HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Tracking Tool on Hospital Websites Can Lead to HIPAA Breaches

Many hospital websites include a tracking tool that collects protected health information (PHI) and sends it to Facebook, posing the risk of major HIPAA breaches. In some cases, the hospital leadership has no idea such a tracking tool is on their website.

According to recent research, 33 of *Newsweek*'s Top 100 Hospitals included the tracker Meta Pixel on their websites.[1] The tracker automatically sends Facebook a packet of data when a consumer schedules a doctor's appointment on the website.

Facebook's parent company, Meta, is facing at least one class action lawsuit related to the tracker. In one lawsuit, the plaintiff claims Meta began sending her targeted ads related to her medical condition after she used the patient portals of a California hospital and health system.[2]

"Meta knows that the user data collected through its Pixel on healthcare defendants' websites includes highly sensitive medical information but, in reckless disregard for patient privacy, continues to collect, use, and profit from this information," according to the lawsuit.

Serious HIPAA Threat

Hospital leaders should be concerned about the implications of the tracker on their HIPAA compliance programs, says **Weston Hall**, JD, partner with Chamblee Ryan in Dallas.

"The clear implications here are that there are multiple, rampant, and ongoing violations of HIPAA occurring so long as this Meta Pixel is installed on the websites for healthcare providers," Hall says. "HIPAA makes clear that covered entities — of which healthcare providers are at the top of the list — may not disclose protected health information to third parties absent either the patient's express consent or a specific contract [that] allows for such disclosure. However, in these cases, it appears that neither a patient's consent has been obtained nor is there a contract that would allow for these disclosures."

Hall notes Section 164.514(b)(2)(i)(A)-(R) details a long list of identifying information that qualifies as PHI.[3] This list includes a patient's name, address, phone number, and much more. Meta has claimed that such PHI is "hashed," meaning the information is protected through cryptography, but Hall says these hashing efforts are subpar, and Meta still uses this information to link Pixel data to individual Facebook profiles.

"A mere cursory look into the implications of the installation and utilization of the Meta Pixel on the website of healthcare providers — particularly the portions of such websites that are specifically utilized by patients seeking appointments and other information related to private care — is flagrantly violating the core of HIPAA, which is to protect private and protected health information from being disclosed to third parties," Hall explains. "These violations are severe and can lead to a number of costly consequences that will be more fleshed out below."

Hall notes there are two classes of violations of HIPAA that a covered entity can commit. The first involves a violation made with reasonable cause, which means "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known," the act or omission violated a provision of HIPAA. The standard for this type of offense boils down to a negligence standard whereby a covered entity will be liable if a reasonable inspection of the situation would reveal the violation in question.

The second class of HIPAA violations is classified as willful neglect, which occurs when the covered entity engages in a "conscious, intentional failure or reckless indifference to

the obligation to comply" with the provisions of HIPAA. This is the more severe class of violation, and it comes with much heftier consequences if proven, Hall says.

The main reason to install Meta Pixel "would be to supply healthcare providers or their business associates with analytics about the ads they've placed on social media websites, such as Facebook and Instagram, to more effectively target people who have visited their websites," Hall notes. "In exchange for these analytics, the Meta Pixel allows Meta to help itself to a broad stream of data as to what buttons patients will click even on the healthcare website's private pages, as well as the contents of any forms filled out online by the patient."

Due to the limited nature of what Pixel provides, along with the fact that it must be installed independently, it is likely such a flagrant misuse and disclosure of PHI would be classified as willful neglect, Hall says.

The liability for HIPAA violations arising from willful neglect can be costly. For violations occurring after Feb. 18, 2009, the cost of a HIPAA violation arising from willful neglect can be as little as $10,000 for novel violations that were remedied within 30 days, to as much as $1.5 million for violations that are identical to other violations occurring within a calendar year.

"These fines are per violation. Given that each disclosure of each bit of protected health information constitutes a separate violation, it isn't hard to see just how massive a fine can become," Hall says.

Hospitals will be held liable for HIPAA violations even if they did not know about the Meta Pixel on their website, Hall says. The covered entity responsible for complying with HIPAA laws is obligated to conduct reasonable inspections to ensure compliance. The Office for Civil Rights could strongly argue a reasonable inspection of their website would reveal Meta Pixel along with the data it is transmitting.

"However, in cases where there was not actual knowledge, there is some leniency," Hall notes. "If a hospital, in fact, was not aware of the Meta Pixel, their violation would likely fall under reasonable cause, which typically results in less severe fines and penalties."

Hospital leaders should check their websites for Meta Pixel or similar programs transmitting PHI to unauthorized third parties, Hall advises. Hospitals that previously used the tool on their websites also will need to respond to the breach by reporting the event to any individuals whose PHI may have been compromised as well as notifying HHS.

"Depending on how big the breach may have been, the hospital may also have to report the incident to the media. If the breach affects more than 500 residents of a state or jurisdiction, the covered entity is required to provide notice to prominent media outlets serving the state or jurisdiction," Hall says. "Unfortunately, in cases where this Meta Pixel was installed, any resulting violations and breaches may easily affect more than 500 residents of any given state or jurisdiction." ■

REFERENCES

1. Feathers T, Fondrie-Teitler S, Waller A, Mattu S. Facebook is receiving sensitive medical information from hospital websites. *The Markup*. June 16, 2022. https://bit.ly/3bIKMyp
2. United States District Court Northern District of California. *Jane Doe v. Meta Platforms, Inc.* July 25, 2022. https://bit.ly/3d0Orl4
3. Legal Information Institute. 45 CFR § 164.514 — Other requirements relating to uses and disclosures of protected health information. https://bit.ly/3vPu8E7