Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Court Vacates HIPAA Online Tracking Guidance

Insight — June 24, 2024

On June 20, 2024, a Texas federal court vacated the Office for Civil Rights' (OCR's) controversial guidance concerning Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, available here. While providers will welcome the decision, the decision does not allow providers, business associates, or vendors carte blanche license to use or disclose protected health information (PHI) for purposes not permitted by HIPAA.

The OCR Guidance. In the wake of a report and several lawsuits alleging that tracking technologies employed by Meta, Google, and other entities were collecting data in violation of privacy laws, the OCR and Federal Trade Commission issued guidance and warnings to healthcare providers that the use of tracking technologies may violate HIPAA.[1] In 2023, the American Hospital Association and others sued the OCR in Texas federal court challenging the guidance. In March 2024, the OCR updated its guidance slightly in response to the lawsuit.[2] In short, the OCR argued that tracking technologies (*e.g.*, cookies, web beacons, tracking pixels, etc.) regularly collect individually identifiable information, including IP addresses. When the data collected also includes information concerning a patient's past, present, or future healthcare or payment for healthcare, HIPAA is triggered and prohibits covered entities and business associates to use or disclose the individually identifiable health information (IIHI) without the person's authorization unless the use or disclosure is permitted by HIPAA and, in the case of business associates, the business associate agreement. To illustrate its analysis, the OCR included the following examples:

- For example, if a student were writing a term paper on the changes in the availability of oncology services before and after the COVID-19 public health emergency, the collection and transmission of information showing that the student visited a hospital's webpage listing the oncology services provided by the hospital would not constitute a disclosure of PHI, even if the information could be used to identify the student.

- However, if an individual were looking at a hospital's webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, 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.[3]

The problem is that the second example creates an impossible standard

for covered entities and business associates: it potentially subjects covered entities or business associates to HIPAA liability based on the subjective intent of person searching the website, which intent the covered entity or business associate has no way of knowing.

The Court Order Vacating the Guidance. In an entertaining opinion, the Federal District Court for the Northern District of Texas concluded that the OCR exceeded its authority by issuing its guidance.[4] According to the Court, the OCR guidance redefines IIHI protected by HIPAA by suggesting that IIHI is created when "online technology connects (1) an individual's IP address with (2) a visit to a [website] with *the intent* to address *the visitor's* specific health conditions or healthcare providers," which the Court refers to as the "Proscribed Combination."[5] The Court concluded that the OCR exceeded its authority by changing the statutory definition of IIHI. Moreover, "[a] user's intent in visiting a [website] is unknowable. Thus, because HIPAA doesn't mandate clairvoyance, covered entities must act as if … the Proscribed Combination is per se IIHI."[6] The net result is that covered entities would be obligated to chance their practices to comply with the new standard; accordingly, the OCR has imposed new obligations which exceeded the OCR's authority. Rather than enjoining its enforcement, the Court entered an order vacating the guidance.

The Net Effect. It is too early to tell whether the OCR will appeal the District Court's decision. In the meantime, however, providers, their business associates, and vendors who may use tracking technologies must still be cautious. Although an IP address coupled with information that a person visited a website may not be IIHI (aka PHI) as suggested by the vacated guidance, HIPAA will still apply if a person's health information is collected along with individually identifiable data, including information confirming that an individual has a certain condition; sought care on a certain date or location; paid for their care; etc. HIPAA has always applied and continues to apply to such PHI. To use or disclose PHI, the covered entity's use or disclosure must fit within a permissible use or disclosure under HIPAA or the covered entity must obtain the individual's HIPAA-compliant authorization.[7] If a covered entity shares such PHI with a vendor or other entity, the covered entity must usually obtain a business associate agreement (BAA) with the other entity, and the other entity may only use or disclose the PHI consistent with the HIPAA rules applicable to the covered entity and as specifically authorized in the BAA.[8] Neither HIPAA nor the Court's Order allows covered entities or business associates to use or disclose PHI collected through tracking technologies or otherwise for non-permissible purposes under HIPAA. Covered entities and their business associates should continue to review their use of online tracking technologies to ensure any uses and disclosures are for purposes permitted by HIPAA or that they have HIPAA-compliant authorizations from the patient. As General website privacy policies and terms of use are insufficient.

For more information about permissible uses of such data—and the limits of such uses—under HIPAA, see our February 19, 2020 article, Use of PHI for Non-Patient Purposes.

[1] *See, e.g., HHS Office for Civil Rights Issues Bulletin on Requirements*

under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information, https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html, and *FTC-HHS Joint Letter Gets to the Heart of the Risks Tracking Technologies Pose to Personal Health Information*, https://www.ftc.gov/business-guidance/blog/2023/07/ftc-hhs-joint-letter-gets-heart-risks-tracking-technologies-pose-personal-health-information.

[2] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[3] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[4] Opinion & Order (6/20/24) in *American Hosp. Ass'n et al. v. Becerra et al.*, No. 4:23-CV-01110-P, (N.D. Tex. 2023), available at https://hr.cch.com/hld/AHAvBecerra23-cv-0111062023.pdf (hereafter "Order").

[5] Order at p.12, emphasis in original.

[6] Order at p.12-13.

[7] 45 C.F.R. § 164.502.

[8] 45 C.F.R. §§ 164.502(e) and 164.504(e).