HHS-OCR Cautions Health Care Providers to Confirm their Websites and Apps are HIPAA-Compliant

Bridget Steele, Barclay Damon LLP

On December 1, 2022, the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued a bulletin to clarify existing requirements regarding the use of third-party tracking technologies on websites and mobile apps in accordance with the HIPAA Privacy, Security, and Breach Notification Rules (the "HIPAA Rules"), which apply to regulated entities—covered entities and their business associates. The OCR bulletin cautioned providers to check use of these tracking technologies on their websites and mobile apps to ensure they are not inadvertently violating HIPAA.

OCR explained that a "tracking technology" is generally a script or code on a website or mobile app that collects information and tracks users. Websites typically use cookies, web beacons or tracking pixels, session replay and fingerprinting scripts. Mobile apps typically collect information entered directly by the user and may also collect information from the user's mobile device.

Many websites run by covered entities (e.g. health care providers) contain or are functionally connected to a web analytics service operated by a third-party vendor. This service may track the user's activity by collecting the user's IP address or mobile device identifier. Some entities might not view an IP address, in and of itself, as ePHI. However, OCR explained in its guidance that this information can be ePHI because, when a covered entity collects this information through its website, the information may connect the individual to the covered entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity) and, thus, relates to the individual's past, present, or future health, health care, or payment for care. The American Hospital Association recently sent a letter to OCR urging them to back off their interpretation in the bulletin as being too broad, but OCR has not yet responded.

Because use of tracking technologies has become widespread, OCR has urged regulated entities to review their websites and mobile apps to ensure they collect information in a HIPAA-compliant manner. For example, if an individual makes an appointment through the website for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, OCR indicates the tracking technology vendor is a business associate and a BAA is required because the vendor is receiving, maintaining, or transmitting PHI on behalf of the entity for a covered function (e.g., health care operations) or services that involve the disclosure of PHI.

In addition, providers' compliance and IT teams should understand what tracking technologies are used and what types of data are collected and shared on their public-facing websites and mobile apps. In the event HIPAA applies to the information collected, then appropriate BAAs need to be in place, data should be collected securely in accordance with the HIPAA Rules, and any applicable website or app privacy policy needs to be consistent with requirements under HIPAA.

Bridget Steele, JD
Counsel
Barclay Damon LLP

About the Speaker

Bridget Steele is counsel at Barclay Damon LLP in the Health Care & Human Services and Data Security & Technology Practice Areas. Bridget assists health care and human service providers with regulatory and compliance matters, including audits and investigations, self-disclosures, not-for-profit corporate governance, contract analysis and negotiation, and transactional matters. Bridget also regularly assists health care clients with HIPAA and health information privacy and security compliance, responding to and reporting data breaches and cybersecurity incidents, and negotiating health care IT contracts.