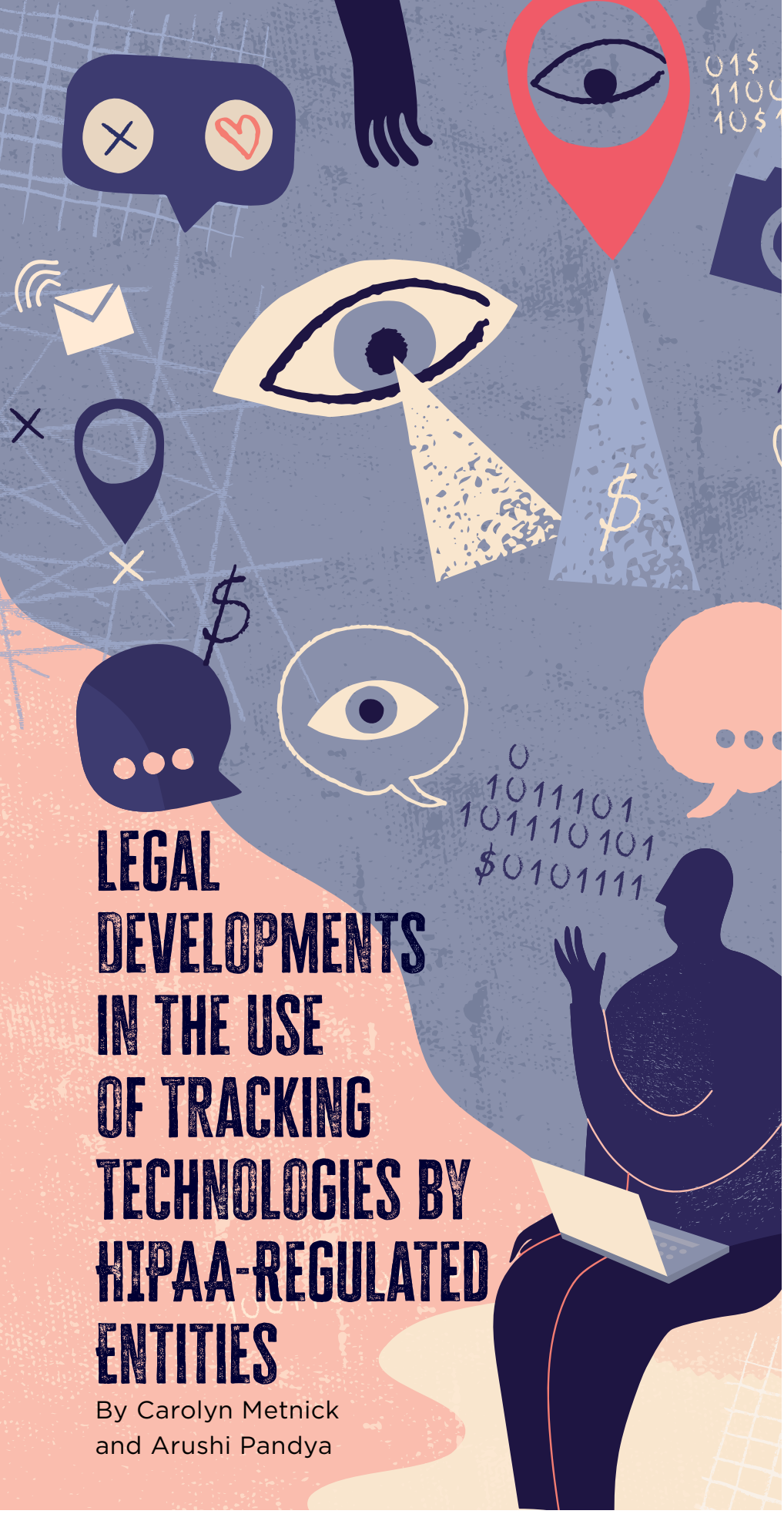

LEGAL DEVELOPMENTS IN THE USE OF TRACKING TECHNOLOGIES BY HIPAA-REGULATED ENTITIES

By Carolyn Metnick and Arushi Pandya

The regulatory landscape surrounding tracking technologies has become complex and difficult to navigate for many businesses, particularly Health Insurance Portability and Accountability Act (HIPAA)-regulated entities. It has recently seen a major shift as a result of the decision from the U.S. District Court for the Northern District of Texas in a case brought by the American Hospital Association (AHA) that challenged, and ultimately vacated, certain portions of the U.S. Department of Health and Human Services (HHS) Office for Civil Rights' (OCR) guidance on tracking technologies. Regardless of the ruling, given the rise of regulatory enforcement and litigation involving tracking technologies over the last few years, HIPAA compliance remains paramount for health care entities, which should continue to closely monitor their use of tracking technologies and the information those technologies collect.

