VOLUME 78 ◆ NUMBER 7

Employee Benefit Plan Review

American Hospital Association v. Becerra: Are Tracking Tools OK Again? Federal Court Dials Back Office for Civil Rights Bulletin

By Paul Bond, Shannon Britton Hartsfield and Beth Neal Pitman

A recent federal court decision is a victory for Health Insurance Portability and Accountability Act (HIPAA) covered entities using third-party tracking tools on unauthenticated webpages. These are websites available to the general public that healthcare providers use to increase the public's access to important health-related information.

Since the final Privacy Rule was issued more than two decades ago, Internet Protocol (IP) address numbers, URLs, device identifiers and "[a]ny other unique identifying number, characteristic, or code" have been among the data elements that must be removed in order for a data set to qualify under the HIPAA de-identification safe harbor. As the final Privacy Rule aged and the digital platforms of healthcare providers expanded, new questions emerged.

For years, a vast majority of healthcare providers offered information to the public on websites. Almost all of these used third-party tools, especially from Google and Facebook (Meta), to better understand how users navigated these public websites, and to support outreach campaigns. Those third-party tools, often involving cookies or pixels, gathered information including IP addresses, URLs and other unique identifying numbers. Did simply visiting a healthcare provider's public website, which included information ranging from provider profiles to public health updates and research to employment and parking directions, really implicate HIPAA? Were third-party tracking providers required to enter into HIPAA business associate agreements?

According to a U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) bulletin issued in December 2022 (2022 Bulletin), it did and they were.

Even though HIPAA has no private right of action, numerous plaintiff class actions were filed charging that such tracking tools violate HIPAA and other privacy laws when they involve transmitting IP addresses of website visitors to third-party vendors. The 2022 Bulletin followed, setting out OCR's position that mobile applications and websites using tracking technologies could lead to HIPAA violations, even on unauthenticated pages requiring no login. The 2022 Bulletin also stated that any information collected about visitors to a public website, even an unauthenticated site, "is indicative that the individual has received or will receive health care services or benefits from the covered entity." Therefore, OCR's original view was that any disclosure of tracking tools

to third parties would require a HIPAA business associate agreement with third-party tracking vendors, or a full HIPAA compliant patient authorization. Following this original guidance, the number of class actions filed against healthcare providers for website cookie and pixel use shot into the hundreds.

Challenge to the Guidance

A number of industry stakeholders became vocal critics of the 2022 Bulletin, particularly with regard to its regulatory overreach. For example, in May 2023, the American Hospital Association (AHA) sent a letter urging OCR to suspend the guidance because it defined protected health information (PHI) too broadly and would impede public access to credible health information that certain websites provide. Instead of softening its position, OCR and the Federal Trade Commission (FTC) sent warning letters in July 2023 to 130 hospitals indicating that they may be using online tracking technologies that involve "serious privacy and security risks."

The AHA, the Texas Hospital Association and other stakeholders teamed up in November 2023 to sue the HHS Secretary and OCR Director in Texas federal court. The plaintiffs argued that the bulletin improperly imposed HIPAA requirements on all uses of tracking technologies, including in cases where a website visitor or app user is not a patient, through an unlawful administrative action.

OCR Response

Likely in response to the lawsuit, approximately four months later, on March 18, 2024, OCR revised its guidance (Revised Bulletin), but maintained that all individually identifiable health information (IHII) "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. . . ."

OCR conceded, however, that "the mere fact that an online tracking technology connects the IP address of a user's device (or other identifying information) with a visit to a website addressing specific health conditions or listing health care providers is not a sufficient combination of information to constitute [IHII] if the visit to the webpage is not related to an individual's past, present, or future health, health care, or payment for health care."

Notably, the Revised Bulletin both expanded the definition of IHII to include a subjective analysis component and provided no assurance that regulated entities could continue to use such tracking tools because there would be no practical way to discern the purpose or intent of a website visitor and whether such visit related to the individual's healthcare.

