Proskauer

HHS Bulletin: Covered Entities' Disclosure of PHI Collected via Online Tracking Technologies Falls under HIPAA

Proskauer on Privacy Blog on **December 14, 2022**

On December 1, 2022, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates when using "online tracking technologies," or what OCR describes as "script or code on a website or mobile app used to gather information about users as they interact with the website or mobile app," which is then analyzed by website owners, app operators or third parties to create user profiles or garner insights into users' online activities.

These might include cookies, web beacons, pixels, session replay software and fingerprinting scripts that track and profile users' web activities, whether on web portals behind an authentication wall or on unauthenticated webpages or mobile apps, and, in some cases, disclose the collected user data to technology vendors for marketing purposes without HIPAA-compliant authorization. As the OCR stated: "**Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of protected health information (PHI) to tracking technology vendors or any other violations of the HIPAA Rules.**"

Beyond the health privacy issues for providers and vendors, this Bulletin brings to mind several topics we discussed in an October post on Amazon's recent acquisitions (including the potential strategic value of One Medical, "a human-centered and technology-powered primary care organization). Under 45 CFR 160.103, a "covered entity" is a health plan, a health care provider, or a health care clearinghouse. Thus, as a primary care organization, One Medical falls under the category of a HIPAA-covered entity and is within this data-valuable environment where the OCR issued the Bulletin on PHI disclosed to tracking technology vendors.

Overview of the OCR Bulletin

PHI. The OCR reiterates throughout the Bulletin that HIPAA applies when covered entities collect user data that include PHI via tracking technologies and also if such data is then shared with technology vendors. But what exactly is PHI? As the Bulletin explains, PHI would include "individually identifiable health information" (IIHI), such as an individual's medical record number, home or email address, or appointment dates, as well as an individual's IP address or geolocation, medical device ID, or any unique online or mobile identifying code. The Bulletin stresses that "IIHI collected on a regulated entity's website or mobile app generally is PHI," even if the user does not have an existing relationship with the covered entity and even if the IIHI does not include specific treatment or billing information (e.g., appointment dates or type of healthcare services).

User-Authenticated Webpages. Patient portals and telehealth platforms generally collect and have access to PHI, including diagnosis and treatment information, billing information and other sensitive data. Therefore, the Bulletin states that a covered entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to only use and disclose (and secure) PHI in compliance with HIPAA. The OCR also reminds covered entities that tracking technology vendors are business associates IF they create, receive, maintain, or transmit PHI on behalf of a regulated entity "for a covered function (*e.g.,* health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI." For example, this can come into play in the case of authenticated portals where users log in to a medical provider's website or app. The Bulletin states that if an individual makes a medical appointment through the website of a covered health clinic and that website uses third party tracking technologies (which might automatically transfer PHI and other consumer data to an outside vendor), then the tracking technology vendor is a business associate and a business associate agreement (BAA) is required.

Unauthenticated Webpages. The OCR takes a slightly different stance on the collection of consumer data on unauthenticated webpages, which are publicly available pages that allow anyone to access the content and typically only contain basic information about a covered entity; as a result, and according to the Bulletin, tracking on such webpages is generally not regulated under HIPAA. However, the OCR states that in some cases, tracking technologies on such unauthenticated webpages may have access to user PHI and may disclose such data to outside vendors, thus triggering the HIPAA Rules. For example, the Bulletin mentions that if a login page of a covered entity's patient portal requires a user to enter registration information such as one's name and/or email address, such webpage then contains PHI and becomes subject to HIPAA. Alternatively, the OCR points to webpages that allow users to search for doctors, view appointment availability or make appointments, or view information about specific symptoms or conditions (e.g., pregnancy) without first logging in and warn that such webpages could potentially collect an individual's email address and/or IP address, thereby potentially disclosing PHI to the tracking technology vendor, and thus triggering the HIPAA Rules.

Mobile Tracking. Mobile tracking often occurs when tracking technologies and mobile software development kits (SDKs) are developed by an outside marketer and embedded in a mobile app. The Bulletin states that information typed in by a user, as well as device-level data (e.g., network location, geolocation, device ID, advertising ID, etc.) collected by a covered entity must comply with HIPAA for any PHI the mobile app uses or discloses. In a nod to the Supreme Court's *Dobbs* decision, the Bulletin states that HIPAA applies to "any PHI collected by a covered health clinic through the clinic's mobile app used by patients to track health-related variables associated with pregnancy…." However, the Bulletin clarifies that the HIPAA Rules do not protect data that users voluntarily enter into "mobile apps that are **not** developed or offered by or on behalf of regulated entities, regardless of where the information came from." [emphasis added]. This would include health information entered into lifestyle- or fitness-related mobile apps operated by an entity not regulated by HIPAA. Though, such data collection would still be regulated by the FTC and potentially under applicable state privacy laws, and perhaps even a comprehensive federal privacy law, if one should ever pass Congress.

Compliance Obligations. The Bulletin restates that regulated entities are required to comply with the HIPAA Rules when using tracking technologies and reminds covered entities to ensure that "all disclosures of PHI to tracking technology vendors are specifically permitted by the Privacy Rule and that, unless an exception applies, only the minimum necessary PHI to achieve the intended purpose is disclosed." It also suggested that regulated entities "should evaluate its relationship with a tracking technology vendor to determine whether such vendor meets the definition of a business associate and ensure that the disclosures made to such vendor are permitted by the Privacy Rule." The OCR closes the Bulletin with a few compliance reminders:

- The HIPAA Privacy Rule does not permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals of this possibility or occurrence in its privacy policy or privacy notice ("Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI").
- The use of cookie consent banners does not constitute a valid HIPAA authorization to a vendor when PHI is being collected, disclosed, used, or stored with the vendor.
- It is insufficient for a technology vendor to agree to remove PHI from the information it receives or de-identify PHI before the vendor saves the information ("Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place and requires that there is an applicable Privacy Rule permission for disclosure").

In addition to the Bulletin, technology and health care companies that are collecting health data should also ensure that they are complying with state privacy and consumer protection laws. HIPAA has often been described as the floor for health care privacy compliance and states may choose to pass and enforce more onerous privacy and consumer protection laws.

View original.