WHAT ARE TRACKING TECHNOLOGIES?

Tracking technologies are scripts or codes that are used to collect information about a user's interaction on the internet. Such technologies include cookies, web beacons, pixels, and browser/device fingerprinting. Web tracking technologies were originally developed, and are generally utilized, for marketing and advertising purposes because they track and analyze information about a user's interactions with a particular website or application. The personal data that are collected by tracking technologies can include IP address, device identifiers, browser types, information about the use of a website, and more. This information may be used to gather analytics, provide personalized content and ads, as well as store searches and other online activity for future online use. Third-party tracking technologies collect information for a company other than the website owner and often are used to track a user's browsing behavior across multiple sites and even across various devices, such as a laptop and smartphone.

Illustration by DrAfter123 via Getty Images

These third-party tracking technologies have been widely installed on websites and have become commonly used in the health care industry, appearing on the websites of hospital systems and other providers. The industry and regulatory focus on third-party tracking technologies in health care was triggered by an investigative article that found the Meta Pixel on the websites of *Newsweek*'s top 100 hospitals in America.[1] A subsequent study of all U.S. hospitals included in the 2018 AHA Survey found that third-party tracking was present on 98.6% of hospital websites and included transfers of information to large technology companies, social media companies, and data brokers.[2] The most common third-party tracking entity was Alphabet, followed by Meta, Adobe Systems, and AT&T.[3]

OVERVIEW OF HIPAA

HIPAA governs the use and disclosure of protected health information (PHI) and establishes privacy, security, and breach notification obligations for covered entities and their business associates. Covered entities include health care providers,[4] health plans, and health care clearinghouses. Business associates include third parties who require access to PHI in order to perform a task or function for a covered entity. Under the HIPAA Privacy Rule, covered entities and their business associates must use appropriate safeguards to protect the privacy of PHI and comply with limitations on the use and disclosure of PHI.[5] The HIPAA Breach Notification Rule categorizes a "breach" as, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI and provides guidelines for appropriate notification of certain breaches of PHI. Finally, the HIPAA Security Rule requires certain administrative, physical, and technical safeguards to be implemented to protect the electronic PHI that is created, received, used, or maintained by a covered entity or business associate. The HIPAA Rules are administered and enforced by the OCR.

PHI is individually identifiable health information that is held or maintained by a covered entity or a business associate and is transmitted or maintained in any medium. The Privacy Rule provides eighteen identifiers that classify information as personally identifiable information, including IP address and any other unique identifying number, characteristic, or code. When tracking technologies are placed on a health care entity's website, the information collected and sometimes disclosed to a tracking technology vendor may include an individual's medical record number, home or email address, or dates of appointment, and therefore be considered PHI.

OCR BULLETIN

In December 2022, OCR released a bulletin regarding the "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates" (the Bulletin).[6] The Bulletin reaffirmed that HIPAA rules may apply when the information collected by regulated entities, both covered entities and business associates, through tracking technologies, or disclosed to tracking technology vendors, constitutes PHI. Consequently, regulated entities may not use tracking technologies in a manner that would result in an impermissible disclosure of PHI in violation of the Privacy Rule.

The Bulletin states individually identifiable health information collected on a regulated entity's website is PHI, even if the individual whose information is collected does not have an existing relationship with the regulated entity or the individually identifiable health information does not include specific treatment or billing information. However, a user's visit to the regulated entity's webpage must relate to the individual's past, present, or future health, health care, or payment for health care for the information collected to qualify as individually identifiable health information. The Bulletin took an expansive view—suggesting that information collected by a tracking technology could qualify as PHI because the information was "indicative that the individual has received or will receive health care services or benefits" from the regulated entity.

Notably, the Bulletin distinguishes between the implications of tracking technologies used on authenticated webpages versus unauthenticated webpages. User-authenticated webpages require a user to log in, such as a patient portal or a telehealth platform. Unauthenticated webpages, on the other hand, do not require a user to log in.

The Bulletin states regulated entities must ensure that any user-authenticated webpages that include tracking technologies only use and disclose PHI in accordance with the HIPAA Privacy Rule. Any electronic PHI collected by the tracking technologies must be protected and secured in accordance with the HIPAA Security Rule. This is because tracking technologies on an authenticated webpage can have access to PHI, such as IP address, medical record number, dates of information, and other identifying information. Further, authenticated websites are typically accessed by patients (or their caregivers), which is why such individuals have credentials, and why the information on the authenticated page is PHI. Additionally, the vendor of a tracking technology would be considered a business associate of a regulated entity if the vendor creates, receives, or maintains PHI on behalf of or to provide certain services to or for a regulated entity. If the tracking technology vendor is a business associate, then the regulated entity is obligated to enter into a business associate agreement with the vendor, as required by HIPAA.

