Coppersmith Communiqué

OCR "Clarifies" its Guidance on Online Tracking. *Not Quite.*

Kristen Rosati and Erin Dunlap, Coppersmith Brockelman PLC
April 2, 2024

On March 18, 2024, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued revised guidance[i] about how HIPAA applies to online tracking—the use of cookies, pixels, and other website analytics tools. Unfortunately, the new guidance made no real substantive changes. It seems OCR is digging in its heels, with no immediate regulatory relief in sight, while health care organizations struggle to comply with the guidance without impacting website functionality and operations too much. Unfortunately, the use of online tracking by health care organizations carries significant risk.

Regulatory risk: Both OCR and the Federal Trade Commission (FTC) have issued guidance on online tracking that set difficult standards to meet.[ii] They have initiated investigations and issued joint "warning" letters to approximately 130 hospital systems and telehealth providers the use of online tracking.[iii] The FTC has imposed penalties against numerous parties related to online tracking.[iv] And the regulatory attention isn't limited to the feds: State Attorneys General (AGs) also are initiating investigations related to online tracking under their state consumer data privacy laws and/or state health information confidentiality laws.

Litigation risk: Numerous lawsuits (including several class actions) have been filed against third-party tracking vendors[v] and hospital systems and telehealth providers[vi] over the disclosure of website user data through online tracking.

Financial risk: Given the regulatory and litigation risk, cyber liability insurers are issuing detailed requests for information to health care organizations to explain their use of online tracking, raising concerns about increases in insurance premiums.[vii]

How did the OCR Online Tracking Guidance Change? We had a small glimmer of hope that OCR would revisit its guidance when the American Hospital Association (AHA) filed a lawsuit against OCR on November 3, 2023, challenging OCR's original guidance on the use of online tracking.[viii] Unfortunately, OCR did not make significant revisions in response to the AHA lawsuit.

Treatment of IP Addresses Alone as PHI: The March 2024 guidance slightly retracted OCR's original position on IP addresses, stating IP addresses may constitute PHI "in some circumstances" and "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 [PHI] 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."

However, the March 2024 guidance suggests that the intent of the website user dictates whether the tracking technology is collecting PHI. Specifically, OCR states that a general website visitor (such as a student writing a term paper about a health condition) would not involve a disclosure of an individual's PHI because the technology "did not have access to information about an individual's past, present, or future health, health care, or payment for health care." However, the collection of identifiable information from an individual looking at a hospital's webpage in order to seek a second opinion on treatment options for that same health condition involves the collection of PHI. This is not a workable distinction, as HIPAA regulated entities will not know the intent of a website user.

Use of Customer Data Platforms: The March 2024 guidance also encourages the use of a Customer Data Platform (CDP), which OCR defines as "software that can combine data from multiple sources regarding customer interactions with a company's online presence to support a company's analytic and customer experience analysis." OCR explained that CDP vendors may be willing to sign business associate agreements and de-identify online tracking data before sending it to online tracking vendors like Google or Facebook.

We agree that the use of a CDP or "middlemen" vendors is helpful for HIPAA regulated entities to maintain some analytical capabilities to determine whether their marketing efforts through social media platforms are effective. But we have noted that HIPAA regulated entities need to "kick the tires" to make sure the CDP vendors are appropriately de-identifying data before sending data to online tracking vendors. In addition, these vendors can be expensive and may be cost prohibitive for some organizations.

Risk Analysis and Risk Management Process: The March 2024 guidance also made clear that HIPAA regulated entities should address the use of tracking technologies in their risk analysis and risk management process. OCR is "prioritizing compliance with the HIPAA Security Rule in investigations into the use of online tracking technologies." This is a big heads-up to HIPAA regulated entities to accelerate their internal analysis on the use of online tracking and to integrate any remaining online tracking into the HIPAA security risk assessment process.

Our Recommendations: Given the continued antipathy of OCR, the FTC and State AGs toward the use of online tracking by health care organizations, we recommend the following actions:

- Take a deep breath. Most HIPAA regulated entities and other organizations that handle health information are dealing with this issue!

- Initiate an internal investigation—under attorney-client privilege—to determine what online tracking your organization uses on its websites and apps. The investigation should determine precisely what data is being sent to what online tracking vendor.

- Get HIPAA business associate agreements in place with any online tracking vendors that are obtaining PHI.

- If your organization is (or was) sending PHI to online tracking vendors without a HIPAA business associate agreement in place, conduct a HIPAA breach reporting risk analysis and document whether or not there is a reporting obligation under HIPAA.

- If your organization is subject to the FTC's Health Breach Notification Rule at 16 C.F.R. Part 318, determine whether there is a reporting obligation under that rule.

- If your organization is subject to a state breach notification law, evaluate whether there is a reporting obligation under that law.

- If the current use of online tracking is not consistent with federal and state laws, develop a detailed work plan to remediate such use. Consider the use of a CDP vendor that de-identifies data before sending it to online tracking vendors but do a close examination of the services to make sure it's the right fit before engaging the vendor.

