Articles + Publications | April 1, 2024

Great Expectations: HIPAA-Regulated Entities Asked to Know Users' Intent on Unauthenticated Webpages

WRITTEN BY

Brent T. Hoard | Emma E. Trivax

On March 18, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued an updated bulletin to "increase clarity for regulated entities and the public" with respect to the use of online tracking technologies by entities subject to HIPAA.

This updated bulletin appears to be in response to a recent lawsuit filed by the American Hospital Association (AHA) and a number of other health organizations[1] regarding OCR's original bulletin from December 2022. The lawsuit specifically challenged OCR's original position regarding the use of tracking technologies as being overly restrictive — particularly for unauthenticated webpages, which are public-facing and can be freely accessed by the public (*i.e.*, no user credentials are required to access the webpage).

But the OCR's latest guidance offers solutions that are, at best, challenging, if not unworkable. In particular, these solutions are based on a regulated entity's evaluation of the intent of each website visitor to determine if tracked data is protected health information (PHI) subject to HIPAA. In this article, we will provide an analysis of the lawsuit, updated bulletin, and then provide five steps you can take to help address potential tracking issues.

Allegations of Unlawfulness in the Original Bulletin. The lawsuit challenges the original bulletin, which restricts hospitals from using third-party web technologies that capture IP addresses on unauthenticated webpages. The lawsuit includes three key challenges to the original bulletin:

1. The guidance is unlawful and harmful because it disrupts hospitals' ability to share health care information, analyze their websites for accessibility, and improve public health.

2. The guidance exposes hospitals to federal enforcement actions and significant civil penalties if they use any third-party technology that captures an IP address during a visit to their websites without proper authorizations in place.

3. Treating the combination of an individual's IP address and a visit to a publicly accessible webpage that includes information about specific health conditions, related services, or health care providers as individually identifiable health information (IIHI) is an incorrect interpretation of IIHI. The AHA suggests that this interpretation is flawed because an individual may visit a webpage not in connection with health care, but for research purposes, for example.

Updated Bulletin Bases PHI Determination on Intent of Public Website Visitors. Seemingly in response to these arguments, the OCR released an updated bulletin that seeks to clarify the definition of IIHI. According to the updated bulletin, the mere connection of an IP address with a visit to an unauthenticated webpage addressing specific health conditions, services, or health care providers does not constitute IIHI ***if the visit is <u>not</u> related to an individual's past, present, or future health, health care, or payment for health care***. Once it is determined that the unauthenticated website visit is related to an individual's past, present, or future health, health care, or payment for health care, and the website is operated by a regulated entity, the IIHI becomes classified as "protected health information" (PHI) and is thus subject to HIPAA protections. The OCR provides the following example:

[I]f 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.[2]

Ultimately, the OCR instead requires regulated entities to make an intent-based determination — whether the user's reason for visiting a webpage relates to health, health care, or payment — about general visitors to a publicly accessible webpage. This may create an unworkable and impractical rule for regulated entities whereby a regulated entity must:

1. Deploy overly restrictive mechanisms on unauthenticated webpages to determine a visitor's intent;

2. Place information about health conditions, services, or health care providers only on authenticated webpages; and/or

3. Treat data from every visitor to an unauthenticated webpage as PHI.

Solutions for Unauthenticated Webpages, Tracking Technologies, and Third Parties. In light of the issues discussed in the prior section, what approach should a regulated entity take with its third-party tracking technology vendors? The OCR suggests two potential solutions for how to share PHI with third-party tracking vendors.

- **Solution 1.** *Establish a business associate agreement (BAA) with each third-party tracking technology vendor, assuming the vendors collect and use the PHI on behalf of the regulated entity for purposes permitted under HIPAA*. This solution seems feasible initially. However, the OCR cautions against entering BAAs with vendors that may not actually be using PHI for HIPAA-permitted purposes. Therefore, regulated entities must ensure these vendors operate under an applicable provision; otherwise, the BAA would not be valid, and the exchange of PHI would not be authorized.

- **Solution 2.** *Obtain individual authorization from every patient whose PHI is shared on an unauthenticated website before it is shared with the vendor.* This approach is impractical (if not impossible), especially considering the OCR's prohibition on creating website banners asking the website user to accept or reject tracking technologies.[3]

Thus, "Solution 1" is realistically the only operational approach that will be feasible for most organizations.

Five Steps You Can Take to Address HIPAA Tracking Issues. If you use third-party tracking technologies on your website and/or apps, and are a regulated entity (*i.e.,* a covered entity or business associate), then you need a practical approach to mitigate against unauthorized disclosures. To address potential noncompliance issues under HIPAA, consider these five steps:

1. **Prepare an inventory of cookies and tracking technologies.** Establish your baseline using tracking technology detection tools and interviews with IT and marketing.

2. **Determine internal uses.** Is the data collected and/or retained in aggregated or de-identified form (*e.g.*, to improve the website)? Is the data used for retargeting or other marketing purposes? What internal functional groups access and/or use the data?

3. **Establish the scope of third-party disclosures.** To avoid the need for individual authorizations when sharing PHI with vendors, confirm that the vendor is utilizing the PHI on behalf of the regulated entity solely for services permitted under HIPAA. Are there contractual limitations/controls in place with the technology vendor? Are there disclosures of the data to any additional third parties (*e.g.*, secondary uses, such as AI/ML or other analytics)?

4. **Amend existing agreements/templates.** Amend existing vendor agreements with business associate agreements, as needed. Include a restriction on any data uses beyond delivering services (applicable to the business associate/vendor and any other sub-business associate service providers).

5. **Add a checkpoint in your vendor contracting and PIA processes.** Avoid future surprises by incorporating a tracking technology checkpoint in your procurement or contracting process and/or PIA workflow.

For more information about the OCR's guidance and other questions related to health care data privacy and security, please contact brent.hoard@troutman.com and emma.trivax@troutman.com.

---

[1] *Amer. Hosp. Ass's, et al v. Rainer*, Case No. 4:23-cv-01110-P (N.D.C. Tex. 2023).

[2] 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.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Health Care + Life Sciences
- Health Care Regulatory
- Privacy + Cyber