The Scope and Legal Implications of Tracking Technologies on Hospital Websites

Matthew S. McCoy, PhD
Perelman School of Medicine, University of Pennsylvania, Philadelphia; and Leonard Davis Institute of Health Economics, University of Pennsylvania, Philadelphia.

Ari B. Friedman, MD, PhD
Perelman School of Medicine, University of Pennsylvania, Philadelphia; and Leonard Davis Institute of Health Economics, University of Pennsylvania, Philadelphia.

Corresponding Author: Matthew S. McCoy, McCoy, PhD, Department of Medical Ethics and Health Policy, University of Pennsylvania, 423 Guardian Dr, Blockley Hall, Philadelphia, PA 19104 (mmcoco@penmedicine.upenn.edu).

In June 2022, STAT and The Markup published an investigative report revealing that 33 of Newsweek's top 100 hospitals had installed tracking code on their websites that surreptitiously transferred sensitive health information to Facebook. Data transfers included details about health conditions, prescriptions, and physician appointments, often linked to patients' internet protocol (IP) addresses, which, like a name or Social Security number, are considered a personal identifier under HIPAA (Health Insurance Portability and Accountability Act of 1996). As troubling as these findings were, emerging research suggests that they captured only a portion of the privacy risks patients encounter on hospital websites.

Amid mounting evidence of tracking, the US Department of Health and Human Services' Office for Civil Rights (OCR) recently issued guidance clarifying its view of HIPAA's application to tracking technologies.2 A growing number of patients have also sued hospitals under state laws for unwanted exposure to tracking.

Even if current legal penalties are not sufficient for deterrence, hospital leaders have a moral responsibility to protect patients from undue privacy risks.

In this Viewpoint, we analyze the scope and legal implications of tracking on hospital websites. We argue that widespread tracking practices may violate both HIPAA and state privacy laws and that even in cases in which legal remedies are relatively small, hospitals have ethical and pragmatic reasons to limit tracking on their websites.

The Scope of Tracking on Hospital Websites

A tracking technology (tracker) is a piece of code that captures information about how individuals interact with a website and transfers that information to a third party.2 Organizations like hospitals install trackers because tracking companies offer them functionality, such as analysis of website traffic, measurement of click-throughs generated by online advertising campaigns, and integration with social media platforms (eg, adding a Facebook "like" button to a webpage). In exchange for these services, tracking companies gain access to valuable information about website users.

WhoTracks.Me, a public database frequently cited by privacy researchers, currently includes 898 distinct trackers ranked by prevalence on the web and classified by primary function and technologic approach to tracking.4 Among the most prevalent trackers in the database are Google Analytics, which collects and analyzes site usage data, and DoubleClick, which provides advertising-related data services and is also owned by Google.

The STAT-Markup investigation exposed the prevalence and function of just 1 tracker, the Meta Pixel, across the websites of a select group of prominent hospitals. Although this focused investigative approach yielded striking findings, it was not designed to reveal the full breadth of tracking on hospital websites. Other recent studies help to complete the picture. Niforatos et al5 examined websites of 60 hospitals—including US News & World Report's 20 top-ranked hospitals—and found that all 60 had at least 1 tracker, with a median of 6 trackers per website, suggesting that hospitals' use of trackers may be more common than the STAT-Markup investigation revealed.

Friedman et al6 reached similar results in a study of all nonfederal acute care hospitals in the United States. They found that more than 98% of 3747 hospital websites included at least 1 tracker, with a median of 16 trackers per site. The study found trackers as frequently on webpages providing information about specific conditions as on hospital homepages, which is significant because although a record that someone visited a hospital homepage reveals comparatively little, that a patient spent time reading about specialists treating depression or cancer can reveal sensitive health information.

