PARKER SMITH & FEEK
An IMA Company

KEEPING UP WITH CLINICAL RISK MANAGEMENT

Navigating Cyber Risks in Healthcare: **Pixel Tracking Technology**

With new cyber risks constantly emerging and evolving, pixel tracking technology has become a top-of-mind risk for healthcare organizations. These "tracking pixels" hidden on organizational websites facilitate the sharing of protected health information (PHI) with a third party, and many organizations may not even realize they have them. As this has become a focal point for litigation and regulatory scrutiny in recent years, understanding and proactively managing pixel tracking technology is imperative in protecting healthcare organizations against evolving cyber risks.

This article explores the multifaceted dimensions of pixel tracking, delving into privacy concerns within healthcare facilities and their consequential impact on cyber insurance coverage, as well as actionable insights for risk mitigation.

WHAT IS PIXEL TRACKING TECHNOLOGY?

Pixel tracking technology, commonly known as "tracking pixels," serves a pivotal role in web analytics and online advertising by monitoring user activity on websites. These pixels often take the form of a piece of code embedded within web pages or emails, remaining invisible to users while seamlessly operating in the background. When a user accesses a webpage, the tracking pixel quietly loads from a remote server, discreetly gathering pertinent data such as IP addresses, browser types, and screen resolutions. This data is then transmitted back to the server for comprehensive analysis, providing valuable insights into user behavior.

The collected data serves a myriad of purposes, including website analytics, ad campaign optimization, and in-depth user behavior analysis. By leveraging this information, website owners and advertisers gain a profound understanding of how users engage with their content, facilitating informed

ABOUT PARKER, SMITH & FEEK

Parker, Smith & Feek's dedicated Healthcare Practice has over 40 years of experience providing healthcare organizations with commercial insurance, risk financing, and risk management expertise, as well as clinical/facility risk management, claims advocacy, employee benefits, wellness and workers' compensation consulting. The breadth of our healthcare footprint is substantial across the Pacific Northwest, and comprises all sizes and types of clients served.

LEARN MORE

Healthcare Industry

Our Services

CONTACT US

Email

Tel: 800.457.0220

FOLLOW US

Danielle Donovan is Parker, Smith & Feek's Clinical Risk Manager, dedicated to helping improve our healthcare clients' operations and mitigate risks. She publishes regular articles to support this effort and provide unbiased advice on issues facing all types of healthcare organizations. Stay tuned for her next installment, and contact Parker, Smith & Feek's Healthcare Practice Group if you would like to learn more.

continued >

decision-making and targeted strategies. According to an article published by The Markup in 2022, 33 out of Newsweek's top 100 hospitals in America were using tracking pixels on their websites.

In recent years, pixel tracking technology has garnered significant attention from plaintiff attorneys, particularly concerning the unauthorized transmission of PHI from hospital websites to Meta without patient consent. This practice has raised considerable concerns regarding HIPAA privacy compliance, making it a focal point of recent legal scrutiny and advocacy efforts. Baker Hostetler observed that over 50 lawsuits have been filed against health systems related to their use of tracking pixels since August 2022.

PRIVACY CONCERNS

Healthcare facilities' public websites may inadvertently disclose PHI to third parties through embedded pixels, violating HIPAA privacy regulations by doing so without patient consent. This situation has led to an uptick in breach events or claims, with many healthcare institutions facing class-action lawsuits stemming from the presence of pixels on their websites.

Some recent significant breach events include:

Kaiser Permanente in 2024

"Kaiser Permanente has determined that certain online technologies, previously installed on its websites and mobile applications, may have transmitted personal information to third-party vendors Google, Microsoft Bing, and X (Twitter) when members and patients accessed its websites or mobile applications," the healthcare giant shared in an emailed statement. The breach impacted 13.4 million current and former patients.

Cerebral in 2023

In March, U.S. mental health startup Cerebral revealed that it had unintentionally collected and shared the private health information of over three million users with Facebook, Google, TikTok, and other major advertising companies through tracking pixels. The company claimed its use of pixel trackers did not breach HIPAA regulations, as it merely connects patients with healthcare providers and does not directly offer care itself.

Advocate Aurora Health in 2022

In October 2022, Advocate Aurora Health experienced a data leak linked to its use of tracking pixels from Google and Meta, affecting nearly three million individuals.

In September, Advocate Aurora Health agreed to pay over $12.2 million to settle a class-action suit over the pixel-related data breach. Several similar lawsuits against health systems and vendors are pending.

