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

HHS-OCR Guidance for Online Tracking Technologies

Article By:

Colin H. Black

Iliana L. Peters

The continued proliferation of tracking technologies has created a landscape of increased exposure for entities serving individuals online. As individuals are increasingly interacting with healthcare services providers online, the Department of Health & Human Services ("HHS") Office for Civil Rights ("OCR") has issued new guidance for regulated entities to address privacy concerns stemming from the use of tracking technologies.

While the guidance does not necessarily clarify which technologies meet the definition of tracking technology, OCR clarifies that tracking technologies include applications used to gather information about users' interactions with websites, which is then analyzed to create insights about users and their online activities. While the definition is not exhaustive, it specifically includes cookies, web beacons or tracking pixels, session replay scripts and fingerprinting scripts.

OCR further clarifies that "Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosure of PHI to tracking technology vendors or any other violations of the HIPAA Rules."[1]

As a threshold matter, the scope of the guidance is limited to entities covered by HIPAA and their business associates (together, "Regulated Entities"). Similarly, the guidance is limited only to information that meets the definition of Protected Health Information ("PHI") under HIPAA.

While the definition of PHI is exceedingly broad, it is not all-encompassing. To be classified as PHI, the information must be reasonably able to identify the individual, be created or received by a Regulated Entity, and relate to the condition, provision of, or payment for health care of an individual. Accordingly, information that is sufficiently de-identified per the HIPAA Privacy Rule's requirements or that cannot reasonably be associated with healthcare is arguably outside the scope of the guidance.

Further, the guidance distinguishes between web services that require authentication. In instances where authentication is required, OCR notes that tracking technologies on a user-authenticated webpage will generally have access to PHI, and accordingly, that the use of tracking technologies on user-authenticated pages will likely violate the HIPAA Privacy Rule. By contrast, if unauthenticated web pages do not generate PHI, they may but outside the scope of the guidance, except that OCR

states that PHI would be at issue in many unauthenticated websites, including a webpage “that addresses specific symptoms or health conditions…or that permits individuals to search for doctors or schedule appointments.”

Finally, the use of the collected data implicates an entity’s relative exposure. For example, we continue to see an explosive growth in litigation and investigations by OCR and State Attorneys General arising out of the use of website tracking tools, including session replay, chatbots, and pixel technologies being framed as “wiretapping” by class-action plaintiffs’ counsel. In essence, plaintiffs’ attorneys and these regulators argue that the use of these technologies to collect PHI, including IP addresses, dates of interaction, and other website identifiers, may be an impermissible disclosure of PHI under the HIPAA Privacy Rule, and a “breach” as defined by the HIPAA Breach Notification Rule and state law.

Accordingly, Regulated Entities must engage in a detailed analysis of what data is collected by any website tracking tools, whether that data can reasonably be considered “PHI” under HIPAA, and whether the use of this data could be construed as an impermissible use or disclosure under the HIPAA regulations. This exercise should include an analysis of the types of technologies utilized to collect information, the specific domains and subdomains where these technologies are used, as well as the historical and persistent nature of the data collected.

In practice, organizations can mitigate their exposure by restricting the use of tracking technologies and, to the extent that such technologies are utilized, by taking effective measures to de-identify the data such that it falls outside the scope of the definition of PHI. To the extent that PHI exists online, it should arguably be secured by authentication and shielded from impermissible use or disclosure. Similarly, organizations should consider means to “sever” identifying information (such as session tokens, IP addresses, geolocation hop data, and similar) from tracking technologies, particularly where these technologies are critical for the functionality of the platform.

Finally, organizations can greatly mitigate their exposure by entering into business associate agreements governing the use and disclosure of PHI with third-parties that provide services online or confirming the HIPAA authorization of individuals before PHI is shared with these parties.

[1] The Guidance points out that entities and activities outside this scope may still be subject to regulatory oversight and intervention by the Federal Trade Commission and other regulators.

National Law Review, Volume XIII, Number 18