With respect to unauthenticated webpages, if tracking technologies do not access or use PHI, which generally is the case, then HIPAA's requirements are not triggered. In the event PHI is accessed, then the use of tracking technologies would be regulated by HIPAA. The Bulletin provides examples of scenarios where visits to unauthenticated webpages do not involve PHI, such as when a user visits a hospital's webpage for information about the hospital's visiting hours and the tracking technology

gathers and transmits information on the user's IP address, geographic location, or other identifying information. The Bulletin acknowledges that a user may visit a regulated entity's website for a variety of reasons, such as research or viewing employment opportunities. Some unauthenticated webpages may become subject to HIPAA based on the information the tracking technologies collect, such as the login page of a patient portal, if the tracking technologies collect login information or registration information. Further, the Bulletin noted that unauthenticated sites that address "specific symptoms or health conditions, such as pregnancy or miscarriage, or that permit individuals to search for doctors or schedule appointments without entering credentials" may have access to PHI.

The Bulletin also provides specific HIPAA compliance obligations that are triggered when regulated entities utilize tracking technologies. For example, regulated entities must ensure they have entered into business associate agreements (BAAs) with tracking technology vendors that access PHI or the disclosure must be pursuant to an authorization or another permissible purpose under HIPAA. The regulated entity's risk analysis and risk management processes should address the use of tracking technologies, as should the regulated entity's administrative, physical, and technical safeguards. Finally, the Bulletin notes breach notification may be required in the event of an impermissible disclosure of PHI to a tracking technology vendor unless there is a low probability that the PHI has been compromised.

In March 2024, OCR updated the Bulletin to provide further clarifications around regulated entities' obligations with respect to tracking technologies. The Bulletin added examples of when visits to unauthenticated webpages may or may not involve the disclosure of PHI.

While the Bulletin reinforces and confirms that the use of tracking technologies on regulated entities' webpages do, in fact, implicate HIPAA, it also creates a complex compliance landscape for regulated entities, which face the burden of determining whether a tracking technology is collecting and disclosing PHI. If the tracking technology is found to be collecting and disclosing PHI, the regulated entity must then evaluate whether an impermissible use or disclosure occurred. The Bulletin leaves many questions unanswered, and is further complicated by the litigious landscape created by class actions.

AHA LITIGATION AND IMPACT OF RULING

AHA, in conjunction with the Texas Hospital Association, Texas Health Resources, and United Regional Health Care System, brought a lawsuit against the Secretary of HHS and the Director of OCR in response to the Bulletin in November 2023.[7] This lawsuit specifically challenged the portions of the Bulletin that considers the use of tracking technologies on regulated entities' unauthenticated webpages to be subject to HIPAA. This includes, for example, linking an IP address with viewing specific health conditions or health care providers (the "Proscribed Combination"). The complaint specifically alleged that the Bulletin, as applied to unauthenticated public webpages, (1) exceeded HHS's authority under HIPAA and the First Amendment and (2) failed to meet rulemaking requirements under the Administrative Procedure Act (APA).

The complaint stated there is a lack of reasonable basis to determine whether the Proscribed Combination sufficiently identifies an individual who visits a webpage for health, care, or payment purposes. For example, an individual may visit a medical condition webpage, but such a visit may not be in connection with the individual's health care or sought services. By concluding the Proscribed Combination constitutes individually identifiable health information subject to HIPAA, plaintiffs alleged OCR exceeded its authority. The complaint also alleged the Bulletin prohibits health care providers from disclosing information about the usage of a public webpage on health-related topics in violation of the First Amendment.

The plaintiffs argued the Bulletin failed to meet the requirements of the APA because the reasoning used by OCR to determine the Proscribed Combination as individually identifiable health information was arbitrary and capricious. Furthermore, the plaintiffs argued the Bulletin was procedurally defective because it was promulgated without a notice-and-comment period and without consulting hospitals and health systems.

In June 2024, the U.S. District Court for the Northern District of Texas issued an opinion that vacated the portion of the Bulletin regarding the Proscribed Combination.[8] The court found that the Bulletin unlawfully expanded the definition of individually identifiable health information and PHI to include data that could not reasonably identify an individual or their health condition, specifically citing that understanding a user's intent when visiting a webpage can be unknowable. The opinion noted that to qualify as PHI, information must relate to an individual's past, present, or future physical or mental health or condition, or receipt of health care or payment for health care, and identify the person or provide a reasonable basis to identify the person. The court held that OCR had exceeded its authority and vacated only the portion of the Bulletin that determines that HIPAA's prohibitions and requirements apply to circumstances where an IP address is connected with a visit to an unauthenticated webpage.

