Analyzing the HIPAA Compliance of Meta Pixel (Facebook and Instagram)

By Marc Heffner

Under the scrutiny of HIPAA compliance, the Meta Pixels emerges as a contentious tool, particularly in areas where patient privacy is not only a priority, but a legal requirement. Investigations into the prevalence of Meta Pixels on healthcare-related websites reveal a majority of healthcare organizations use tracking tools on their online platforms. This raises serious questions about the sanctity of Protected Health Information (PHI) and whether Meta Pixels can coexist with HIPAA's stringent requirements.

The crux of the problem lies in the Meta Pixel's functionality as a tracking tool. The pixel collects data reflecting user activities on a website, which, in the context of healthcare, can result in PHI being inadvertently shared.

Consider a patient who needs a dentist to extract a tooth. Using their browser with their associated IP address, the patient lands on a page for a dental organization that discusses their expertise in tooth extraction. Because of the tracking method on the dental organization's website, a trigger occurs, and the practice sends an automated message back to the IP address informing the end user that they are open 24 hours a day, seven days a week and can extract their tooth and relieve any pain right away.

This is great marketing in any other industry, consumers come to the website and find a solution to their pain. Since we are in healthcare this triggering action can violate HIPAA. The organization collected information in the open and sent something back, publicly disclosing the patient's medical condition over the internet. Medical and dental organizations must properly mask sensitive patient

information, including medical conditions, demographic information including IP addresses before sending an automated response.

In light of this, people in the healthcare industry are being told to carefully check out websites and make their online space safer by adding strong privacy protections. The following plan outlines the most important things to think about when making sure you're following HIPAA rules:

- **Risk Assessments:** Conduct a risk-based evaluation of tracking technology, identifying if tools like Meta Pixel are operational on the entity's website.
- **Patient Consent:** Verify that any data collected has been done with the patient's knowledge and consent - a foundational tenet of HIPAA guidelines.
- **Business Associate Agreements:** Seek HIPAA-compliant tracking vendors willing to enter into BAAs, thus establishing a compliant relationship for data handling.
- **Data Transmission Scrutiny:** Prioritize obtaining a lucid comprehension of the scope of pixel-data being transmitted before authorizing its release.
- **Proactive Policy Implementation:** Employ a proactive stance in security by ensuring that all policies and procedures are not just HIPAA adherent but are practiced diligently.

Through these strategies, healthcare providers can find their way through the complicated world of pixel trackers, finding a balance between using cutting-edge technology for marketing pixels methodologies and the strict need to protect patient privacy.

Cyber carriers are also rethinking how they handle losses caused by claims related to the use of tools like Meta Pixel. These broad exclusions happen a lot of the time unless there is a solid Business Associate Agreement (BAA) in place to govern how PHI is handled. This shows how important it is to do your research and reinforces the rule that PHI and PII cannot be shared without knowledge and permission.

Pixel trackers can help improve the user experience, but they can also spread personal health information without permission. The healthcare sector has to walk a fine line between these two issues. It is very important for covered entities to make sure that they fully understand and follow the rules that protect patient data. As the story about Meta Pixels possibly being HIPAA-compliant develops, it sends a clear message to the healthcare community: patient privacy is still very important and requires a strong dedication to privacy rules and protocols.

About the Author:

Marc Heffner is the founding partner of DSO Marketing X™ and serves as a Fractional CMO specializing in the dental vertical. With 25 years of experience in holistic marketing, Marc has a proven track record of steering growth for multi-location dental practices and private equity firms in the healthcare space.

His expertise lies in crafting sound marketing strategies, developing strong marketing teams and introducing new technology platforms to achieve ambitious goals.

Marc's marketing philosophy revolves around **creating pathways to growth opportunities** for corporations willing to invest in their future. He has led marketing growth for organizations from the early days of social media to its current state in the customer-centric electronic media world. Marc understands the transformative power of social media on brands and organizations, and emphasizes the importance of well-strategized and smartly executed plans.

Marc holds an MBA from Pepperdine University's Graziadio School of Business, a Bachelor of Science in Mass Communication from the University of Utah, and a Certificate in Digital Marketing Analytics from the Massachusetts Institute of Technology (MIT) Sloan School of Business.

For more information about Marc's Fractional CMO team at DSO Marketing X™, visit DSOMarketingX.com. You can also reach out to Marc via email at MHeffner@DSOMarketingX.com or by calling 714-270-9205.

25+ Years of Experience • Over $1 Billion in Revenue • Fortune 500 Experience

SIGN UP FOR A FREE CONSULTATION TODAY

©2024 DSO Marketing X • dsomarketingx.com