The Growing Legal Risk of Online Tracking Technologies on Healthcare Websites

By Justin Joy, JD, CIPP

The use of website tracking technology, such as the Meta Pixel, in the healthcare industry continues to garner media attention. A prior Sentinel article in February 2023 provided information about the risk posed by website tracking technology, and a May 2023 article provided additional information on the topic, as well as guidance on mitigating this risk. This article focuses on how this risk has materialized into legal claims which class action plaintiffs are asserting against healthcare organizations across the country.

At least for now, the class action lawsuits are generally targeting hospitals and larger health systems. Many defendants in these lawsuits are settling the cases for millions of dollars.[1] Notably, while Facebook's parent corporation, Meta Platforms Inc. ("Meta"), is not the only vendor providing tracking technology, for many reasons, it appears to be the

most prominent in terms of attention on this issue. Like many other similarly situated technology companies, Meta states that it is not acting as a business associate on behalf of any HIPAA covered entity utilizing its technology. However, Meta itself is facing litigation related to the alleged improper collection of medical information and other data containing personally identifiable information. Meta has argued that it should not "be held liable for certain healthcare providers' alleged misuse of a publicly available tool," and the litigation against it should be dismissed.[2] This and other arguments were not prevailing in Meta's efforts to dismiss a medical information privacy class action case related to its online tracking technology.[3]

This legal risk is not confined to large healthcare systems and technology platforms, and the scope of these lawsuits could easily broaden to encompass medical practices who utilize tracking technology on their websites. Potential class action plaintiffs can check whether tracking technology is being utilized on a medical practice's website the same way that anyone can, using the Blacklight service developed by The Markup discussed in the earlier Sentinel articles, or by using another website privacy inspection service or app. If your practice has not yet determined whether tracking technologies are being utilized—particularly on password protected areas of websites, where protected health information ("PHI") is accessed and transmitted, such as a patient portal—now is the time to do so.[4]

While the legal risk posed by website tracking technology may seem like a new technical matter that few patients or healthcare providers do or should know about, a key element of many claims centers around the various notices that have been made available to the healthcare industry on the issue. Lawsuits often reference the guidance and other information that the U.S. Department of Health and Human Services Office for Civil Rights ("OCR") has issued specifically addressing this topic. In addition to the OCR bulletin referenced in the May 2023 Sentinel article, a joint letter was sent by the Federal Trade Commission ("FTC") and OCR in July 2023 to about 130 healthcare organizations cautioning providers "about the privacy and security risks related to the use of online tracking technologies that may be integrated into their websites . . . that may be impermissibly disclosing consumers' sensitive personal health data to third parties." Along with the allegations about prior notice of this issue, other allegations and claims in the class action lawsuits include improper collection and disclosure of private clinical and billing information, invasion of privacy, and violation of various state laws.[5]

In addition to the legal risk from class action plaintiffs, utilizing website tracking technology also presents significant regulatory risk. While no related HIPAA enforcement actions or settlements have been announced to date, numerous healthcare organizations have provided breach notifications to millions of patients about this issue.[6] In issuing the July 2023 letter referenced above, OCR stated it continued "to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue." Notably, while the action did not involve a HIPAA regulated entity, the FTC took "enforcement action for the first time under its Health Breach Notification Rule against the telehealth and prescription drug discount provider

GoodRx Holdings Inc., for failing to notify consumers and others of its unauthorized disclosures of consumers' personal health information to Facebook, Google, and other companies."[7]

As suggested in prior articles, the most effective way to mitigate the risk is to remove or at least control tracking technology utilized on your medical practice's website, particularly any areas that contain protected health information, such as a patient portal. However, the first step in that process is to determine whether tracking technology is utilized on any webpage controlled by or integrating with your healthcare organization. In many instances, this legal risk cannot be mitigated by the execution of a business associate agreement with the tracking technology vendor because as noted above, most of these vendors do not consider themselves to be business associates, nor are these technology vendors providing the type of service that would make them business associates. In any instance, even with a business associate agreement in place, disclosures to a business associate still must have a permissible purpose pursuant to the HIPAA Privacy Rule, unless patients provide disclosure authorization.

Given the amount of information promulgated by various government agencies over the past several months on this topic, healthcare organizations should be aware that they are presumed by class action plaintiffs to be on notice of this issue, and, as a result, groups should take the necessary steps to reduce the significant legal exposure associated with this risk.

[1]. Naomi Diaz, "How much health systems are paying to settle Pixel lawsuits," Becker's Health IT (Aug. 23, 2023), https://www.beckershospitalreview.com/cybersecurity/how-much-health-systems-are-paying-to-settle-pixel-lawsuits.html.

[2]. Jessica Davis, "Meta punts pixel tool responsibility, says privacy fault is on providers," SC Media (May 10, 2023), https://www.scmagazine.com/news/meta-health-providers-using-pixel-tool-responsible-for-patient-privacy.

[3]. Steve Alder, "Federal Judge Tentatively Advances Meta Pixel Medical Privacy Class Action," HIPAA Journal (Aug. 18, 2023), https://www.hipaajournal.com/federal-judge-tentatively-advances-meta-pixel-medical-privacy-class-action.

[4]. Such a check should also be performed whenever design or configuration changes are made to webpages to confirm that tracking technologies have not been added as part of the change.

[5]. Courts across the country have routinely recognized that HIPAA itself does not provide a private right of action. However, many of these lawsuits leverage allegations of a defendant healthcare organization's failure to meet certain HIPAA Privacy Rule and HIPAA Security Rule requirements as part of their case.

[6]. Steve Alder, “Meta Facing Scrutiny Over Use of Meta Pixel Tracking Code on Hospital Websites,” HIPAA Journal (Oct. 24, 2022). To be sure, as a regulatory matter, whether a breach has occurred is a legal determination based on the specific facts involved with an incident.

[7]. Following the GoodRx matter, the FTC has announced at least two other enforcement actions related to similar alleged practices of unauthorized disclosure of personal health information to third parties through tracking technologies integrated into websites and apps.
