

Report on Patient Privacy Volume 22, Number 12. December 07, 2022 Privacy Briefs: December 2022

By Jane Anderson

◆ **The HHS Office for Civil Rights (OCR) has issued a bulletin to highlight the obligations of covered entities and business associates when using online tracking technologies such as Meta Pixel and Google Analytics.**^[1] “Some regulated entities regularly share electronic protected health information (ePHI) with online tracking technology vendors and some may be doing so in a manner that violates the HIPAA Rules,” OCR said Dec. 1. “The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes ePHI. Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of ePHI to tracking technology vendors or any other violations of the HIPAA Rules.” OCR’s bulletin addresses potential impermissible disclosures of ePHI by HIPAA-regulated entities to online technology tracking vendors, explaining what tracking technologies are, how they are used and what steps regulated entities must take to protect ePHI when using tracking technologies to comply with the HIPAA rules.

◆ **Community Health Network has become the latest health care organization to report a breach due to pixels placed on its website by Facebook and Google: the Indianapolis-based health system said Nov. 18 that the protected health information of 1.5 million patients was exposed.**^[2] “As part of our continued effort to improve access to information about critical patient care services and manage key functionalities of our patient-facing websites, Community uses service providers to help evaluate the accessibility of those websites and information regarding the trends of users navigating the sites,” the health care organization said in a statement. “For a period of time, Community, like many other health systems, worked with those service providers to implement and utilize certain Internet tracking technologies provided by third parties such as Google and Facebook.” When concerns about these pixels were raised,^[3] Community said it initiated an investigation and determined that “the configuration of certain technologies allowed for a broader scope of information to be collected and transmitted to each corresponding third-party tracking technology vendor (e.g., Facebook and Google) than Community had ever intended.” According to Community, the scope of information that could have been transmitted included: computer IP addresses, dates, times and/or locations of scheduled appointments, information about an individual’s health care provider, the type of appointment or procedure scheduled, communications through MyChart—which may have included first and last names and medical record numbers, information about whether an individual had insurance and if an individual had a proxy MyChart account, the name of the proxy.

This document is only available to subscribers. Please log in or purchase access.

[Purchase Login](#)