AHA Files Lawsuit Against HHS for Guidance Restricting Third-Party Trackers

NOVEMBER 21, 2023

On November 2, 2023, the American Hospital Association (AHA) – alongside the Texas Hospital Association, Texas Health Resources, and United Regional Health Care System – brought a lawsuit against the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) to block enforcement of its December 2022 bulletin (the "Bulletin"), which provided OCR's interpretation of how the Health Insurance Portability and Accountability Act (HIPAA) applied to covered entities' and business associates' use of tracking pixels on websites and mobile apps.

In the Bulletin, OCR emphasized that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules." The agency gave examples of the types of activities that may violate HIPAA, including the potential use of trackers on unauthenticated webpages (i.e., webpages where a regulated entity may not know who the person accessing the website is, including if they are a patient or not). After releasing the Bulletin, OCR (in conjunction with the Federal Trade Commission (FTC)) sent letters to approximately 130 hospital systems and telehealth providers encouraging them to review and take actions in light of the Bulletin.

Through its lawsuit, AHA is challenging OCR's interpretation of HIPAA as it applies to trackers and the potential implication of its broad interpretation on the healthcare industry. According to AHA, the vast majority of hospitals and health care organizations use tracking technologies on their websites, and the complaint highlights some of the ways that trackers are used to improve users' experience. For example, the complaint notes that website data analytics might tell a hospital how many IP addresses looked for information on a certain vaccine in a particular area, which would help hospitals better distribute resources. Videos embedded on healthcare organizations' websites can offer various types of information to the public, such as providing virtual tours of hospital facilities. Translation-technologies help limited-English proficiency patients access and understand healthcare information on hospitals' websites. Location technologies could help provide transportation information to community members. AHA's complaint also asserts that third-party analytics and advertising tools are present on various federal agency website pages addressing specific health conditions and healthcare providers. Examples provided in the complaint include certain of the Veterans Health Administration's, Medicare's, and Department of Defense's Military Health System's webpages.

If successful, AHA's lawsuit would mitigate the compliance risk associated with HIPAA-regulated entities using advertising trackers on their websites and mobile devices (both for the aforementioned purposes and others), as it would mean that the use of trackers by HIPAA-regulated entities in some contexts (such as with regard to unauthenticated users) would fall outside the scope of HIPAA. This does not mean, however, that there will not be other challenges that healthcare entities will have to pay attention to if they rely on trackers and similar technologies. Along with HHS, the FTC has also been paying close attention to the use of advertising trackers and the sharing of sensitive health information with advertising networks. The FTC may look to fill any gap to OCR's enforcement authority (and it is clear, from their joint letter, that the two agencies are coordinating on this issue). Additionally, state comprehensive privacy laws (such as the California Consumer Privacy Act) and new consumer health privacy laws (such as Washington's My Health My Data Act) are also going to be relevant for the processing of health data and, specifically, the disclosure of health data to advertisers. Healthcare entities that rely on tracking technologies should pay attention to AHA's lawsuit but also account for these other regulatory requirements that may apply to them.

We have provided a summary of the Bulletin and AHA's complaint below. We will continue to keep you updated on notable HIPAA developments through the WilmerHale Privacy and Cybersecurity Blog.

The Bulletin

The Bulletin notes that the unauthorized use of third-party tracking technologies could be a violation of the HIPAA Privacy, Security, and Breach Notification Rules (the "HIPAA Rules") and that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules." The Bulletin states that notice of third-party tracking in a regulated entity's privacy policy or terms and conditions is not sufficient and such notice does not allow impermissible data disclosure to third parties.

Notably, the Bulletin covers both user-authenticated and unauthenticated pages. User-authenticated pages require users to log-in before they can access the webpage. The Bulletin notes that tracking technologies on user-authenticated pages usually have access to PHI including users' IP addresses, medical record numbers, dates of appointments, and even sensitive treatment, billing, and prescription information within the portal. Thus, the Bulletin mandates that regulated entities must configure their user-authenticated pages that use tracking technologies to only allow the technologies to use, disclose, and collect information in compliance with the HIPAA Privacy and Security Rules.

The Bulletin further adds that tracking technologies on unauthenticated public pages could also sometimes also give third parties access to PHI, in which case HIPAA rules would apply. For instance, if a tracking technology on a regulated entity's unauthenticated public webpage addresses pregnancy or miscarriage, the regulated entity might be disclosing to the tracking technology vendor health information – i.e., pregnancy status – of the user (in combination with their IP address). Thus, according to the bulletin, the HIPAA Rules would apply. The Bulletin's application of the HIPAA Rules to such public unauthenticated webpages is the crux of AHA's complaint.

The Complaint

The allegations in the complaint are centered around HHS' alleged overbroad conception of PHI. Specifically, the complaint alleges that:

- **HHS' position on trackers on unauthenticated public webpages is purportedly broader than the HIPAA Privacy Rule's definition of health data.** The complaint asserts that under the Privacy Rule, protected PHI must be individually identifiable health information (IIHI), which is defined as information that relates to an individual's past, present, or future physical or mental health condition, receipt of healthcare, or payment for healthcare; **and** either identifies the individual or provides a reasonable basis to believe the information could be used to identify the individual. According to the complaint, the OCR maintains through the Bulletin that when an online technology connects (1) an individual's IP address with (2) a visit to an unauthenticated public webpage that addresses specific health conditions or healthcare providers, that combination of information (the "Proscribed Combination") is subject to HIPAA restrictions. However, the complaint alleges this conception does not explain why there would be reasonable basis to believe that the combination of information shared could identify the individual whose health, healthcare, or payment for healthcare relates to the webpage visit. For instance, the complaint contemplates a situation where a website user visits the page but not for their own healthcare— for example, an academic or journalistic researcher or someone visiting a webpage on behalf of a relative or friend.
- **Non-private health information is allegedly protected speech under the First Amendment.** The complaint asserts that the broad definition of IIHI under the Bulletin is a violation of the First Amendment because disseminating non-private health information is protected speech and content-based restrictions on that speech are subject to strict scrutiny. Since the Bulletin prohibits healthcare providers from disclosing information about usage of a public webpage depending on whether the page contains specific health-related content, according to the complaint, this is a content-based restriction would not survive strict scrutiny because it is not narrowly tailored to protect patient's privacy interests.
- **HHS' Bulletin constitutes alleged arbitrary and capricious rulemaking and lack of notice-and-comment rulemaking.** The complaint asserts that because OCR provided no reasoning for its purported expanded definition of IIHI on an unauthenticated public webpage, the Bulletin's rule is arbitrary and capricious. The complaint further alleges that the Bulletin's rule was a legislative rule for which OCR was required to, but did not, undertake notice-and-comment rulemaking under the Administrative Procedure Act.

The plaintiffs make several requests for relief, including that declaratory judgment be entered that IP addresses are not considered IIHI and for permanent injunctive relief enjoining OCR from enforcing the Bulletin's rule.

Authors

Kirk J. Nahra

PARTNER

Co-Chair, Artificial Intelligence Practice

Co-Chair, Cybersecurity and Privacy Practice

kirk.nahra@wilmerhale.com

+1 202 663 6128

Ali A. Jessani

SENIOR ASSOCIATE

ali.jessani@wilmerhale.com

+1 202 663 6105