March 16, 2023

Warning for Providers—New Guidance on Data Risks Associated With Websites and Portals

In December 2022, the U.S. Department of Health & Human Services' Office for Civil Rights (OCR) issued a bulletin (the Bulletin) highlighting the obligations of Health Insurance Portability and Accountability Act of 1996 (HIPAA)-covered entities and their business associates (collectively, the Regulated Entities) when using online tracking technologies that collect and analyze information about users through websites, portals or mobile applications. The Bulletin addresses potential impermissible disclosures of electronic protected health information (ePHI) by Regulated Entities to online tracking technology vendors and provides steps for protecting ePHI when using these technologies. This article summarizes the requirements of the Bulletin and provides practical recommendations to mitigate HIPAA exposures associated with the tracking features of websites, etc.

Background Information

Online tracking technologies associated with websites and apps provide insightful information regarding the behaviors of users, including what content or features attract visitors and which pages they frequently browse. For website and app owners, these insights are used to enhance the website and app functionalities and design and to provide updates that enrich the user experience. These technologies may allow healthcare providers to offer more robust, remote and interactive services to patients. For example, scheduling an appointment with a doctor, ordering online prescription refills, direct messaging, paying bills online or receiving services through a telehealth visit are now all immensely simpler using an app or a website. The COVID-19 pandemic further empowered this necessary reliance on technology services in healthcare. However, even with all these benefits to healthcare access, online tracking technologies also open the door to data misuse through data breaches or identity theft through the software or application vendor.

Defining Tracking Technologies

OCR released the Bulletin in response to the growing data privacy-related scrutiny of online tracking technologies. OCR defines a tracking technology as a script or code on a website or an app used to gather information, including individually identifiable health information, about a user's interaction with the website or app. Once the information is collected, it is analyzed by the website or mobile app owner or a third party to create insights about users' online activities. All the collected information is generally ePHI and triggers HIPAA Privacy, Security and Breach Notification rules (collectively, HIPAA), which mandate that covered entities may not disclose ePHI to third parties unless such disclosure is made pursuant to an individual's HIPAA-compliant authorization or a HIPAA exception (such as for treatment, payment or healthcare operations). OCR additionally provides guidance for how tracking technologies may be used by Regulated Entities in three specific contexts: (1) user-authenticated webpages, (2) unauthenticated webpages and (3) mobile apps, each of which is described below.

1. **User-Authenticated Webpages**

A user-authenticated webpage is one that requires a user to log in to obtain access. Common examples of user-authenticated webpages include patient portals and telehealth platforms. Tracking technologies on user-authenticated webpages generally have access to ePHI, including an individual's Internet protocol (IP) address, medical record number, home and/or email address, dates of appointments, and even the individual's diagnosis and treatment, prescription, billing and other sensitive information. Thus, OCR mandates that Regulated Entities must ensure that any user-authenticated webpages that include tracking technologies only use and disclose ePHI in compliance with HIPAA and enter into a business associate agreement (BAA) with each tracking technology vendor.

2. **Unauthenticated Webpages**

In contrast, an unauthenticated webpage is one that does not require a user to log in to obtain access. An example of such a webpage includes a "brochure type" webpage, where, for example, an individual can view general, public-facing information or news about a Regulated Entity. Tracking technologies used on unauthenticated webpages generally do not have access to individuals' ePHI and thus are not typically regulated by HIPAA. That said, OCR provides two scenarios involving unauthenticated webpages that would, in fact, make the webpages subject to HIPAA:

- *Scenario No. 1*: A Regulated Entity's login or registration page (which may be the website homepage) in which the individual enters credential information (e.g., name, email address) on that page. Such information is ePHI and therefore protected by HIPAA.
- *Scenario No. 2*: A webpage that addresses specific symptoms or health conditions or that permits individuals to search for doctors or schedule appointments without entering credentials. In this instance, the tracking technologies could collect an individual's email and/or IP address. Here, the Regulated Entity is disclosing ePHI to the tracking vendor, and that information is protected by HIPAA.

3. **Mobile Apps**

Healthcare mobile apps have proliferated in recent years and are commonly offered by technology companies, software providers and others. When mobile apps are developed or offered by Regulated Entities, though, the Regulated Entities must ensure the mobile apps comply with HIPAA. Many of these mobile apps use tracking technologies that collect user information, including fingerprints, network location, geolocation and device ID, all of which is ePHI. Disclosure to the mobile app or any other third-party vendor must comply with HIPAA, including the need for a BAA. However, OCR states that HIPAA does not apply to mobile apps that are not developed or offered by or on behalf of Regulated Entities (such as a general website search engine available to the public). These apps may be subject to other laws, like the Federal Trade Commission's Health Breach Notification Rule.

Conclusion

The Bulletin provides a broad interpretation of what constitutes ePHI and how Regulated Entities may gather, use and disclose, knowingly and unknowingly, that information using online tracking technologies through websites and portals. Because this is the first time a specific alert has been issued to physicians, health systems and hospitals, it shows the need for Regulated Entities to continuously assess usage of these tracking technologies and the risk of compromise of ePHI. Balancing the need for greater access to care for patients with protecting the very health data collected through this access will be a concern for Regulated Entities for years to come.

Practical Tips When Using Tracking Technologies

- Enter into a BAA with a tracking technology vendor that meets the definition of a "business associate."
- Ensure that all disclosures of ePHI to tracking technologies are permitted by HIPAA and, unless an exception applies, only the minimum necessary ePHI to achieve the intended purpose is disclosed. This should be specifically stated in either the agreement with the vendor or the BAA.
- Address the use of tracking technologies in the covered entity's risk analysis and risk management processes required by HIPAA, as well as implement other administrative, physical and technical safeguards in accordance with the HIPAA Security Rule, including:
    - Encrypt ePHI that is transmitted to the tracking technology vendor.
    - Enable and use appropriate authentication, access, encryption and audit controls when accessing ePHI maintained in the tracking technology vendor's infrastructure.

Healthcare providers often find it daunting to negotiate with technology vendors and ensure all the regulatory requirements are addressed, and healthcare technology companies need to ensure the development of compliant technology to see success in the healthcare marketplace. Our healthcare and technology lawyers deal with these issues daily and are available to help.

Would you like to receive our *Day Pitney C.H.A.T. Newsletter?* Sign up here.

Authors

Susan R. Huntington

Partner

Hartford, CT | (860) 275-0168

Washington, D.C. | (202) 218-3909

shuntington@daypitney.com