THOMAS D. BIXBY
LAW OFFICE LLC

LEGAL ADVICE FOR HEALTH PLANS

PRIVACY LAW ALERT
December 5, 2022

HIPAA Applies to Website, Mobile App Tracking Technologies

Cookies, Web Beacons, and Other Common Technologies Subject to Rules

Last week, the Department of Health and Human Services Office for Civil Rights (OCR) issued a bulletin reminding covered entities and business associates that "tracking technologies" commonly used on websites and in mobile phone apps often implicate HIPAA Privacy, Security, and Breach Notification Rules. Tracking technologies include, for example, cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts. When a covered entity (or its business associate) (referred to as a "regulated entity" in the Bulletin) uses tracking technologies that collect and track protected health information, the practice, including any resulting uses or disclosures of the tracking information, is subject to HIPAA. And any tracking-technology vendor that the regulated entity permits to access such information is a business associate that must be subject to a business associate agreement.

The Bulletin is available on the OCR's website (click here).

The OCR asserts that "tracking technologies on a regulated entity's user-authenticated webpages [*e.g.*, a member portal] will generally have access to PHI," such as an individual's IP address, e-mail address, "or other identifying information that the individual may provide when interacting with the webpage." Thus, according to OCR, a regulated entity "must configure any user-authenticated webpages [*e.g.*, member portals] that include tracking technologies to allow such technologies to ***only*** use and disclose PHI in compliance with the HIPAA Privacy Rule [and comply with the Security Rule]." (Emphasis in original.)

Moreover, OCR emphasizes that HIPAA often may apply to tracking technology practices used on a regulated entity's public facing webpages. Specifically, for example, OCR indicates that "the login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page)," may implicate HIPAA because the patient needs to provide credentials (*e.g.*, name, e-mail address) to access the portal and "such information is PHI." OCR therefore concludes that HIPAA will apply to tracking technology practices on a regulated entity's public-facing website if tracking technologies collect information from (or about) the portal login page. The OCR also suggests that other public-facing webpages, (*e.g.*, provider directories) could implicate HIPAA "in certain circumstances."

Similarly, the Bulletin warns that mobile apps offered by regulated entities:

> "collect a variety of information provided by the app user, including information typed or uploaded into the app, as well as information provided by the app user's device, such as fingerprints, network location, geolocation, device ID, or advertising ID. Such information collected by a regulated entity's mobile app is PHI, and thus the [covered entity or business associate] must comply with the HIPAA Rules for any PHI that the mobile app uses or discloses, including any subsequent disclosures to the mobile app vendor, tracking technology vendor, or any other third party who receives such information."

The OCR concludes by emphasizing that, among other things:

- The terms of use and privacy policy for a website or mobile app are not a substitute for complying with HIPAA requirements;
- "Banners that ask users to accept or reject a website's use of tracking technologies" do not qualify as a HIPAA authorization;
- Tracking technology vendors that access protected health information must be subject to business associate agreements; and
- A covered entity's (or business associate's) periodic HIPAA Security Rule risk assessment should evaluate these tracking technology practices.

* * * * * * * * * * *

For more information, please contact Tom Bixby at (608) 661-4310 or TBixby@tbixbylaw.com