Scrutiny of Online Tracking Technologies Continues

Insights 07.24.23

On July 20, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) sent a joint letter to approximately 130 hospital systems and telehealth providers to emphasize the agencies' position that the use of online tracking technologies on websites or mobile apps involves "serious privacy and security risks." In particular, OCR and FTC note that tracking technologies, such as the Meta/Facebook pixel and Google Analytics, create risk as they gather identifiable information about users that interact with a website or app (such as IP addresses), potentially resulting in impermissible disclosures of an individual's personal health information. Notably, in addition to sending this letter, OCR and FTC also announced the distribution of this letter publicly, presumably as notice to the industry at large.

PROFESSIONAL

ANDREA FREY
Partner
San Francisco
San Diego

STEPHEN K. PHILLIPS
Partner
San Francisco

PAUL T. SMITH
Of Counsel
San Francisco

The joint letter follows prior warnings and guidance issued by both agencies in recent months, indicating heightened scrutiny of health systems and telehealth providers over uses and disclosures of individually-identifiable information gathered by online tracking technologies.

OCR issued a bulletin in late 2022 identifying the risks related to use of tracking technologies for covered entities and business associates under the Health Information Portability and Accountability Act of 1996 (HIPAA). The bulletin flags risks of such technologies, whether on a website where the user whose information is gathered is logged in (such as a patient on a telehealth platform or a patient scheduling an appointment on a clinic's website), or on a mobile app that collects information provided by the user's device, such as geolocation. Though OCR acknowledges that tracking technologies on "unauthenticated webpages" – meaning webpages that do not require users to log in – generally do not have access to protected health information (PHI), OCR also states that is not always the case. Examples include webpages that address specific symptoms or health conditions, or that permit individuals to search for doctors or schedule appointments without entering credentials, may have access to PHI, such as due to collection of an IP address.

Many view OCR's position as aggressive, if not going too far, with respect to this last category. For example, it is very possible that a person browsing the website is doing just that – browsing – to learn more about a particular provider or health condition, whether for market research, for a friend, to learn more about the provider when applying for a job, or numerous other reasons, where an IP address does not reliably disclose anything about the visitor's physical or mental

health status. Nevertheless, OCR has taken this position and does not appear to be wavering since first issuing this bulletin last year.

Separately, the FTC has also been significantly stepping up its enforcement activity in the health care industry, as well as engaging in rulemaking to further emphasize that its scope of authority under the FTC Health Breach Notification Rule (HBNR) extends to health care and wellness websites and mobile apps. For more information, see our recent article about the FTC's proposed amendments to the rule and increased scrutiny of digital health and wellness companies here.

Of course, neither HIPAA nor the HBNR prevent regulated entities from building internal capabilities to track visits to its own web site. Further, neither prevent regulated entities from engaging a third party service vendor to assist with tracking and reporting of web site activity, as long as a business associate agreement (BAA) is in place with the vendor or the patient has authorized the disclosure of their information to the tracking vendors if the tracking involves PHI. However, these options may not always be practically or even logistically possible for regulated entities to obtain, particularly as many of the prominent tracking technology vendors refuse to enter into BAAs.

Importantly, mere disclosure of the use of such tracking technologies to individuals is insufficient under both HIPAA and the HBNR (as opposed to receipt of an authorization that comports with the HIPAA requirements or some form of consent from consumers under the HBNR[i]), if the tracking technology results in an impermissible disclosure of personal health information to third parties. In such instances, a risk assessment may be warranted to determine whether any of these impermissible disclosures constitute a reportable breach under either HIPAA or the HBNR, triggering potential notification requirements.

More broadly, complaints submitted to OCR in recent years have grown significantly – an increase of 69% between 2017 and 2022 – as recently noted by OCR as part of its announcement regarding a renaming of its Health Information Privacy Division to the Health Information Privacy, Data, and Cybersecurity Division. This uptick in number of complaints submitted potentially indicates that individuals are increasingly more concerned about the privacy and security of their health information.

Ultimately, given both OCR and the FTC's increased scrutiny of online tracking technologies, health care providers, digital health companies, and other health care industry stakeholders should review which tracking tools are currently being used across their online platforms, what information is being collected and disclosed by these tools, and whether reasonable privacy and data security measures are in place to protect such information.

For further information, please contact Amy Joseph in Boston, Andrea Frey, Stephen Phillips, or Paul Smith in San Francisco, or any other member of our Hooper, Lundy & Bookman team.

[i] In its proposed amendments to the HBNR, the FTC is seeking comment regarding how it should define "authorization" or "affirmative express consent" of an individual in connection with the disclosure of their information, including the acceptability of consent via clicking to "agree" or "accept" through a pre-checked box or agreeing to terms and conditions without being required to review such terms and conditions. However, for the proposed rule, the FTC declined to provide a definition at this time, on the basis that the agency believes prior commentary and enforcement actions make clear what satisfies the standard of "meaningful choice" from consumers and what would not amount to an authorized disclosure of personal health information.

RELATED CAPABILITIES

Digital Health

Health Information Privacy and Security

Hospitals and Health Systems