Published on *The National Law Review* https://natlawreview.com

Is Your Website Collecting PHI Under OCR's New Tracking Technologies Bulletin?

Article By:

Dianne J. Bourque

Lara D. Compton

Kathryn F. Edgerton

Cassandra L. Paolillo

Kate F. Stewart

Covered Entities and Business Associates should promptly and carefully review their use of online tracking technologies on their websites and mobile apps following a bulletin (Bulletin) published by the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) on December 1, 2022. The Bulletin addresses multiple facets of compliance with HIPAA when using online third-party tracking technologies (Tracking Technologies). In doing so, OCR significantly expands its interpretation of the definition of Protected Health Information (PHI) to include, in some instances, identifiable information gathered by Tracking Technologies where a user visits a website and does not interact with the entity in any other way. In its Bulletin, OCR interprets the act of an individual visiting a website as evidence of a relationship or anticipated future relationship between the visitor and the entity.

The Bulletin was seemingly prompted by recent news articles that describe entities subject to HIPAA (Regulated Entities) sharing patient appointment information (including information about reproductive health services) with social media companies by using tracking pixels and other technologies. OCR also appears to be responding to concerns about the privacy of reproductive health information in the wake of the *Dobbs vs. Jackson Women's Health Organization* decision (see our prior coverage of privacy issues post-*Dobbs* here and here). In the Bulletin, several of the provided examples specifically address reproductive health information.

The reports related to the sharing of patient appointment information using tracking pixels implicated the use of Tracking Technologies by a number of hospitals, leading to several breach notifications for patients whose information Tracking Technologies may have compromised and, subsequently, to class action lawsuits. While these incidents related to the use of Tracking Technologies on password-protected patient portals, the Bulletin indicates that a Regulated Entity may be collecting PHI when it

uses Tracking Technologies on websites that do not require any user authentication. OCR takes the position that this can be the case regardless of whether an established relationship exists between the Regulated Entity and the individuals using a website or mobile app. This broad interpretation of the scope of PHI has significant implications for complying with HIPAA privacy, security, and breach notification requirements. Notably, the Bulletin does not have the force and effect of law and was not subject to notice and comment rulemaking. However, Regulated Entities should be aware that the Bulletin represents OCR's current position on the issue of Tracking Technologies.

Tracking Technologies and the Definition of PHI

Tracking Technologies involve the use of a script or code (e.g., cookies, tracking pixels and codes, fingerprinting scripts, web beacons) on a website or mobile app to gather information about users as they interact with the website or mobile app. These Tracking Technologies are ubiquitous on webpages and help drive targeted ads (including banner and social media ads), including ads for the products and services of a business with which a user has interacted, as well as products and services from similar businesses.

In the Bulletin, OCR takes the position that all individually identifiable health information (IIHI) collected on a Regulated Entity's website or by its 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." In taking this stance, OCR transforms information that many had assumed to be personal information subject to general privacy controls (including a website privacy policy) into individually identifiable health information. Pursuant to the HIPAA regulations, IIHI must "relate to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." OCR posits that in collecting information through its website, a Regulated Entity "connects" the website visitor to the Regulated Entity and is therefore "indicative that the individual has received or will receive health care services or benefits from the covered entity." While this interpretation is well intentioned given the privacy concerns raised by tracking website activity post-Dobbs, in practice it will extend the definition of PHI to include information that may not actually relate to any health care needs of the individual visiting a website.

Tracking Technologies on User Authenticated Pages

Unsurprisingly, OCR takes the position in the Bulletin that Tracking Technologies on user-authenticated webpages (Authenticated Pages) require the Regulated Entity and any Tracking Technology vendor to comply with HIPAA in handling the information gathered by the Tracking Technology. An Authenticated Page is a webpage that requires the user to log in before accessing content and includes provider patient portals, health plan beneficiary portals, and telehealth platforms. OCR states that generally Tracking Technologies on Authenticated Pages would have access to PHI, such as an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage (which in some cases may include individuals' diagnosis and treatment information, prescription information, billing information, or other information within the portal). OCR does not discuss the exceptions to this general rule, nor does the Bulletin provide any actionable guidance regarding proper configuration of Authenticated Pages using Tracking Technologies.

Tracking Technologies on Unauthenticated Pages

Contrary to the understanding of many, OCR takes the position that Tracking Technologies on Regulated Entities' unauthenticated webpages (Unauthenticated Pages) are collecting PHI in certain cases and that such information is subject to the requirements of HIPAA. An Unauthenticated Page is a webpage that does not require the user to log in before accessing content and may include some provider website landing pages and telehealth platform provider search pages. OCR provides the following examples of Unauthenticated Pages where a Tracking Technology would capture PHI by virtue of collecting individually identifiable information:

- Login pages of a patient portal or a user registration webpage where an individual creates a login for the patient portal; if the individual enters credential information on that login webpage or enters registration information (e.g., name, email address) on that registration page, such information is PHI that could be collected by Tracking Technologies.

