

Report on Patient Privacy Volume 24, Number 4. April 11, 2024 OCR Doubles Down on Pixel Ban, Offers Examples of Unlawfully Disclosed PHI

By Jane Anderson

The HHS Office for Civil Rights (OCR) is reiterating—with strong language—that HIPAA covered entities covered (CEs) should avoid using web tracking technologies in situations that could reveal protected health information (PHI) or risk violating HIPAA regulations. However, the new bulletin raises questions about when tracker use is permitted.

In the March 18 bulletin issued “to increase clarity for regulated entities and the public,” OCR updated its guidance on web-tracking technologies known as pixels, adding details and specific examples of what is—and is not—allowed.^[1]

“Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules,” OCR said in its bulletin. “For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.”

OCR also made it clear that it was prioritizing compliance with the HIPAA Security Rule in investigations into the use of online tracking technologies. “OCR’s principal interest in this area is ensuring that regulated entities have identified, assessed, and mitigated the risks to ePHI [electronic PHI] when using online tracking technologies and have implemented the Security Rule requirements to ensure the confidentiality, integrity, and availability of ePHI.”

The revisions published by OCR “provide new examples of what HIPAA permits and prohibits with respect to the use of online tracking technologies,” wrote Adam Greene and Rebecca Williams, attorneys with Davis Wright Tremaine LLP. “But these examples highlight a problem with the original guidance, as regulated entities may still find it impossible to distinguish between what is and is not a disclosure of protected health information (PHI) subject to HIPAA.”^[2]

Greene and Williams also said that prioritizing compliance within the HIPAA Security Rule is surprising because the guidance seems primarily focused on privacy issues. The focus on security indicates that covered organizations should prioritize verifying that the risk of impermissible PHI disclosures related to web tracking is addressed in risk analyses and risk management plans, they said.

Pixels from technology companies such as Alphabet Inc. (the parent company of Google) and Meta (the parent company of Facebook and Instagram) operate in the background on websites that have installed them, gathering details about medical conditions and other topics that website visitors may be researching on the site. The tracking devices also collect information about patients’ prescriptions and doctors’ appointments, delivering that data to third-party companies such as Facebook and Google.^[3]

Investigations in 2022 found that Meta Pixel and other pixels were installed on many or even most hospitals’ websites, although multiple health care entities have since removed them.

In December 2022, OCR first clarified that CEs and business associates (BAs) are not permitted to use the technologies “in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.”^[4]

The American Hospital Association has sued OCR over OCR’s position on tracking technologies, saying that the agency overreached.^[5] Since then, that lawsuit has drawn support from 17 state hospital associations and 30 hospitals and health systems.

This document is only available to subscribers. Please log in or purchase access.

[Purchase Login](#)