epsilon
life sciences

CLIENT ALERT

HHS Updates Its Online Tracking Guidance

Earlier this week, the Department of Health & Human Services (HHS) updated its landmark 2022 guidance on the use of online trackers by the healthcare industry. Through the Office for Civil Rights (OCR), the U.S. agency enforces HIPAA, and it caused significant upheaval when the bulletin was first issued because of the hard line it took against the use of cookies, pixels, and similar technologies by covered entities. As a result, 2023 saw dozens of class action lawsuits filed against healthcare organizations, and even a counter-legal action by the American Hospital Association against HHS itself.

HHS updated its prior bulletin directly, so the old version is not immediately available online. However, we examined archived versions of the old bulletin and produced a comparison document of new changes, which are summarized below. Changes include new clarifications, examples, recommendations, and enforcement priorities from OCR.

Changes to Online Tracking Guidance

Overall, the changes issued by HHS could be described as cosmetic. The agency largely held to its broad interpretation of protected health information (PHI) as including IP address and other pseudo-identifiers when combined with certain online activity. As before, the distinction between authenticated and unauthenticated web pages was key.

HHS both slightly expanded and somewhat softened its opinions on what constitutes individually-identifiable health information (IIHI) – which is a prerequisite for data to be PHI under its health information regulations. In the first case, HHS amended "medical device ID," to read, "device ID," in its listing of relevant data elements. This small change may be intended to add computer-based devices that a user must leverage to access online resources. On the other hand, it also eased its previous rulings with the following helpful caveat:

> "But 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 webpage addressing specific health conditions or listing health care providers is not a sufficient combination of information to constitute IIHI 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." - HHS Office for Civil Rights

Clarifying Examples

The most useful additions to the guidance are in the form of examples of what does and does not, in OCR's opinion, constitute IIHI/PHI. While keeping to its former guidance that all authenticated webpages will likely maintain and transmit PHI if tracking technologies are used, it provided several examples of what non-authenticated webpages and purposes would not be covered by HIPAA, specifically, information about job postings, visiting hours, or data used for academic research.

> "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." - HHS Office for Civil Rights

Again, HHS gives, and it takes away, by including PHI examples. This includes what many have suspected all along: that web applications like appointment schedulers and symptom-checkers are considered PHI by OCR. More cryptically, the guidance also now includes a counter example:

> “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.” - HHS Office for Civil Rights

It's not clear how covered entities should take action on this new advice, apart from making a risk-based decision based off how it suspects its users use its site. This will be difficult because a visitor looking at an oncology page for academic research, as opposed to treatment research, looks the same to a hospital website administrator.

Additional Options

One new recommendation that HHS makes we want to highlight, since it shows they have considered workarounds covered entities could use. In the section about how to contract with tracking technology vendors, HHS acknowledges that some vendors may refuse to sign a BAA. Probably the most infamous and widely-used tracking technology in this category is Google Analytics. In a case where a vendor will not make satisfactory assurances of HIPAA compliance through a BAA, HHS recommends using a Customer Data Platform (CDP) as an intermediate step. A CDP that will agree to HIPAA terms can then deidentify the visitor data before it goes to the non-compliant third-party.

In our experience, there are several CDPs able to serve this function, if setup and enabled properly, allowing the organization to proxy sensitive traffic through a database either hosted and controlled by the covered entity or a third-party business associate.

Our consultants have worked with counsel and clients to do just that, most importantly in a manner that meets the deidentification requirements of the HIPAA Privacy Rule.

Parting Thoughts

Perhaps the most notable departure from the old guidance is an entirely new concluding section and paragraph discussing OCR’s “Enforcement Priorities.” Despite most of the guidance above stemming from requirements under HIPAA’s Privacy Rule, it is HIPAA’s Security Rule that HHS cites as its primary compliance concern. When investigating the use of online trackers, OCR says that its principal interest lies in security risks to PHI. While this does give encouragement to those struggling to adopt this guidance for their digital properties, it should be remembered that the FTC in 2023 used “security breach” language in its regulation to enforce its use of the Health Breach Notification Rule for what were essentially, allegedly privacy violation by GoodRx. Crucially, HIPAA’s Security Rule does contain BAA requirements and encryption standards, so this enforcement priority may not be the concession to healthcare organizations it first appears to be.

How Epsilon Life Sciences Can Help

In response to legal action and for proactive compliance efforts, Epsilon Life Science’s forensic consultants work closely with counsel and health clients to identify tracking technologies on web sites and mobile apps, pinpoint data categories being transmitted to third-parties, and workshop solutions tailored to meet letter of the law while still allowing critical healthcare outreach functions. Please contact us if you have any questions about this guidance, or for a discussion on how to manage this fast-moving risk area. See here for our prior overview and insights on the topic of online tracking technologies.

Nick Weil, JD, CIPT
nweil@epsilonlifesciences.com
949.275.4578

Brian Segobiano, CIPP/E
bsegobiano@epsilonlifesciences.com
317.860.8025