COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 11. November 09, 2023 Privacy Briefs: November 2023

By Jane Anderson

◆ **The American Hospital Association (AHA) is urging federal lawmakers to intervene with the HHS Office for Civil Rights (OCR) so that hospitals and health systems can continue to use online tracking pixels on their websites.**[1] In a response to a request for information from Sen. Bill Cassidy, R-La., on the privacy implications of pixels, AHA said that OCR's December 2022 guidance that many pixels violate HIPAA "inflicts meaningful harm on patients and public health" because it prevents hospitals and health care systems from being able to provide their communities with reliable health care information. "AHA urges Congress to make clear to OCR that the agency should withdraw the rule immediately," the AHA said. Meanwhile, a study from cybersecurity company Feroot found that the vast majority of health care and telehealth websites are collecting data via trackers and transferring it without consent from the users.[2] Feroot analyzed hundreds of health care and telehealth websites and found that more than 86% are collecting and transferring data without obtaining consent from the user. More than 73% of login and registration pages have trackers, the study found. About 15% of the tracking pixels identified by Feroot read and collect a user's keystrokes, meaning they could identify Social Security numbers, names, email addresses, appointment dates, internet protocol addresses, billing information, medical diagnoses and treatment, the study found. Some of the most common tracking pixels were from Alphabet Inc.'s Google, Microsoft Corp., Meta Platforms Inc. (the parent company of Facebook, Instagram and Threads), and ByteDance (the parent company of TikTok), the study found.

◆ **An August cyberattack at three Prospect Medical Holdings hospitals in Connecticut was far more debilitating than hospital officials publicly acknowledged; the attack now threatens a planned sale of two of the hospitals to Yale New Haven Health, an investigation by the *CT Mirror* found.** The attack affected Manchester, Rockville General and Waterbury hospitals, as well as medical offices affiliated with the hospitals. Over the course of the more than 40-day breach at the hospitals, administrators at two facilities issued 29 "divert notifications" to emergency personnel throughout the region, according to ambulance dispatch logs obtained by the nonprofit publication. In addition, the hospitals were unable to bill Medicaid for payment, forcing the state Department of Social Services to advance them about $7.5 million. "A review of the records shows the facilities had to cancel nearly half of their elective procedures and at times over the nearly six-week period couldn't process X-rays or CT scans that are vital for treating potential stroke or heart attack victims," the investigation found. "At one point in mid-August, state officials were so concerned about staffing issues at Waterbury Hospital they considered activating the volunteer Medical Reserve Corps, which had previously been done only during the height of COVID." All three hospitals declared "all services back online on Sept. 12, nearly six weeks after the attack began, according to diversion notifications." But the hospitals are still recovering financially, and documents uncovered in the *CT Mirror* investigation revealed that Yale executives have questioned whether they still want to acquire Manchester and Waterbury hospitals, as previously agreed.[3]