- Webpages of Regulated Entities that address specific symptoms or health conditions, such as pregnancy or miscarriage.

- Webpages of Regulated Entities where users can search for a provider or schedule an appointment, even if the page does not require a log-in to perform the search.

While OCR appears to distinguish a general home page for a multi-specialty provider offering information about the provider's location and services (where tracking the IP addresses visiting the site would not constitute the collection and sharing of PHI) and condition or symptom-specific pages (where OCR indicates the tracking of IP addresses visiting the site would constitute the collection and sharing of PHI), it does not offer any guidance related to the homepages of single-specialty providers or providers that treat a single (or a handful of related) conditions. Nor does OCR provide guidance on when, in OCR's interpretation, a webpage's information is so specific to a symptom or health condition that information collected by a Tracking Technology on that page is PHI.

Mobile App Information

Also, the Bulletin addresses Tracking Technologies used in mobile apps but does not break new ground in this area. OCR reiterates that the information provided by the app user or collected by the app (including fingerprints, network location, device ID, or advertising ID) is PHI and subject to HIPAA.

Compliance Obligations

As discussed above, a significant amount of information collected by Regulated Entities through Tracking Technologies may be subject to HIPAA, especially given OCR's expansive view of when website user data constitutes PHI. To the extent Tracking Technology on a webpage or mobile app has access to PHI, the use of the Tracking Technology must be HIPAA-compliant. Disclosures of the PHI that result from the use of Tracking Technologies, including vendors, must comply with the Privacy Rule. Tracking Technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of Regulated Entities in connection with the services they provide and a business associate agreement (BAA) must be put into place with such vendors. Notably, the Bulletin also provides the following clarifications and reminders:

- Describing the use of Tracking Technologies in a website's or mobile app's privacy policy, notice, or terms and conditions of use is insufficient for meeting HIPAA obligations.

- Marketing uses of PHI collected through Tracking Technologies must be authorized in accordance with HIPAA (or fall within an exception) and website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do not constitute a valid HIPAA authorization for marketing purposes.

- De-identification of PHI by a Tracking Technology vendor prior to saving it does not change the vendor's status as a business associate.

- Unless an exception applies, only the minimum amount of PHI necessary to achieve an intended purpose (which must be permitted under the Privacy Rule) may be disclosed to technology vendors.

- When performing a HIPAA security risk assessment, the use of Tracking Technologies must be evaluated and the Regulated Entity should ensure that appropriate safeguards are in place to address security risks from Tracking Technologies.

- The disclosure of PHI to Tracking Technology vendors without a BAA in place may constitute a breach under HIPAA and any such disclosure must be analyzed under the four-factor "low probability of harm" standard.

Recommended Next Steps

We recommend that all Regulated Entities perform data mapping to understand the data collected from websites and apps and identify the PHI (as described under the Bulletin) collected through Tracking Technologies. Regulated Entities should evaluate the use, disclosure, and security of such PHI for HIPAA compliance and should address any compliance gaps. As part of this process, Regulated Entities should pay careful attention to the following:

- Whether identifying information collected from individuals via websites and mobile apps is PHI, keeping in mind OCR's position in the Bulletin that an existing relationship with the individual is not necessarily required.

- What identifiable health information can be inferred by the data collected using Tracking Technologies, and whether that information will be shared with third parties (e.g., vendors) given that the types of information viewed can create health related inferences that OCR could consider PHI.

- What information is shared with Tracking Technology vendors and whether HIPAA compliance is required in making such disclosures. To the extent the use of Tracking Technologies may have resulted in unauthorized disclosure of PHI to third parties, Regulated Entities should consult counsel for purposes of evaluating breach reporting obligations.

- Whether any information that is collected by Tracking Technologies is used for marketing purposes or sold to third parties and to what extent that information is PHI requiring a HIPAA authorization for such activities.

- Whether BAAs are required with Tracking Technology vendors.
- Whether use of Tracking Technologies involving PHI were evaluated as part of the Regulated Entity's HIPAA security risk assessment.

OCR's expansive view of PHI, as articulated in the Bulletin, may make it difficult for some Regulated Entities to ascertain their actual HIPAA compliance obligations when undertaking any of the above-listed measures. We will continue to monitor for any additional guidance from OCR.

National Law Review, Volumess XII, Number 341