PUBLICATION

OCR Enforcement Action Likely: Reminder of Steps to Take Now

Authors: Julie A. Kilgore, Alisa L. Chestler
October 02, 2023

Are you a health care provider, business associate, or other entity subject to the requirements of the Health Insurance Portability and Accountability Act (HIPAA) regarding the use and disclosure of protected health information (PHI)? Do you know whether any of the web pages on your websites or mobile apps use third-party tracking technologies? Do you know what data you're disclosing to third-party tracking technology companies and how that data is being used by those companies? Have you re-evaluated whether any third-party tracking technology has been updated or modified since you last reviewed it? If you answered "yes" to the first question but "no" (or even "I'm unsure") to the following questions, you are at risk of violating HIPAA, and this alert is specifically for you, so keep reading.

As we enter Cybersecurity Awareness Month, the continued disclosures of PHI in violation of HIPAA by hospitals, telehealth providers, and other HIPAA-regulated entities to third-party tracking technology companies remain top of mind as we wait for the Office of Civil Rights (OCR) to bring its first enforcement action on this topic. Numerous events, such as class action lawsuits, issuance of regulatory guidance and warnings, and enforcement actions brought by the Federal Trade Commission (FTC) against non-HIPAA-regulated entities over the last year point to probable enforcement activity in the future. To raise awareness about these unauthorized and impermissible disclosures of PHI, we want to remind you of the steps you should be taking now to minimize any potential liability. Join us in celebrating October as Cybersecurity Awareness Month by either examining or re-examining your disclosures of PHI to third-party tracking technology companies to ensure you're in compliance with HIPAA.

Over the last year, two key themes have emerged:(1) regulatory agencies have repeatedly expressed significant concerns about third-party tracking technologies having unauthorized or impermissible access to PHI and other health-related information; and (2) class action lawsuits against HIPAA-regulated entities related to third-party tracking technologies have been on the rise. Key events within those two broader themes are highlighted below.

Timeline of Key Events:

- In mid-2022, a study was published showing that many top hospitals were disclosing PHI to third parties via tracking technologies used on their websites.
- Following that publication, numerous class action lawsuits were filed against health care providers, with more than fifty lawsuits total filed by the end of 2022.
- Due to the rise in lawsuits related to unauthorized or impermissible disclosures of PHI via third-party tracking technologies, 2022 ended with the Department of Health & Human Services (HHS) issuing guidance on the topic. Key components of the guidance included the following:

  - HIPAA-regulated entities must still comply with HIPAA's requirements for disclosures of PHI to third-party tracking companies;
  - Tracking technologies are scripts or code on a website or mobile app used to gather information about users as they interact with the website or mobile app, such as cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts;

  - PHI includes information about an individual, including an IP address, collected on a HIPAA-regulated entity's website or mobile app where the collection of that information connects the entity to the individual and relates to the individual's past, present, or future health, health care, or payment for health care;
  - Third-party tracking technologies on user-authenticated web pages and mobile apps generally have access to PHI; and
  - Third-party tracking technologies on unauthenticated web pages generally do not have access to PHI but still may if, for example, it is a login page, the page addresses specific symptoms, or the page permits the scheduling of doctor appointments.
- 2023 began with more lawsuits filed against HIPAA-regulated entities, and the FTC began bringing enforcement actions against non-HIPAA-regulated entities for the unauthorized disclosure of personal health information to third-party tracking technology companies pursuant to the Health Breach Notification Rule.
- In April 2023, the director of OCR stated that its first enforcement action concerning tracking-tool-related HIPAA violations would hopefully be filed soon.
- In July 2023, the FTC and HHS sent joint warning letters to 130 health care organizations, alerting them of the serious privacy and security risks related to the use of online tracking technologies on websites and mobile apps. Key components of the letters included the following:

  - Reminded HIPAA-regulated entities to comply with the HIPAA Privacy, Security, and Breach Notification Rules for disclosures of PHI to third-party tracking technology companies;
  - Committed to ensuring that consumers' health privacy remains protected with respect to this critical issue;
  - Stated they are closely watching developments in this area; and
  - Strongly encouraged HIPAA-regulated entities to review the laws and take actions to protect the privacy and security of PHI.
- In September 2023, the FTC and HHS broadly published the warning letters sent to the 130 entities.

Now that you're also convinced enforcement action is likely on the horizon for HIPAA-regulated entities, here's a reminder of the steps to take or re-evaluate now to minimize the risk of lawsuits, enforcement actions, and potential liability, and most importantly, to protect the privacy and security of your patients' PHI.

Steps to Take or Re-Evaluate in Consultation with the Advice of Appropriate Legal Counsel:

- Determine whether your website or mobile app contains third-party tracking technologies.
- Where third-party tracking technologies are present on a website, determine whether the web page is authenticated or unauthenticated to assist in evaluating whether PHI is present.
- Where PHI is located and being disclosed to third-party tracking technology companies, determine whether such disclosure is permitted by the HIPAA Privacy Rule.

  - If so, ensure that such disclosure is pursuant to a business associate agreement with a business associate.
  - If not, ensure that you've obtained appropriate HIPAA authorizations to disclose PHI prior to the disclosure.
- If you discover PHI is being disclosed in an impermissible or unauthorized manner, do the following:

  - Conduct a risk assessment and if required, comply with the notification requirements of the HIPAA Breach Notification Rule; and
  - Cease the disclosure of PHI to third-party tracking technology companies until you can do so pursuant to either a business associate agreement or a valid HIPAA authorization from the patient.

- Address the use of third-party tracking technology companies in your risk assessment and risk management processes on an ongoing basis.

There's no better time than Cybersecurity Awareness Month, while also on the horizon of probable OCR enforcement action, to take steps to ensure your disclosure of PHI to third-party tracking technology companies is not the next item included within the Timeline of Key Events above.

If you have any questions or need additional information regarding this alert, please do not hesitate to contact Julie A. Kilgore, Alisa L. Chestler, or any member of the Baker Donelson Data Protection, Privacy, and Cybersecurity team.