U.S. Risk, LLC

PRIVACY UPDATE: TRACKING PIXELS

Companies are now facing numerous lawsuits alleging privacy violations relating to website pixels and trackers. The suits allege violations due to illegal data collection, and one of the most often claimed complaint involves healthcare organizations and the Meta (Facebook's parent) pixel. Hundreds of healthcare providers and other businesses are being targeted by class action lawsuits across the country, alleging the unauthorized disclosure of personally identifiable and/or health information, seeking civil damages for each disclosure.

ABOUT TRACKING PIXELS

Several companies (including Facebook's parent company, Meta) offer tools to track website user interactions. These trackers run a script when a user visits a website in a browser with the purpose of collecting information about that user. Typically, trackers are added to the website either manually by a developer or through partner integration. Social channels such as Twitter, TikTok, Snapchat and LinkedIn also use pixels similar to those of Facebook.

When a social media pixel is installed, it enables the collection and combination of information found on users' social profiles (demographic data, interests/topics followed, topics posted about, etc.) along with behavioral data gathered from the users' interactions with that company's website.

› Impact of Tracking Pixels in Healthcare

For years, a tracking tool installed on many hospitals' websites has been collecting patients' highly sensitive personal identifiable information and personal health information sending it to Meta/Facebook.

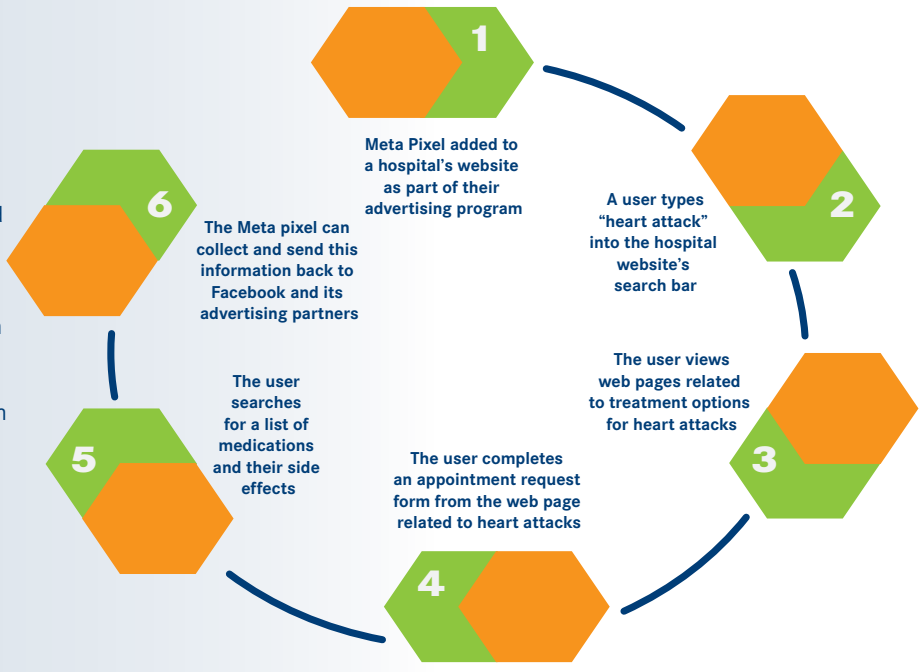
A recent investigation on the sharing of healthcare data with Meta/Facebook via Meta Pixel on these websites found that 33 of the top 100 hospitals in the United States had the Meta Pixel code on their websites, and 7 hospitals had the code installed on their patient portals behind logins, yet consent to share data was not obtained.

Federal law, state law, and HIPAA require patient consent and a business agreement to share personal health information between companies. In addition to the exposure organizations may face from class action lawsuits, breach notifications and regulatory enforcement may also cause significant expense.

Do you know if you're using tracking pixels?

There are several variations of this litigation trend emerging with some resulting in class actions and others in regulatory inquiry. To find out if you're using any tracking mechanisms on your website or patient portal, start with your marketing team. Tracking pixels are often placed to collect data for targeted advertising. This can be through social media platforms, google, or third party vendors. Email blast campaigns often contain tracking pixels as well.

For those with tracking pixels, a typical exclusion will include the use of code that redirects or causes to be redirected information from an individual to a third party. Exclusions typically don't apply to third parties with whom the insured organization has an in-force Business Associate Agreement (BAA) that governs the handling of PHI for that particular information.



U.S. Risk, LLC

PRIVACY UPDATE: TRACKING PIXELS

› Data Breach Scenarios

• Class action lawsuit against WakeMed asserting an alleged data breach stemming from the Meta Pixel. The claim states that the information of nearly 500,000 patients was shared with Meta (Facebook) through the use of the Meta pixel tool installed on the hospital website collecting patients' highly sensitive personal identifiable information and personal health information.

• Sixteen claims including common law invasions of privacy – intrusion upon seclusion, invasion of privacy, breach of contract, unjust enrichment and a wide range of violations were included in a class action suit filed in California. The plaintiff, a patient of UCSF Medical Center and Dignity Health Medical Foundation, claimed her sensitive health information was unlawfully obtained by Meta when she entered the information into an online patient portal. UCSF had added the Meta Pixel code to the web pages of the patient portal. The lawsuit seeks damages and injunctive and equitable relief.

• A class action suit was filed against data giant Oracle claiming the company is tracking and monitoring more than 5 billion people and alleging that tracking oftentimes occurs without the users' knowledge or consent. Part of the complaint alleges that the Oracle JavaScript tracking code obtained personal information by collecting user data from web forms, the URLs users visited as well as their webpage title and keywords, the exact date and time of visits, and more.

THE BOTTOM LINE

Exposure due to tracking pixels will continue to increase and even the most diligent organization can be susceptible to a claim. A trusted expert highly experienced in cyber policy wording and how to customize policy terms needs to be brought into the process as early as possible to help clients assess their exposure in this fast-changing arena and ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.