Erum Ahmed

Facebook data breach could cost health systems millions

Article

The news: A tracking tool on at least 33 US hospital websites is sending sensitive health information to **Facebook**, according to a test conducted by The Markup and STAT.

- The Markup tested the websites of Newsweek's top 100 US hospitals.
- Around 33 of the hospitals had a Meta Pixel tracker.

What's a Meta Pixel tracker? It's Meta's ad tracking tool that helps companies track visitor activity to understand the actions they take on their website.

The Markup found that whenever someone clicked a button on 33 hospital websites to make an appointment, the Meta Pixel sent "a packet of data" to Facebook. This data is connected to an IP address, which can be linked to an individual household.

- For example, clicking the "Schedule Online Now" button on Wisconsin-based **Froedtert Hospital's** website led the Meta Pixel to send Facebook the text of the button, the doctor's name, and the condition selected from the dropdown menu (in this case, Alzheimer's), per The Markup.
- **Frodtert Hospital** reportedly removed the Meta Pixel from its website after reviewing the new findings.
- Similarly, the Meta Pixel installed on **Piedmont Healthcare's** patient portal sent Meta details (like name, date, time, and doctor's name) about a patient's upcoming doctor appointment.

The big takeaway: The privacy leak could be a breach of HIPAA and cost health systems millions.

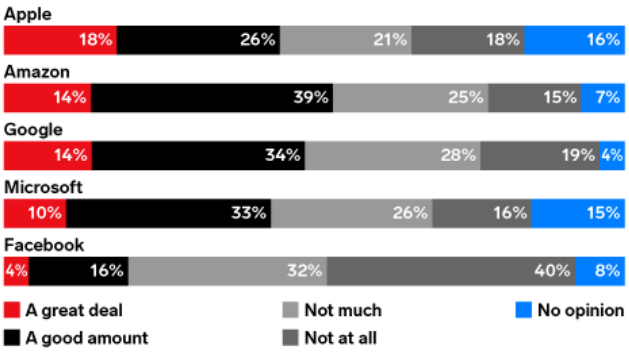
The Meta Pixel blunder could come with a hefty price tag for the hospitals involved if patients decide to take legal action against their hospital for an alleged HIPAA violation. In fact, the **average cost of a healthcare data breach is now $9.42 million**, per the HIPAA Journal.

Meta isn't required to adhere to patient privacy laws like HIPAA, but hospitals are. The only workaround to sharing patient data is if it's de-identified prior to sharing it with a third party.

- For example, the **Mayo Clinic** is working with startup **K Health** to develop an algorithm for individualized hypertension treatment. Mayo Clinic's patient data was likely deidentified (by removing patient names, phone numbers, and addresses) to accommodate HIPAA.

How Much US Internet Users Trust Companies to Responsibly Handle Their Personal Information and Data on Their Internet Activity, by Company, Nov 2021

% of respondents



Note: ages 18+; numbers may not add up to 100% due to rounding
Source: Washington Post and Schar School of Policy and Government at George Mason University as cited in article, Dec 22, 2021

272820 eMarketer | InsiderIntelligence.com