DECEMBER 8, 2022

For more information, contact:

Marisa Maleck
+1 202 626 9117
mmaleck@kslaw.com

Adam Solander
+1 202 626 5542
asolander@kslaw.com

Robert Hudock
+1 202 626 5521
rhudock@kslaw.com

Igor Gorlach
+1 713 276 7326
igorlach@kslaw.com

Kasey Ashford
+1 202 600 1107
kashford@kslaw.com

Hunter McGhee
+1 404 572 4612
hmcghee@kslaw.com

King & Spalding

# HHS Office for Civil Rights Issues Guidance Regarding HIPAA Requirements for Online Tracking Technologies

On December 1, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services provided guidance on the intersection of the Health Insurance Portability and Accountability Act (HIPAA) and the use of online tracking technologies. These technologies (sometimes called cookies, pixels, and web beacons) track user interactions with websites, collect and analyze information about those interactions, and send that information to third parties (generally for analytics or advertising purposes).

OCR notes that the use of this tracking technology may result in the impermissible disclosure of Protected Health Information (PHI)[1] from a healthcare provider's website to advertisers. OCR makes clear that covered entities under 45 C.F.R. 160.103 "are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors." Generally, disclosure of an individual's PHI without their HIPAA-compliant authorization (other than for treatment, payment, or healthcare operations and a few additional statutorily-specified purposes) would constitute an impermissible disclosure and violation of HIPAA's Privacy Rule, which could result in the need to report to OCR or monetary penalties (civil and sometimes criminal).

For user-authenticated pages—i.e., for pages where the user must log in to access the site—a provider generally must ensure that any trackers comply with the HIPAA Privacy Rule and Security Rule as data sent from these pages will almost certainly constitute PHI. OCR considers tracking technology vendors as business associates of the providers if such vendors "create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function" or provide certain services involving the disclosure of PHI. According to OCR, providers must ensure the disclosures made to tracking vendors are permitted by HIPAA's Privacy Rule and enter into a business associate agreement (BAA) if the vendor is a business

associate. Importantly, several major vendors providing tracking services generally will not enter a BAA when providing such services. The result is that many tracking technologies on user-authenticated pages will run afoul of HIPAA's rules under the guidance.

For non-authenticated pages—i.e., for pages where users do not have to log in—HIPAA rules apply where tracking technologies have access to PHI. For instance, if a person enters her login credentials (such as name and email) on a user registration webpage to create a login for a patient portal, this is considered PHI and HIPAA rules apply to the use of tracking technology. Tracking technology that collects an individual's email address or IP address when she searches for an available appointment on the provider's website also falls under HIPAA's regulations. In both instances, OCR says that the HIPAA Security Rule and Privacy Rule apply.

For individual interactions through a provider's mobile app, such as a person using a provider's app to track her menstrual cycle, body temperature, or store her prescription information, the same rules apply. OCR also notes that the PHI collected through an app is potentially broader than that collected on a website, including information typed or uploaded into the app and information provided by the user's device, such as fingerprints, network location, geolocation, device ID, or advertising ID.

In short, OCR's guidance means many if not most covered entities utilizing tracking technologies are potentially violating the HIPAA Privacy Rule. Under the HIPAA Privacy Rule, covered entities must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individuals' HIPAA-compliant authorizations are required before the PHI is disclosed to the vendor. Notice in a privacy policy or a provider's terms and conditions, or the use of website banners asking visitors to accept or reject the use of tracking technology, is insufficient. It is also insufficient for a tracking technology vendor to agree to remove or de-identify the PHI it receives.

The OCR bulletin clarifies that any BAA with a tracking vendor that is a business associate must meet the regulatory requirements for BAAs. The BAA must specify how a vendor is permitted to use or disclose PHI and require the vendor to safeguard the PHI. The vendor must report any security incidents including breaches of unsecured PHI to the regulated entity.

While OCR's guidance provides much needed clarity, it still leaves many questions unanswered. Generally, the Privacy Rule requires the reporting of "breaches," i.e., an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. The guidance does not address in detail how a four-factor risk assessment analysis to determine whether an incident is a breach is affected when tracking technology has been turned off and third parties have not retained the PHI.

Nor does this guidance directly address a situation in which "obfuscated" elements of PHI are sent. What is not clear is whether a "breach" occurs if a covered entity "discloses" through technology a visitor's actions on a public ("non-authenticated") portion of a health care provider's website if it somehow "obfuscates" that action. Consider a hospital that shares the IP address and a generic "event" name ("Event 1") when a user logs in but not the log in credentials themselves. The guidance says that while login or user registration webpages "generally are unauthenticated because the individual did not provide credentials to be able to navigate to those webpages," "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." OCR thus takes the position that "if tracking technologies on a regulated entity's patient portal login page or registration page collect an individual's login information or registration information, that information is PHI and is protected by the HIPAA Rules." The guidance is silent, however, as to whether the "obfuscated" login or

registration information (i.e., as donated by the "event" name "Event 1") is protected PHI versus just the actual login or registration information.

The use of tracking technology has recently increased, and OCR's specific guidance on the issue shows it is an area of focus for the enforcement of HIPAA. Regulated entities should review the use of tracking technologies both on their webpages and on any mobile apps. If the provider uses tracking technology, it should ensure it enters into a BAA with the business associate vendor or alternatively seek individual authorization for disclosure of PHI from each user.

## ABOUT KING & SPALDING'S DATA, PRIVACY AND SECURITY PRACTICE

The firm's Data, Privacy and Security practice includes over 80 lawyers and professionals based in many of the firm's offices and encompasses global data protection legal issues faced by multinational organizations, including data protection, crisis management in responding to internal and external data, privacy and security incidents, information governance and compliance, and defending clients in enforcement proceedings and litigation. We are "boots on the ground" crisis managers, deploying our incident response team, when needed, to manage the fast-moving logistics and coordinate across work streams during the initial hours and days of a privacy or security incident.

The firm's practice has substantial experience with the technology at the heart of OCR's guidance. The firm is unique in its ability to employ forensic tools to easily determine whether and where this technology resides on websites and has substantial experience in advising legal departments, IT specialists, and marketing departments about how to use this technology within the bounds of the rules. The firm also has substantial experience handling inquiries from OCR, state Attorneys General, and the Federal Trade Commission about the use of this technology.



[1] PHI includes, among other things, an individual's medical record number, home address, email address, dates of appointments, IP address, geographic location, medical device IDs, and unique identifying codes, even if the IP address or geographic location is not connected to specific healthcare services.