Although the court's decision does not alter the HIPAA obligations to which regulated entities are subject with respect to their authenticated webpages, it does reduce and alter the analysis of risk for the collection of information on unauthenticated sites. Regulated entities must still ensure that their use of tracking technologies on authenticated webpages complies with HIPAA, but the ruling may ease HIPAA compliance burdens for regulated entities on their unauthenticated webpages. For example, regulated entities would still

need to enter into BAAs with tracking technology vendors, as needed under HIPAA.

LOPER BRIGHT AND RELATED IMPACT

The regulatory environment surrounding tracking technologies is further muddled in light of the recent Supreme Court decision in *Loper Bright Enterprises v. Raimondo*.[9] *Loper Bright* overturned the *Chevron* doctrine, which required courts to defer to "permissible" agency interpretations when evaluating an unclear statute.[10] After *Loper Bright*, courts must exercise their own independent judgment in deciding whether an agency has acted within its statutory authority. This ruling may result in additional litigation by providing regulated entities with another avenue to challenge HHS's actions in this space in order to reduce their HIPAA compliance burdens.

TAKEAWAYS FOR HIPAA-REGULATED ENTITIES AND STEPS FOR COMPLIANCE

The *AHA* decision does not significantly alter the obligations of HIPAA-regulated entities, and such entities should not rely upon the ruling as a basis for relaxing their compliance procedures or plans. OCR's update of its guidance reflects that it prioritizes tracking technologies for enforcement and that evaluation of Security Rule compliance is a key factor in its investigations. Given the *AHA* ruling primarily impacts IP addresses gathered on unauthenticated webpages, OCR may shift its focus to authenticated webpages, but it should not be expected to decrease its investigative activities. Class actions also have not diminished in light of the *AHA* litigation. Consequently, while all webpages should be closely scrutinized and monitored, tracking technologies on authenticated webpages should receive particular attention to minimize risk, as should tracking technologies on unauthenticated sites where sensitive information or user-driven information beyond IP addresses is collected.

As such, HIPAA-regulated entities should continue to investigate their use of tracking technologies and collaborate with their legal counsel. Entities should perform an audit to determine the tracking technologies present on their websites and the information collected by such trackers. To the extent trackers are located on authenticated webpages, entities should ensure they comply with HIPAA. For example, entities should evaluate whether they have entered into a BAA with the relevant tracking technology vendor and, if not, consider whether the parties should enter into one moving forward or whether individual authorizations should be obtained. The business associate's own tracking technologies and use of the PHI it has received also should be evaluated. Further, remediation also may need to be considered, including a breach risk assessment. As publicly available tools to evaluate websites for tracking technologies become more prevalent, entities should closely review their own websites to reduce the risk of patient complaints and identification by plaintiffs' attorneys.

In addition to HIPAA, entities also should be aware of any state laws that may be implicated by the use of tracking technologies and other federal laws, such as the FTC Act. The privacy statements and claims made by regulated entities should be evaluated on an ongoing basis to confirm it accurately represents the information that is being collected. Other documentation, such as privacy notices, also should be reviewed to ensure they accurately reflect the entity's information collection practices. If a regulated entity identifies the basis for a potential impermissible disclosure of PHI through tracking technologies, it should conduct a risk assessment and make any necessary breach notifications.

Although ensuring the use of tracking technologies is in accordance with HIPAA is difficult, there are a variety of steps regulated entities can take to manage their exposure. Agency action and general litigation around the use of tracking technologies is expected to remain active and dynamic, so regulated entities should ensure they stay up-to-date on the most recent developments. By remaining proactive in scrutinizing their use of tracking technologies, regulated entities can reduce their HIPAA risks.

Carolyn Metnick *is a partner in Sheppard Mullin's Corporate Practice Group in Chicago and is a member of the Healthcare and Privacy and Cybersecurity teams.*

Arushi Pandya *is a regulatory health care and life sciences attorney in Washington, D.C., with a focus on privacy and digital health.*

ENDNOTES

1. Feathers Todd, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022).

2. Ari B. Friedman et al., *Widespread Third-Party Tracking on Hospital Websites Poses Privacy Risks for Patients and Legal Liability for Hospitals*, 42 Health Aff. 508 (2023), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11145977/#:~:text=We%20found%20that%20third%2Dparty,advertising%20firms%2C%20and%20data%20brokers.

3. *Id.*

4. In order for a health care provider to be a covered entity, it must engage in electronic transactions for which HHS has adopted a standard, which most health care providers do (although there are exceptions).

5. The HIPAA requirements for covered entities and business associates differ slightly, but for simplicity, we will not delve into the distinctions.

6. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dep't of Health & Hum. Serv., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

7. Am. Hosp. Ass'n v. Rainer, Case No. 4:23-cv-011110-P (N.D. Tex. Nov. 2023).

8. Am Hosp. Ass'n v. Becerra, No. 4:23-cv-1110, 2024 WL 3075865 (N.D. Tex. June 20, 2024).

9. 144 S. Ct. 2244 (2024).

10. Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984).