KRIEG DEVAULT

Insights

Lawsuit Challenges HHS Guidance on the Use of Web Tracking Technologies

November 29, 2023

By: Stephanie T. Eckerle and Christopher J. Kulik

On November 2, 2023, parties including the American Hospital Association ("AHA") sued the U.S. Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") in a federal court in Texas. In their complaint they challenge the enforcement of an OCR guidance bulletin (the, "Bulletin"), dated December 1, 2022, which addresses the applicability of HIPAA to the use of website tracking technologies. The AHA asks the court to bar enforcement of the Bulletin, among other things. The litigation is important to healthcare providers because the use of website tracking technologies provides useful data about how individuals interact with provider websites.

OCR has made web trackers used by healthcare providers an enforcement priority. As recently as this past July, OCR and the Federal Trade Commission sent joint warning letters to hospitals and telehealth providers cautioning them that their use of web trackers – such as Google Analytics and Meta Pixel – may violate HIPAA. OCR asserted that "these tracking technologies gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users." Additionally, there has been a wave of data privacy class action lawsuits related to the use of web tracking technologies.

Tracking Technologies

Website trackers involve the use of machine-readable script or code imbedded in the pages of a website. When a user opens a webpage or interacts with the page in any way, the tracker provides data to an entity (in the case of Meta Pixel, for example, Facebook) ("Tracking Technology Vendor") along with the IP address of the user. The Tracking Technology Vendor compiles the data and provides it to the owner of the website to provide useful insights into consumer behavior with respect to the webpage. In the case of a patient accessing a patient portal, a website tracker may track and transmit to the Tracking Technology Vendor the fact that the patient has opened the portal. However, it may also transmit the patient's health information on the page the user accessed to the Tracking Technology Vendor as well. Since the data being transmitted back to the Tracking Technology Vendor includes the patient's IP address, OCR has taken the position that it is not "de-identified" for purposes of HIPAA. In the case of Google serving as the Tracking Technology Vendor, it automatically pairs up a user's identity with the information obtained by the website tracker for users who are signed into a Google account.

Many entities rely on website tracking tools to measure data such as traffic to, and user interface with, their websites. HIPAA-regulated entities analyze interactions and activities on their websites to help improve a patient's care and experience by quantifying what topics and services garner the most attention. Unfortunately, Tracking Technology Vendors do not consider themselves to be business associates for purposes of HIPAA and likely would not agree to enter into a business associate agreement with a covered entity.

What does the Bulletin Cover?

The Bulletin highlights the obligations of HIPAA covered entities and business associates with respect to the use of tracking technologies on user-authenticated webpages, unauthenticated webpages, and mobile applications. Notably, the Bulletin provides that covered entities may not impermissibly disclose protected health information to Tracking Technology Vendors or use tracking technologies in a way that leads to impermissible disclosures of PHI.

According to OCR, such an impermissible disclosure could occur, for example, when the Meta Pixel tracking tool sends information back to Facebook that a particular user with a particular IP address has accessed a webpage with laboratory results and transmits all of the data on the page to Facebook.

What's the Issue Then?

Health care providers have been pressed to evaluate their use of web trackers given the broad guidance issued in the Bulletin concerning what constitutes individually identifiable health information ("IIHI"). The Bulletin specifies that IIHI collected on a covered entity's website is generally PHI, even if the individual visiting the website does not have an existing relationship with the covered entity and the IIHI (e.g., an IP address) lacks detailed treatment or billing information. OCR's position is that when a covered entity collects an individual's IIHI using its website, the information connects the individual to the covered entity, reflects that the individual has received (or will receive) health services or benefits from the covered entity and, therefore, relates to the individual's past, present, or future health care or payment for care.

The AMA and its co-plaintiffs allege that the Bulletin is flawed and that it was improperly implemented. The complaint focuses on the "Proscribed Combination," which refers to the Bulletin's position that when an online technology connects an individual's IP address with a visit to an unauthenticated webpage (i.e., one that does not require a user to log-in) containing health conditions or health care providers, that such combination is subject to HIPAA use and disclosure restrictions. Specifically, the complaint asserts that the Bulletin's rule that the Proscribed Combination constitutes IIHI exceeds HHS's authority under HIPAA. The complaint also details concerns over OCR's alleged circumvention of the administrative notice and comment rulemaking process.

The end result may be that healthcare providers may need to forego website tracking technology on certain pages within their websites that display sensitive, protected information. The technology behind website tracking tools is sophisticated and complex. Providers will likely need to consult their webmasters, IT experts, and attorneys to achieve an acceptable balance between data-based website feedback and patient privacy compliance. Providers utilizing web trackers should also review and audit their websites for compliance as part of their annual risk analysis and conduct a risk assessment following a potential breach of PHI through the use of web trackers.

For questions regarding your compliance efforts, please contact Stephanie T. Eckerle, Christopher J. Kulik, or your regular Krieg DeVault health care attorney.

Disclaimer: The contents of this article should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult with counsel concerning your situation and specific legal questions you may have.