HIPAA

Hospitals' use of trackers on webpages dealing with serious or stigmatized illnesses violates most people's expectations of privacy, but does it violate HIPAA? In a December 2022 bulletin, OCR suggested that it does.2 The bulletin distinguishes between tracking on user-authenticated webpages (ie, pages requiring log-in) and unauthenticated webpages on the websites of HIPAA "covered entities," which include health plans, health care clearinghouses, and any health care providers that electronically transmit health information. The bulletin emphasizes that because trackers on unauthenticated webpages "generally have access" to what HIPAA calls "protected health information" (PHI), they must be configured in compliance with the Privacy Rule's requirements.2 But there may be HIPAA concerns even on unauthenticated webpages, the bulletin suggests. The bulletin describes that if a patient searches for physicians or appointments on an "unauthenticated...
webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage and a tracker transmits the page URL linked to the user's IP address, "the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply." This is because the information is "indicative of the individual has received or will receive health care services or benefits from the covered entity."2

This interpretation of HIPAA suggests that many hospitals may be violating the HIPAA Privacy Rule. Data transfers like those uncovered in the STAT-Markup report, which included details such as patient names and appointment information, clearly implicate HIPAA. Given the volume of tracking on hospital websites, it is reasonable to believe that similar transfers occur on at least some hospital websites beyond the 100 included in the investigation. Although Friedman et al studied only unauthenticated webpages and did not examine the contents of data transfers, they found evidence of pervasive tracking on symptom-specific webpages. Because trackers routinely transmit data that include URLs linked to user IP addresses, it is likely that many transfers from symptom-specific webpages matched the bulletin's example of possible PHI disclosure.

Covered entities may disclose PHI, including for marketing purposes, with HIPAA-compliant authorization from patients. But valid HIPAA authorization requires notification of reasons for disclosure and, if for marketing purposes, stating when remuneration is provided for the disclosure. Without such authorization, a hospital that discloses PHI through trackers for marketing uses violates HIPAA.

For several reasons, however, OCR's bulletin and HIPAA itself may have limited direct effects on hospitals' tracking. First, although the bulletin signals OCR's intention to seek civil monetary penalties for HIPAA violations based on trackers, it is not legally binding. The OCR's interpretation of HIPAA, particularly its views on unauthenticated webpage tracking, could be challenged legally. Second, even if OCR successfully imposes penalties for tracking-related violations, penalties are capped at levels relatively modest (just over $1.9 million per year) compared with health system budgets. Third, HIPAA does not have any private right of action, meaning that, although attorneys general can pursue violations in some states and individuals can file complaints to OCR, people cannot sue hospitals directly for HIPAA violations. That means that patients' concerns that hospitals have violated their HIPAA rights will not translate directly into a flood of lawsuits against hospitals.

State Laws

Even with HIPAA's limitations, hospitals' use of tracking may also violate state privacy and wiretap laws. In 2021, for example, Mass General Brigham agreed to an $18.4 million settlement with patients who claimed that the hospital system had violated their rights under Massachusetts state law by using trackers on its website without obtaining proper consent.3 State laws provide patients with a mechanism for seeking damages from hospital systems, but patients seeking damages must demonstrate harm from tracking. Although tracking companies may use information gleaned from patients' hospital website browsing to target them with unwanted, embarrassing, or misleading advertising, to exclude them from favorable offers and opportunities, linking these practices to legally recognizable harms may prove difficult.7 As part of the Mass General Brigham settlement, likely made to avoid litigation costs, Mass General denied the allegations and stated that they did not believe that any plaintiff sustained injuries due to trackers on their websites. Thus, although the lawsuit resulted in a cash settlement, it did not establish a legal record or precedent of a court's recognizing harms from tracking on hospital websites.

Conclusions

The OCR's guidance and recent lawsuits signal growing concern about hospitals' use of tracking technologies. Hospital leaders should take heed and proactively remove trackers from their websites. Even if current legal penalties are not sufficient for deterrence, hospital leaders have a moral responsibility to protect patients from undue privacy risks. Given both media scrutiny and mounting legal challenges, maintaining trackers may also cause hospitals reputational harms. Lawmakers should also consider whether new tools are needed to address modern privacy risks. HIPAA was intended to create a rule that "strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing." But nearly 30 years after its passage, the law's parameters and penalties may no longer be a match for the scale and nature of modern threats to patient privacy.