Court Decision

In a final judgment and strongly worded opinion, *American Hospital Association v. Becerra*,[1] the U.S. District Court for the Northern District of Texas, Fort Worth Division, declared a portion of OCR's Revised Bulletin unlawful and, therefore, vacated. The decision did not affect the remainder of the Revised Bulletin.

The court observed that "unauthenticated public webpages" (UPWs) do not require user verification or login credentials, but are still able to create a "more bespoke user experience" through use of third-party tracking tools and, "[i]n theory, a third party could connect the dots between a person's IP address and the searches performed: if an IP address corresponds to Person A, and Person A looks up the symptoms of Condition B, one might conclude Person A has Condition B."

The court noted that the 2022 Bulletin indicated that HIPAA obligations could be triggered by circumstances similar to those related to a new HHS rule established in the Revised Bulletin which the court described as a "Proscribed Combination." The Proscribed Combination occurred when an "online technology connects (1) an individual's IP address with (2) a visit to a UPW addressing specific health conditions or healthcare provider" and, as the court aptly noted, required the "clairvoyance"" of healthcare providers.

The court acknowledged that OCR changed its position somewhat in the Revised Bulletin, but the Proscribed Combination remained problematic if the individual's reason for visiting a UPW related to their healthcare, even though the covered entity had no way to discern that reason.

The court discussed at length whether it has jurisdiction to review the Revised Bulletin. The opinion stated that "[t]his Court knows a law when it sees one, and the Proscribed Combination is a law. Thus, the Revised Bulletin is a 'final agency action' subject to judicial review."

The court found that the Revised Bulletin requires "covered entities to perform the impossible," because even if the UPW's metadata could identify an individual, the information only became IIHI if the visitor's motive related to that individual's healthcare. The court noted that the "issue is that the Proscribed Combination does not and cannot identify an individual or the individual's PHI without an unknowable subjective-intent element – an element not countenanced by the controlling statutory text."

The court went on to find that HHS lacked statutory authority holding that the "Proscribed Combination is unlawful" and the portion of the Revised Bulletin related to the Proscribed Combination would be vacated. In finding that OCR lacked authority, the court rejected OCR's argument that the guidance was "subject to judicial review" and commented that "even if subsequent enforcement actions would be judicially reviewable, the Hospitals 'need not assume such risks while waiting

for [HHS] to "drop the hammer" in order to have their day in court.'"

The court concluded by noting that "this case isn't really about HIPAA, the Proscribed Combination or the proper nomenclature for PHI in the Digital Age. Rather, this is a case about power. More precisely, it's a case about our nation's limits on executive power." In this situation, what some may perceive as a "small executive overstep" was significant "for covered entities diligently attempting to comply with HIPAA's requirements."

Key Takeaways and Best Practices

HIPAA's rules have not changed, and the use of tracking technology by HIPAA-regulated entities will continue to require compliance oversight. The decision does not immediately end the many class actions brought against healthcare providers regarding website cookie and pixel use. However, the decision should make such suits significantly less attractive to plaintiffs. Following are several best practices for HIPAA-regulated organizations to consider in the light of the court ruling:

- Continue to monitor uses of tracking technologies – especially with respect to patient portals requiring authenticated access – as the remainder of the Revised Bulletin was not vacated;
- Assess privacy policies and HIPAA Notice of Privacy Policies for adequate notice to patients and conformance with operations (i.e., do you do what you say you do?);
- Determine where consents and authorizations may be needed, even on unauthenticated websites; and
- Evaluate the need for business associate agreements with technology vendors that have access to PHI (as defined in the regulation), and conduct contractor diligence regarding its uses of tracking technology.

Note

1. American Hospital Association v. Becerra, No. 4:23-cv-01110-P (N.D. Tex. June 20, 2023).

The authors, attorneys with Holland & Knight LLP, may be contacted at paul.bond@hklaw.com, shannon.hartsfield@hklaw.com and beth.pitman@hklaw.com, respectively.