AMWINS®

Meta Pixel Class Action Lawsuits Focus on HIPAA – For Now

In the past year, we've seen a surge in class action lawsuits alleging violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These cases cite healthcare companies' usage of online tracking technologies and subsequent sharing with the likes of Meta, Google and others for purposes of targeted advertising, often resulting in the sharing of confidential medical information such as medical conditions, appointment information, medications, provider names and more.

Many of these same suits also claim that Meta Pixel coding enables the collection and receipt of IP addresses and patient search terms without consent. And it's worth noting, many cases include information collected on an entity's main website, as well as through password protected portals.

The main issue in many of these cases is that once the information is shared, the "breach" is considered to have already happened. So, even if unsuspecting marketing departments turn off this feature, there's still potential for liability to exist.

CONTACT

To learn more about how Amwins can help you place coverage for your clients, reach out to your local Amwins broker.

LEGAL DISCLAIMER

Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions. Please refer to your policy for the actual language.

Courtesy of Amwins Group, Inc.

Tracking Technology Isn't New

Marketing departments have long used tracking technology like Meta Pixel to collect information from users visiting a website. However, a **recent study** by The Markup found that 33 of the top 100 hospitals in America were using Meta Pixel and sending Facebook information whenever a person clicked a button to schedule a doctor's appointment. The study also determined that seven of the health systems surveyed also had Meta Pixel installed inside password protected patient portals.

As a result, Meta and the health care systems investigated for the article in The Markup are facing mounting criticism and legal action – Meta for using the data to target social media ads directly related to personal information and the hospitals for collecting patient information protected under HIPAA, including names, health conditions, email addresses, etc.

Litigation Could Lead to Regulation

Meta is currently facing at least 50 class action lawsuits and the U.S. Congress has begun an inquiry into a number of **telehealth companies accused of sharing patients' answers to medical intake questions**. Litigation alleging that the use of tracking vehicles from Meta, Google, TikTok and more, violates the federal Video Privacy Protection Act (VPPA) and may constitute wiretapping under federal and state wiretapping laws, is also on the rise. Pennsylvania has seen an inordinate number of these cases in the past year.

While most suits have not been fully litigated, they have caught the attention of State Attorneys General and raise a number of legal questions. One important question is what role – if any – terms of service and website disclosures play and how the use of tracking technology applies to both the Electronic Communications Privacy Act and Stored Communications Act.

The Office of Civil Rights (OCR), which is responsible for enforcing HIPAA, issued a **bulletin** in December 2022 stating that "regulated entities are not permitted to use tracking technologies that would result in impermissible disclosures of protected health information (PHI) to tracking technology vendors." The bulletin also determined that individual IP addresses are considered unique identifiers. While the document is meant only to provide clarity and not set legal precedent, many organizations have already begun to make changes based on this early guidance.

In July, that bulletin was followed by a joint letter from the Federal Trade Commission (FTC) and OCR to approximately 130 hospital systems and telehealth providers, warning them about privacy risks from online tracking technology. The letter reiterated risks posed by unauthorized disclosure of PHI to third parties and the responsibility entities covered by HIPAA have to protect this information under the law.

It's still too early to tell if additional regulation will be enacted, but there are already parallels to compliance rules put in place within the payment card industry (PCI). These compliance rules were established in the early 2000s when the FTC gained oversight of consumer protections. They were designed to help ensure the security of credit card transactions, specifically credit card data provided by cardholders and transmitted through card processing transactions.

How Your Clients Can Mitigate Risk

With so many questions about Meta Pixel liability unanswered, insureds need to be prepared. At the very least, an organization's Chief Legal Officer, Chief Technology Officer and Chief Privacy Officer must be fully aware of what tracking technology is in place and how it is being used, including what information is being gathered and with whom the information is being shared.

Entities should perform a risk-based assessment of their use of tracking technology.

- Assess whether the entity's website uses Meta Pixel or other tracking software.
- Determine how long data has been collected and if the data collected complies with applicable data privacy laws.
- Verify data is being gathered with the knowledge and consent of the user.
- Review contracts with third-party vendors and/or business associates to ensure compliance.
- Remove tracking software if necessary.
- Work with an insurance broker to review cyber insurance coverage and discuss options that relate to potential fines and penalties.

If a breach has been discovered, entities must conduct a risk assessment and, if necessary, make appropriate HIPAA notifications.

Having the appropriate legal representation is also key. Law firms with a firsthand knowledge of Meta Pixel and tracking software cases are essential. They can help insureds determine whether the case has merit, or if the plaintiff is simply looking for a quick settlement.

Market Impacts

Due to the nature of the risk, the massive loss potential, and the possibility of losses bleeding into D&O insurance coverage, many cyber carriers are reconsidering how, and if, to cover losses related to Pixel-based claims. Some are adding sweeping exclusions to preclude cover for these types of losses, while others are offering a carve-back for situations where the insured has an in-force Business Associate Agreement (BAA) governing the handling of PHI. Some carriers have also begun to employ a **free, online tool** to determine if tracking codes are being used on a particular website. All that is required to gather this information is the URL of the website.

As the industry learns more about this exposure and faces losses like the **$18.4M settlement** resolving a class action lawsuit against Mass General Brigham Hospital, we expect rates will be adversely impacted. Underwriters will want to confirm that insureds are performing their due diligence properly. Insureds should be prepared to detail what safeguards are in place to ensure that PHI and personally identifiable information (PII) aren't being shared without the knowledge and consent of the user. Underwriters will also want to know what protections are built into contracts with third parties.

Looking Ahead

While healthcare is the sector currently facing the most profound impact, there are rumblings that education may be next. Much like HIPAA, the **Family Educational Rights and Privacy Act (FERPA)** protects the privacy of student education records. It applies to public and private elementary, secondary and post-secondary schools, and prohibits educational institutions from disclosing PII in education records without the written consent of an eligible student, or if the student is a minor, the student's parents.

Educational institutions should be taking the necessary steps to understand how tracking technology is used on their sites. Now is the time to perform a risk-based assessment; it's imperative to complete due diligence before there is a potential breach.

Amwins Can Help

At Amwins, our cyber liability specialists are at the forefront of this emerging issue. We not only understand the potential impact to your clients, but we can also provide you with the market access needed to help protect your clients from exposure. Reach out to your local Amwins broker today.

Contributing Authors

- Steve Vallone, EVP with Amwins Brokerage in San Francisco, CA
- Nick Economidis, SVP and Leader of Cyber Insurance Team, Crum & Forster in Morristown, NJ
- Paul Karlsgodt, Partner and Leader of Privacy and Digital Risk Class Action and Litigation, Baker Hostetler in Denver, CO
- Lynn Sessions, Partner and Leader of Healthcare Privacy and Compliance, Baker Hostetler in Houston, TX