issued an updated bulletin which sought to provide more clarity for HIPAA regulated organizations regarding the data captured on websites and mobile apps. OCR provided several example situations to demonstrate the scenarios in which HIPAA would apply and those in which it would not apply. One such example is that of an individual looking at a hospital's webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor. In this scenario, OCR stated that "the collection and transmission of the individual's IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual's health or future health care." However, this scenario would require the hospital to determine the reason for an individual visiting the website, which is not information readily available to the hospital.

OCR said in public court filings that it believed it could revise the bulletin in such a way so as to render further litigation unnecessary. However, the lawsuit continued.

American Hospital Association et al. v. Becerra et al.

On June 24, 2024, the Texas federal court issued a ruling in response to both parties' motions for summary judgment. AHA argued that HHS had exceeded its statutory authority in issuing the

bulletin and sought to enjoin HHS from enforcing it, while HHS argued that it had not exceeded its statutory authority in issuing the bulletin. Ultimately, the court denied HHS' motion and granted in part and denied in part AHA's motion.

The court stated that OCR's bulletin provided several examples of actions that would trigger obligations under HIPAA as a result of a covered entity collecting individually identifiable health information (IIHI) such as "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to an [unauthenticated public webpage] addressing specific health conditions or healthcare providers." In the bulletin, OCR stated that this circumstance involving the combination of an individual's IP address coupled with a visit to an unauthenticated public website (i.e., the individual had not logged in) addressing specific health conditions or healthcare providers would constitute IIHI under HIPAA. The court referred to this combination of data as a "Proscribed Combination." The court noted that the Proscribed Combination "does not and cannot identify an individual's PHI without an unknowable subjective-intent element" and viewed the bulletin's reliance on the intent of an individual to visit a website as a determining factor in whether identifying information about an individual is IIHI. The court stated that it was impermissible to require a HIPAA regulated entity to determine an individual's motivation for visiting a particular website. HHS had argued that, while the Proscribed Combination does not necessarily identify the individual and their condition, the information can become IIHI if it provides a "reasonable basis" to believe the information can be used to identify the individual. The court noted that while HHS should be afforded deference in determining what is reasonable in most circumstances, citing the *Chevron, USA, Inc. v. Natural Resources Defense Council, Inc.* case, they stated that even the "reasonable basis" language could not save the Proscribed Combination. In addition, in the intervening time since the Texas federal court issued its opinion, the US Supreme Court overruled the *Chevron* framework and the deference it provided to an agency's interpretation of a statute.

Ultimately, the court held that the Proscribed Combination is unlawful and that OCR exceeded its authority under HIPAA. However, the court declined to grant AHA's request to enjoin OCR's enforcement of the bulletin, and instead vacated the Proscribed Combination from the bulletin.

Next steps for HIPAA regulated entities

While the court's ruling affects the application of OCR's bulletin to visits to certain unauthenticated websites of HIPAA regulated entities, many other aspects of the bulletin remain as subregulatory guidance from OCR. The Proscribed Combination only addresses a specific circumstance under which the potentially identifiable information is an IP address and an individual visits an unauthenticated public webpage that addresses health conditions or healthcare providers. It is unclear whether the bulletin would apply to an unauthenticated website if tracking technologies collect other identifiers of an individual instead of or in combination with an IP address (such as geographic location or email address). Questions also

remain as to whether OCR will enforce the aspects of the bulletin which are still in effect or reissue the bulletin with changes consistent with the court's ruling.

Given the many uncertainties following the Texas federal court ruling, entities that are regulated by HIPAA should continue to closely evaluate their use of online tracking technologies. As many organizations have reported PHI breaches to OCR involving tracking technologies, and as the FTC also has issued enforcement actions against companies utilizing tracking technologies to disclose consumer information, this issue is becoming a key enforcement consideration for both federal agencies. Organizations should have a clear understanding of what information is captured by cookies, pixels, and other similar technologies and, importantly, what information, if any, is disclosed to the third-party vendors. HIPAA regulated entities should analyze whether any such disclosures rise to the level of a reportable breach of PHI.

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

Julia E. Cassidy
212.940.3137
jcassidy@nixonpeabody.com

Laurie T. Cohen
518.427.2708
lauriecohen@nixonpeabody.com

Valerie Breslin Montague
312.977.4485
vbmontague@nixonpeabody.com

Rebecca Simone
516.832.7524
rsimone@nixonpeabody.com