COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 33, Number 1. January 08, 2024
Website Tracker Issues Are Underrated HIPAA Risk, Experts Say

By Jane Anderson

Website tracking technologies on many health care organizations' websites are an under-appreciated HIPAA compliance risk and they should consider analyzing what trackers are lurking and take steps to ensure they're HIPAA compliant, experts say.

The HHS Office for Civil Rights (OCR) has signaled that the use of these trackers—little snippets of computer code present on many websites—is a high enforcement priority, Trisha Lee, senior consultant at BerryDunn, said at a Dec. 5 HCCA webinar.[1] "We know that many organizations have cybersecurity as their primary high risk to their organization, but tracking technology is well up there," Lee said.

Meta Pixel, Google Analytics and other similar trackers operate in the background on websites and collect user data—including personally identifiable data in many cases—when users visit websites that have the trackers embedded. The trackers can collect numerous metrics that provide beneficial insights for the owners of the websites.

However, they also can scoop up information about searches performed on websites and may, in certain cases, collect information about patients' prescriptions and doctors' appointments. Investigations have found that these trackers are installed on many—or even most—hospitals' websites. They sometimes are found inside patient portals, where patients have identified themselves by logging in.