Online Tracking Codes: The New HIPAA Compliance Nightmare

In recent years, most health care organizations with an online presence use website and mobile app tracking technology to determine how users navigate and engage with their sites and apps. They then use this information to improve site experience so it better aligns with user needs and preferences.

However, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) recently determined that tracking technologies pose a significant HIPAA disclosure risk. According to the OCR, providers, hospitals, insurers and other HIPAA-covered entities, and their business associates, should not use tracking technologies in a manner that would result in impermissible disclosures of personal health information (PHI) to tracking technology vendors or other third parties. The OCR has signaled this is now an enforcement priority, and it is likely in response to a growing number of such disclosures affecting millions of patients and the resulting litigation.

The OCR issued a **Bulletin** to highlight covered entity and business associate obligations when using online tracking codes. A brief overview is provided here:

Tracking Technology

Tracking technology is a script of code on a website or mobile app that is generally not apparent to the user. According to the OCR guidance, websites commonly use cookies, web beacons or tracking pixels, session replay scripts and fingerprinting scripts to track and collect user information. Mobile apps typically embed tracking code within the app to directly collect user info, and the apps may also capture unique user mobile device-related identifiers such as device ID or advertising ID. This type of information enables a mobile app owner, vendor, or any third party who receives such detail, to build individual profiles about the user.

HIPAA Rules Apply to Regulated Entities' Use of Tracking Tech

Tracking technologies placed on a regulated entity's website or mobile app capture individually identifiable health information (IIHI) that a user provides during an online experience. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. According to the OCR guidance:

> *All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity … and thus relates to the individual's past, present, or future health or health care or payment for care.*

Two Categories of Web Page Tracking

A user-authenticated web page requires a user to log in before accessing a page, such as a patient portal or a telehealth platform. PHI collected on these pages may include a user's IP address, medical record number, home or email addresses, appointment dates, diagnosis, or treatment, billing or prescription information. The OCR guidance requires that a regulated entity configure any user-authenticated pages that include tracking technologies "to allow such technologies to only use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule."

CHRISTIAN & BARTON, LLP
ATTORNEYS AT LAW

If tracking vendors create, receive, maintain or transmit PHI for a function that involves the disclosure of PHI, the covered entity **must have a valid business associate agreement** (BAA) with the vendor to ensure the PHI is protected in compliance with HIPAA regulations. For example, if a user makes an appointment through the website of a covered provider that uses tracking code, then the site could automatically transmit information regarding the appointment and the user's IP address to a tracking vendor. In this situation, the tracking vendor is considered a business associate or sub-business associate and a BAA or sub-BAA is necessary.

An unauthenticated web page does not require a user login to view content. These pages contain content of a general nature, such as provider location, services or policies. Tracking technology on these pages do not usually have access to PHI and are not always regulated by HIPAA. However, HIPAA Rules can apply to unauthenticated pages when:

- tracking technology appears on a patient portal login or registration pages and those pages collect login or registration info

- tracking technology is present on pages that address specific symptoms or health conditions, or permit a search for either a specific provider or available appointments without a login as there may be access to the user's email or IP address, which is considered PHI in this circumstance

Mobile App Tracking

Apps collect information that a user types or uploads as well as info about the user's device. The OCR guidance indicates all such information collected by a regulated entity's mobile app is PHI and therefore the entity must comply with all HIPAA Rules for any PHI that the mobile app uses or discloses. The guidance also allows that HIPAA Rules "do not protect privacy and security of information that users voluntarily download or enter into mobile apps that are not developed or offered by or on behalf of regulated entities." However, in those situations other laws may apply, such as the Federal Trade Commission (FTC) Act and the FTC's Health Breach Notification Rule.

HIPAA Compliance Obligations When Using Tracking Technology

Compliance steps covered entities should take include:

- Identify the use of tracking technology via the website or app's privacy policy, note or terms and conditions. Note, however, that PHI disclosures to a technology vendor are not permitted based solely on this admission of using tracking technology. Instead, entities must ensure all appropriate vendors have signed a BAA and that there is an applicable permission prior to a disclosure.

- If there is not an applicable Privacy Rule permission or if the vendor is not a business associate, then a user's HIPAA-compliant authorization must be requested before the PHI is disclosed. According to the OCR, a website banner that asks users to accept or reject a website's use of cookies or other tracking technology does NOT constitute a valid HIPAA authorization.

- Require vendors to remove PHI from the information received or de-identify the PHI before the vendor saves the information.

- It is essential to establish a BAA with every tracking technology vendor that meets the definition of a "business associate" and require that they have sub-BAAs with their subcontractors if they are providing such tracking technology.

- The OCR guidance also notes that breach notification protocols be triggered when an impermissible PHI disclosure to a tracking vendor occurs because it compromises the security or privacy of PHI when there is no Privacy Rule requirement or permission to disclose and there is no BAA with the vendor.

Strategies for Covered Entities

HIPAA-regulated entities should conduct regular website and app audits to verify what data is being collected, identify tracking code use and determine if the potential exists for PHI disclosures. For tracking activities that disclose PHI to a third party, ensure a viable BAA is in place and/or obtain appropriate HIPAA-complaint authorizations from users before a disclosure occurs. Finally, consider working with legal counsel to assist with business associate identification and necessary agreements, privacy policy updates, regulatory and litigation risk assessments, and breach guidance.

For additional information, please contact:

Jonathan M. Joseph, Esq.
jjoseph@cblaw.com | 804.697.4125

Christian & Barton, LLP
901 East Cary Street, Suite 1800
Richmond, Virginia 23219

This article is provided as an informational service and does not constitute legal counsel or advice, which can only be rendered in the context of specific factual situations. If a legal issue should arise, please contact an attorney listed in this article, or retain the assistance of other competent legal counsel. Case results depend on a variety of factors unique to each case and results do not guarantee or predict a similar result in any future case undertaken.

©Christian & Barton, LLP 2023
All Rights Reserved