The Hidden Dangers of Online Trackers

By Brian Johnson

Recent events have drawn attention to the widespread use of online trackers and raised privacy concerns for healthcare organizations. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has issued a bulletin following filed complaints, class action lawsuits, breach notifications, and investigations that bring attention to this issue. The bulletin specifically addresses the collection of protected health information (PHI) by online trackers and the possibility of unauthorized data sharing with third parties. It is essential that healthcare organizations take proactive measures to ensure that the data collected by these trackers and shared with third parties comply with the regulations set forth in the Health Insurance Portability and Accountability Act (HIPAA).

In a previous Sentinel article titled "The Dangers of Using Meta Pixel on Your Website," we discussed the presence of the Meta-supplied tracker and provided guidance on removing it from your website. [1] In this article, we expand the topic of online trackers, highlight the key concerns outlined in the OCR bulletin, and provide guidance on mitigating potential risks.

An online tracker is a computer code placed within a website that is designed to collect information about a visitor's interactions with the site. Most trackers are supplied to website owners free of charge by third-party vendors such as Meta and Google. The trackers are generally invisible to website users. When the code runs, it sends the collected data to the tracking vendor for analysis. A common practice is to collect usage data to identify areas for improvement and provide a better experience for visitors. This includes collecting data on page load times, most visited pages, downloads, number of clicks, time spent and keyword searches. Additionally, trackers are often used to collect information on conversion rates, for example, the number of visitors who completed the process to schedule an appointment after clicking the "schedule now" button. Tracking vendors also benefit from the presence of the tracker. The collected data is often used for marketing and online ads. Website owners should be aware that in the presence of tracking technology any content on the page can be consumed by the tracking vendor. This can have unintended consequences for pages that include health data.

The concern for healthcare organizations is when trackers collect health data that leads to impermissible data sharing. According to HIPAA regulations, PHI data can only be shared with third parties when explicit permission has been granted, or in the case of permissible uses and disclosures not requiring patient authorization, such as for recognized health care operations or when a business associate agreement (BAA) has been executed with the third-party tracking vendor. [2] To address the issue, OCR issued a bulletin titled, “Use

of Online Tracking Technologies by HIPAA Covered Entities and Business Associates." [3] The bulletin provides guidance on tracking technologies, types of data collected, common usage scenarios, and compliance with the Privacy Rule.

The bulletin distinguishes between unauthenticated pages, such as the homepage of a publicly accessible website for a medical group, and user-authenticated pages, such as a patient portal. The former contains generic information about a practice and has less risk when a tracker is present. The latter requires users to log in and often contains individually identifiable health information (IIHI) such as patient name, address, phone number, appointment times, health history, prescriptions, and lab results. The presence of a tracker on a user-authenticated page likely has access to PHI and introduces the potential of impermissible sharing with third parties.

The OCR bulletin stresses that "Regulated entities are required to comply with the HIPAA rules when using tracking technologies." [3] This means that Covered Entities and Business Associates must obtain explicit permission to share information with tracking vendors for marketing purposes. Otherwise, if the tracking vendor meets the requirements of a business associate, a business associate agreement (BAA) must be in place. However, simply providing protected health information (PHI) to a tracking vendor or having a signed BAA does not automatically make them a business associate. [3] The tracking vendor must meet the explicit definition of a business associate, otherwise HIPAA compliant authorizations are required. The bulletin also cautions against the use of website banners that require visitors to accept the usage of tracking technologies, as this does not meet the requirements for HIPAA authorization. It is important for regulated entities to ensure that they are compliant with HIPAA rules when using tracking technologies to protect the privacy and security of PHI.

The bulletin does not mention specific trackers or vendors by name; however, Meta Pixel (formally Facebook Pixel) has been the subject of multiple class action lawsuits related to its tracking technology. An investigation by The Markup found thirty-three of the top one hundred healthcare providers using the tracking technology with evidence of sensitive data being shared through patient portals and online schedulers.[4] One example demonstrated the use of an appointment scheduler sending Facebook the name of the doctor, including her specialty, along with the patients' first name, last name, email address, phone number, zip code and city. To help healthcare organizations identify the presence of Meta Pixel's tracking technology on their websites, The Markup has developed a tool called Blacklight.[5] This tool can scan a website and alert healthcare organizations if Meta Pixel is present. If a healthcare organization finds the tracker on their website, they should investigate its presence.

It is crucial for healthcare organizations to assess their websites for all tracking technologies and evaluate compliance with HIPAA regulations. To achieve this, organizations should first identify where health data is displayed or collected from visitors. They should then search for the presence of trackers within those sections of the website. If trackers are found, organizations should determine what data they are collecting and if

it's necessary to share with the tracking vendor. If the trackers have no value, they should be removed. However, if they are necessary, organizations must ensure that the trackers disclose the minimum necessary PHI, and that appropriate BAAs and authorizations are in place. Lastly, recurring examination of tracker technologies should be added to the risk analysis and risk management procedures for the organization.

In conclusion, the use of online trackers has raised privacy concerns for healthcare organizations. The previously discussed OCR bulletin addresses this issue, specifically focusing on the collection of protected health information (PHI) and the possibility of unauthorized data sharing with third parties. Practices must take proactive measures to ensure that the data collected by these trackers and shared with third parties comply with HIPAA regulations. The OCR bulletin provides guidance on tracking technologies, types of data collected, common usage scenarios, and compliance with the Privacy Rule. If you have questions about cybersecurity or access to these resources, call 800-342-2239 or email Contact@svmic.com.

If you experience a cybersecurity incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak with the Claims department.

Other individuals in your organization, such as your administrator, privacy or security officer, or information technology professional, may benefit from these articles and resources. They can sign up for a Vantage account here.

1. The Dangers of Meta Pixel on Your Websites | SVMIC
2. 45 CFR 164.502(e) - Uses and disclosures of protected health information
3. Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates | HHS.gov
4. Facebook Is Receiving Sensitive Medical Information from Hospital Websites – The Markup
5. Blacklight – The Markup