Report on Patient Privacy Volume 22, Number 7. July 07, 2022
In the Wake of Meta Pixel Allegations, CEs, BAs May Be at Risk Under HIPAA, Experts Say

By Jane Anderson

Facebook parent company Meta faces a class-action lawsuit following disclosure that a tracking tool installed on hospitals' websites has been collecting patients' protected health information (PHI)—including details about their medical conditions, prescriptions and doctor's appointments—and sending it to Facebook.

The investigation, conducted by The Markup, tested the websites of *Newsweek*'s top 100 hospitals in America and found the tracker Meta Pixel on one-third of them.[1] Although Facebook and Meta almost certainly are not covered by HIPAA, the hospitals involved are covered, and some experts speculated that this form of data-sharing may be a HIPAA violation.

Rebecca Herold, president of SIMBUS360 and CEO of The Privacy Professor, told *RPP* that, based on information publicly available about The Markup's investigation, it appears PHI input into hospital websites and portals is being sent to Facebook by the Meta Pixel tracker.

Covered entities (CEs) are responsible for the PHI they collect from their patients and insureds, Herold said, adding, "Meta Pixel is a data leak vulnerability that creates significant risk of unauthorized PHI sharing." She urged CEs and business associates (BAs) to take steps to identify and remove Meta Pixel and other trackers from their websites immediately.

David Harlow, chief compliance and privacy officer at Insulet Corporation, agreed that "to the extent a hospital passes along PHI in one form or another to Facebook, as detailed [in The Markup investigation], that could be a HIPAA violation." The regulatory definition of PHI is quite broad and may include any health information associated with any identifier, including an IP address, he said.

"A hospital might argue that the website is open to all, and information gleaned from the [tracker] would only be associated with the Facebook profile of an existing user, who has agreed to their terms of use," Harlow told *RPP*. "There are two potential issues with this response: First, while Facebook has said that it treats health care and information that it obtains in this matter differently (e.g., scrubbing and deleting certain data), it has previously been called to account because it did not enforce its own privacy policies. Second, Facebook has been known to create 'ghost' profiles for individuals who have not actually opened accounts on the platform and agreed to terms of use."