The Federal Trade Commission (FTC) has also taken an active interest in how healthcare organizations share patient information with mobile health apps, given that these entities have historically operated outside the purview of HIPAA regulations. In March 2023, the FTC initiated enforcement actions against GoodRX and BetterHelp for their practices involving the sharing of patient health data through third-party tracking pixels, enabling the analysis and inference of user activity—an indication of the growing regulatory scrutiny in this area.

THE IMPACT ON CYBER COVERAGE

Aware of this vulnerability, some cyber insurance carriers have begun implementing limitations or restrictions on coverage. These restrictions have come in the form of "website tracking exclusion" endorsements on their policies. Such endorsements explicitly exclude coverage for indemnity and defense for claims related to a breach of PHI when pixel or code-tracking technologies were involved. However, there are still cyber carriers who may be willing to

continued >

underwrite this exposure when proper controls are in place. There may also be some coverage for this exposure in other insurance policies. It is essential to work closely with an insurance broker specializing in technology and healthcare to create an insurance profile that contemplates all angles of coverage.

RISK MITIGATION

To address the risk of pixel tracking technologies effectively, organizations can take the following proactive steps:

+ Collaborate with your IT team to conduct a thorough review of pixel technology deployed on your public-facing website and those utilized by third-party vendors or health apps. This review process may involve leveraging external search tools like themarkup.org/blacklight to ensure comprehensive scrutiny.
+ Not all pixel tracking is bad. Bring together leaders from the organization's IT and marketing teams to develop appropriate guidelines and policies regarding the information collected and its intended use. Consider using the FTC's research questions as a template when evaluating how pixel tracking is deployed at your organization.
+ Provide targeted training sessions for marketing and communications personnel to raise awareness about the potential HIPAA privacy and security implications associated with utilizing tracking pixels. If employing tracking technology, consider implementing consent mechanisms or authorization protocols for the sharing of PHI and whether disclosure is allowed per state and federal regulations.
+ Conduct a thorough assessment of your current cyber insurance policies with a seasoned insurance broker. Identify any coverage exclusions or limitations related to pixel tracking and explore alternative coverage options available through other property and casualty policies if necessary.

If you are concerned about how pixel tracking technology may be impacting your organization, don't hesitate to get in touch with an experienced cyber risk expert.

References and Resources

1. BakerHostetler. (2023, April 27). BakerHostetler launches 2023 Data Security Incident Response Report. www.bakerlaw.com/insights/bakerhostetler-launches-2023-data-security-incident-response-report/
2. Feathers, T., Waller, A., Mattu, S., & Fondrie-Teitler, S. (2022, June 16). Facebook is receiving sensitive medical information from hospital websites. The Markup. themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites
3. Heaton , K. (2022, December 14). Cyber risk revealed: Pixels and tracking technology. beazley. www.beazley.com/en-us/articles/cyber-risk-revealed-pixels-and-tracking-technology
4. (OCR), O. for C. R. (2022, December 1). Use of online tracking technologies by HIPAA covered entities and business associates. HHS.gov. www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html
5. Tech risks: How pixels and biometrics lead to privacy claims - news - tools & intel: CRC Group. Wholesale & Specialty Insurance | CRC Group. (n.d.). www.crcgroup.com/Tools-Intel/post/tech-risks-how-pixels-and-biometrics-lead-to-privacy-claims
6. Versel , N. (2023, December 5). Tips to manage safe pixel tracking. Healthcare IT News. www.healthcareitnews.com/news/tips-manage-safe-pixel-tracking
7. The FTC Office of Technology. (2023, March 16). Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking. Federal Trade Commission. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking
8. Miliard, M. (2022a, October 20). Advocate aurora notifies patients of potential tracking pixel breach. Healthcare IT News. https://www.healthcareitnews.com/news/advocate-aurora-notifies-patients-potential-tracking-pixel-breach
9. Miliard, M. (2022b, November 16). New healthcare privacy challenges as online data tracking, sharing methods evolve. Healthcare IT News. https://www.healthcareitnews.com/news/new-healthcare-privacy-challenges-online-data-tracking-sharing-methods-evolve
10. Page, C. (2023, April 17). The crackdown on pixel tracking in telehealth is a warning for every startup. TechCrunch. https://techcrunch.com/2023/04/17/pixel-tracking-hipaa-startups/
11. Pallardy, C. (2023, June 1). Tracking pixels continue to cause data privacy issues in healthcare. Information Week. https://www.informationweek.com/data-management/tracking-pixels-continue-to-cause-data-privacy-issues-in-healthcare#close-modal
12. Pallardy, C. (2024, May 2). Tracking pixels and another Big Health Care Breach. InformationWeek. https://www.informationweek.com/cyber-resilience/tracking-pixels-and-another-big-health-care-breach#close-modal