- Develop an internal policy on the use of online tracking. We think it will help in an OCR, FTC, or State AG investigation to demonstrate that your organization is taking steps to address the use of online tracking systematically.

- Make sure you understand the current privacy law landscape, including what laws apply to your organization, in responding to questions from your cyber liability insurer. Cyber security insurers also may want to know if you have had the use of online tracking technology reviewed by an attorney. In responding, don't explain the actual advice provided, or you may waive attorney-client privilege.

- Keep an eye out for developments, particularly what happens in response to the AHA lawsuit in the next few months. We expect the courts may eventually require OCR to undertake a formal rule-making process to conform to the Administrative Procedures Act.

KBR and EFD

About the Authors

Kristen Rosati is considered one of the nation's leading "Big Data" and HIPAA compliance attorneys. She has deep experience in data governance and strategy, data sharing for research and innovation, and biobanking and genomic privacy. Kristen is a Past President (2013-2014) and Fellow (2021) of the American Health Law Association (AHLA), the nation's largest health care legal organization. She has received numerous recognitions in Chambers USA, Best Lawyers in America and Super Lawyers, and has been recognized in "Most Outstanding Women in Business," "Most Influential Women in Arizona Business," and Arizona's Top 100 Lawyers.

Erin Dunlap is a nationally recognized health information privacy attorney, regularly advising clients on compliance with HIPAA, patient access laws, and other state consumer data privacy and breach notification laws. Erin has successfully represented clients through privacy and security-related investigations initiated by HHS/OCR, State AGs and other state agencies following data breaches, patient complaints and whistleblower claims. She has been ranked as a top lawyer in healthcare by Chambers USA.

Kristen and Erin have counseled many health care organizations in the evaluation and remediation of online tracking, and in responding to government investigations.

[i] *See* *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (OCR, March 18, 2024).
[ii] *Id.*; *Updated FTC-HHS Publication Outlines Privacy and Security Laws and Rules that Impact Consumer Health Data* (OCR and FTC, Sept. 15, 2023); *Collecting, Using, or Sharing Consumer Health Info.? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule*, (FTC, Sept. 2023); Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking (FTC, March 16, 2023); *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data* (FTC, July 11, 2022).
[iii] *See* *HHS Off. for Civil Rights and the Fed. Trade Comm'n Warn Hosp. Sys. and Telehealth Providers about Privacy and Sec. Risks from Online Tracking Techs* (HHS, July 20, 2023). *See also, e.g.* Letter from Melanie Fontes Rainer, Director OCR, and Samuel Levine, Director, FTC Bureau of Consumer Protection, to Zachariah Booker, CEO, ADHD Online (July 20, 2023).
[iv] *See, e.g.*, *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advert.*, (FTC, Feb. 1, 2023); Agreement Containing Consent Ord., *In re* Betterhelp, Inc., No. 2023169 (FTC, March 2, 2023) imposing $7.8 settlement). *See also* Todd Feathers, *The FTC Is Taking on Telehealth's Data Sharing Problem—Starting with GoodRX* (The Markup, Feb. 1, 2023).
[v] In 2022, Facebook parent Meta agreed to pay $725 million to settle a class action lawsuit that claimed the social media giant gave third parties access to user data without their consent. *See* Arjun Kharpal, *Facebook Parent Meta Agrees to Pay $725 Million to Settle Privacy Lawsuit*, CNBC (Dec. 23, 2022, 4:47 AM).
[vi] *See* Steve Alder, *Mass Gen. Brigham Settles 'Cookies Without Consent' Lawsuit for $18.4 Million*, THE HIPAA JOURNAL (Jan. 20, 2022). See also *Doe v. Hey Favor, Inc. (3:23-cv-00059)*; Mary Kekatos, *Lawsuit accuses Cedars-Sinai hospital's website of sharing patient data with Meta, Google*, ABC NEWS (Feb. 15, 2023, 3:07 AM).
[vii] We have seen cyber security insurers ask specific questions about:

- the collection, use and disclosure of data, including personal information, geolocation information, biometric data, and information on children under the age of 13;
- the use of codes, software, tools, or other technology that tracks, collects, or otherwise records user activity including Flash Cookies, Meta Pixel, Microsoft Clarity, or any similar tracking tool or technology, and whether data subjects are provided the right to opt-out of this type of activity;
- whether the management of online marketing technologies is done internally or externally;
- whether data subjects can log into online services using account credentials associated with thirty-party social media;
- whether an applicant/insured has a published privacy policy;
- whether an applicant/insured buys data pertaining to individuals from third parties; and
- whether an applicant/insured has a process in place to respond to data subject requests (access requests, right to erasure/rectification/processing restriction/objection/automated decision making/etc.) and complaints based on applicable privacy regulations.

[viii] *See* *Lawsuit Challenges Federal Rule that Ties Providers Hands in Efforts to Reach Their Communities*, AM. HOSP. ASS'N.