ALERTS | 12.02.2022

New OCR Bulletin Calls for Review of Website Tool Use by Covered Entities

As you may have seen, the HHS Office for Civil Rights ("OCR") issued new HIPAA Privacy Rule guidance on December 1, 2022 entitled, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates." You can find the bulletin here.

This bulletin marks the first time OCR has issued specific guidance on the use of website tracking/AdTech tools by covered entities and is an important development. We highlight below several aspects of the guidance that may warrant further review and analysis of your use of various website tools as you build out internal best practices, and further ensure regulatory compliance.

While we believe there may be multiple avenues, depending on the facts, by which one could defend against the enforcement of this OCR guidance, in the short run it may make sense to give additional thought to the following:

1. **OCR makes the assumption that someone sending Individually Identifiable Health Information ("IIHI") through a covered entity's website or mobile app is someone who "has received or will receive health care services or benefits from the covered entities."** We know, as a practical matter, that many visitors to hospital or other provider/insurer websites are not patients or future patients. They may be friends or family members of a patient, potential donors, individuals looking for general information, or job seekers. OCR, however, is starting from the position that use of such a website is an indicator that someone has received or is about to receive services from the covered entity. In other words, OCR's presumption is that HIPAA applies, and the information will be considered "Protected Health Information ("PHI"), even if the individual does not have an existing relationship" with the covered entity.
2. **OCR takes a broad view of the pages on a general informational website that implicate HIPAA.** While associating HIPAA requirements with pages such as a patient portal login page or user registration page may not be surprising, OCR states its view that webpages "that address[] specific symptoms or health conditions, such as pregnancy or miscarriage, or that permit[] individuals to search for doctors or schedule appointments [even] without entering credentials" implicate HIPAA. This means that OCR's current view is that the combination of a visitor's IP address with information about a specific clinician or type of service constitutes PHI and that covered entities my only allow website tools to convey that information to third parties with which it has a BAA in place, unless the website visitor has executed a HIPAA-compliant authorization.
3. **OCR takes the view that back-end anonymization or agreements to remove and not use PHI are legally inadequate.** The guidance states that the collection of IIHI by third-party tracking technology vendors would be a disclosure of PHI. Furthermore, OCR states that "it is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information."
4. **OCR states that privacy policies and cookie/tracker opt-outs also are insufficient.** The guidance makes clear that OCR will not permit the disclosure of PHI through website tools simply by informing users of the disclosure in the entity's privacy policy or notice, or by allowing users to opt-out of the use of these tools through a "cookie banner."
5. **OCR expects covered entities to have BAAs in place with tracking technology vendors or for covered entities to be able to demonstrate that the Privacy Rule permits the transmittal of PHI without the individual's authorization.** Absent one of these standards being met, OCR states that entities must provide a breach notification "unless the regulated entity can demonstrate that there is a low probability that the PHI has been compromised." This would require covered entities to prepare and hold a written analysis/opinion to provide to OCR upon request. Given that covered entities do not know who is using their website and many of these website visitors are not current or future patients, the concept of notifying website visitors of a potential breach is untenable if not completely impossible.

© 2026 Choate, Hall & Stewart LLP | Two International Place, Suite 3000 | Boston, MA 02110 | 617-248-5000

6. **OCR describes "tracking technology" broadly and in a manner that we assume would include services like Google Analytics, Hotjar and others, in addition to the Meta/Facebook Pixel which is called out by name.**

Our Healthcare and Government Enforcement & Compliance teams are well-versed in helping clients work through issues related to their use of website tools – both from a proactive compliance program enhancement perspective, and also in the face of civil litigation or government investigations. If you have questions about your institution's use of website tools, please reach out to your regular contact at Choate or one of the partners below.

Printable version.

Christine G. Savage
Co-Head of Government Enforcement & Compliance

Adam J. Bookbinder
Co-Head of Government Enforcement & Compliance