ECKERT SEAMANS ATTORNEYS AT LAW

December 13, 2022

Data Privacy & Security Update

New HIPAA Guidance Regarding Website and Other Tracking Technologies

By Sandra R. Mihok and Emma M. Lombard

On December 1, 2022, the Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS") issued a bulletin warning covered entities and business associates ("regulated entities") that the use of online tracking technologies may violate the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy, Security, and Breach Notification Rules ("HIPAA Rules"). OCR's bulletin is intended to clarify that regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors. Even when a business associate agreement is n place, OCR cautions that tracking technologies may not be used in a manner or for a purpose which violates HIPAA.

The bulletin has been issued in response to recent reports that Meta Pixel tracking code has been employed on the websites of hospitals and that the tracking code transferred data to Meta, including HIPAA-regulated protected health information.

What Are Tracking Technologies?

Though they may take many different forms, tracking technologies collect information from users as they interact with websites or mobile applications ("apps"). Examples of tracking technologies on websites include cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts. Tracking technologies are also often embedded within mobile apps, collecting information directly provided by the user or capturing information from the user's mobile device, such as a device ID.

After information is gathered through tracking technologies, it can be analyzed in a variety of purposes, for example to analyze data to improve care or patient experience. Other times, tracking technologies are used to create user profiles or even for marketing purposes. Some of these purposes may violate the HIPAA rules.

How HIPAA Applies to Tracking Technologies

Regulated entities using tracking technologies inherently disclose individually identifiable information to third party vendors. This information may include what is traditionally considered protected health information ("PHI") like an individual's contact information, medical record number, or appointment dates, but may also include an individual's IP address or geographic location, medical device ID, or any unique identifying code, all of which OCR clarifies also constitutes PHI. Even where the individual has no preexisting relationship with the regulated entity, the data still qualifies as PHI because the information collected connects the user to the regulated entity. From this, it can be inferred that the individual has received or will receive health care services or benefits from the covered entity, rendering the information provided "related" to the individual's past, present, or future health care or payment for care.

What Regulated Entities Can Do to Comply

To ensure compliance with the HIPAA Rules, a regulated entity should consider whether a technology tracking vendor (including, for example Google and MetaPixel) has a legitimate purpose as a business associate for its collection of identifiable information such that a business associate agreement should be in place. OCR explains a covered entity's obligations by distinguishing between three destinations where tracking technologies may be used, all of which presuppose that a permissible reason for the disclosure exists:

- User-authenticated webpages are those that require a user to log in before they can access a webpage, and which routinely contain PHI, such as a patient portal or a telehealth platform. If a regulated entity uses third party tracking technologies on user-authenticated webpages, it should enter into a BAA with any tracking technology vendor who qualifies as a business associate.
- On unauthenticated webpages, which are those that do not require users to log in prior to accessing and generally do not contain PHI, a regulated entity still must assess its use of tracking technologies, and would be required to enter into a BAA with a vendor who qualifies as a business associate under the following non-exhaustive circumstances:
    - Where tracking technologies on a regulated entity's patient portal login page or registration page collect an individual's login information or registration information prior to logging in;
    - Where tracking technologies could collect an individual's email address and/or IP address when searching for available appointments with a health care provider; or
    - Where tracking technologies could collect an individual's email address and/or IP address when visiting webpages that address specific symptoms or health conditions.

When a regulated entity lacks either business associate agreement with a vendor or a permissible use for the disclosure, or if a vendor does not qualify as a business associate, a regulated entity must obtain HIPAA-compliant authorizations prior to making any disclosure of PHI to that vendor. OCR confirms that website banners prompting users to "accept" or "reject" the use of tracking technologies like cookies do not constitute valid HIPAA authorizations. It is similarly insufficient for a vendor to agree to de-identify any PHI it receives prior to saving the information.

OCR encourages regulated entities to identify the use of tracking technologies within their website or mobile app's privacy policy, notice, or terms and conditions of use; to incorporate the use of tracking technologies in their HIPAA risk management process.

ECKERT SEAMANS ATTORNEYS AT LAW

This Data Security & Privacy Alert is intended to keep readers current on developments in the law. It is not intended to be legal advice. If you have any questions, please contact Sandra R. Mihok at 412.566.1903 or smihok@eckertseamans.com, Emma M. Lombard at 609.989.5024 or elombard@eckertseamans.com, or any other attorney at Eckert Seamans with whom you have been working.