akerman

Blog Post

OCR and FTC Issue Warning to Hospital Systems and Telehealth Providers about Tracking Technologies

July 31, 2023

By Elizabeth F. Hodge, Jordan T. Cohen, and Ameer Al-Khudari

On July 20, 2023, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) announced they were sending a joint letter to approximately 130 unidentified hospital systems and telehealth providers highlighting the agencies' concerns about the use of tracking technologies on websites and mobile apps in violation of HIPAA. While the joint letter was directed to a small number of recipients, in the announcement OCR and the FTC encouraged all companies they regulate to review their data-tracking practices and ensure that their tracking technologies are not impermissibly disclosing consumers' sensitive personal health data to third parties. The letter — and the decision to publicly announce its existence — suggests that OCR and the FTC are likely to prioritize the enforcement of HIPAA and other laws against those entities that the agencies believe are impermissibly using tracking technologies.

The Joint Letter

With the letter, the FTC and OCR draw recipients' attention to "serious privacy and security risks related to the use of online tracking technologies" that are "impermissibly disclosing consumers' sensitive personal health information to third

Related People

Ameer Al-Khudari
Jordan T. Cohen
Elizabeth F. Hodge

Related Work

Data Privacy and Security
Healthcare
Hospitals and Health Systems

Related Offices

Chicago
New York
West Palm Beach

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Read blog posts

parties." The letter explicitly references the Meta/Facebook Pixel and Google Analytics tracking technologies.

Citing recent research, media reports, previous FTC enforcement actions, and an OCR guidance document from December 2022, the letter describes how "tracking technologies gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users." The agencies then call out HIPAA-regulated covered entities and business associates by urging their compliance with the HIPAA Privacy, Security, and Breach Notification Rules with regard to protected health information (PHI) transmitted or maintained electronically or otherwise. OCR and the FTC underscore that "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules." And for those entities not covered by HIPAA, the agencies highlight that such entities may nevertheless be obligated to protect against impermissible disclosures of individuals' information under the FTC Act and the FTC Health Breach Notification Rule.

How We Got Here

In its December 2022 guidance, OCR announced that tracking data on a covered entity's website is PHI:

Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI. Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage.

OCR's statement that data tracked from a patient logging into a user-authenticated website is PHI is not particularly surprising. However, OCR went a

step further by stating that tracking data captured on unauthenticated websites (i.e., publicly available websites that can be viewed without a username and password) may also be PHI. According to the agency, tracking data (e.g., an IP address) of an individual searching about symptoms or health conditions on a covered entity's website would constitute PHI even if the visitor is not currently a patient. OCR emphasized the HIPAA compliance obligations for those capturing PHI tracking data. In the months that followed OCR's guidance, entities subject to HIPAA have reported large health data breaches related to past use of tracking technologies.

For its part, the FTC has already taken enforcement actions in cases involving the use of tracking tools. BetterHelp, an online therapy provider, shared customer data with parties including Facebook, Snapchat, Pinterest, and an online advertising firm. In addition to a $7.8 million civil penalty, BetterHelp agreed to a third-party privacy assessment every two years for two decades.

Early in 2023, the FTC pursued enforcement using the Health Breach Notification Rule (HBNR) for the first time. GoodRx was subject to a $1.5 million civil penalty for failing to disclose that it shared user data with third parties, including Facebook and Google. A few months later, the FTC enforced the HBNR against Easy Healthcare, the developer of fertility logging app Premom, with the company agreeing to pay $100,000. On July 25, 2023, the FTC published a blog summarizing takeaways from its cases involving consumers' health information and warning companies that collect or use health data that the privacy of health information is a top priority for the agency.

Enforcement

OCR Director Melanie Fontes Rainer and FTC Bureau of Consumer Protection Director Samuel Levine closed the letter with a reminder that both agencies are closely watching developments in this area. Also,

according to public comments by other OCR officials, the agency is actively investigating the use of website tracking tools by certain HIPAA-covered entities. Given the keen interest that OCR and the FTC are showing in tracking technologies, organizations regulated by either agency should consider doing the following in anticipation of future enforcement activity:

- Confirm whether and how their organization uses tracking technologies;
- Train compliance officers and compliance committee members about tracking technologies and how they may violate HIPAA or other laws;
- Understand the data collected by tracking technologies, with whom the data is shared, and how the recipient uses the personal health information;
- Identify what consents or authorizations the organization has from individuals if their health information is shared or disclosed by tracking technologies;
- Assess whether the sharing or disclosing of data via tracking technologies is compliant with HIPAA, the FTC Act, and the FTC's Health Breach Notification Rule, as applicable;
- Determine whether the organization can modify its use of tracking technology to minimize or eliminate the sharing or disclosure of personal health information shared with the vendor.

Akerman's Health Law Rx blog will continue to monitor OCR's and the FTC's enforcement activities related to the use of online tracking technology and the privacy of personal health information.

*The authors would like to thank summer associate **Ameer Al-Khudari** for his assistance with this article.*