PROVIDER WEBSITES AND PATIENT PRIVACY

Understanding the legal risks of tracking technologies.

BY NANCY L. PERKINS, JD, MPP

Most ophthalmologists maintain websites to promote their practices and facilitate patient onboarding, including the submission of new patient registration forms, insurance details, and medical histories. These websites often employ tracking technologies such as cookies, pixels, and tags, which collect data about a visitor's browser or device. This information allows the website to customize its responses during future visits and optimize the user experience. Some tracking technologies are supplied by third-party vendors, such as Google and Meta, which may use the collected data for purposes beyond website functionality, including targeted advertising. This could compromise patient privacy, raising legal concerns.

THE OFFICE FOR CIVIL RIGHTS' BULLETIN ON ONLINE TRACKING TECHNOLOGIES

In late 2023, the Office for Civil Rights (OCR) at the US Department of Health and Human Services—responsible for enforcing HIPAA's privacy, security, and breach notification regulations—issued a Bulletin highlighting the risks that online tracking technologies may pose to HIPAA-covered entities, such as health care providers and health insurance plans. The OCR Bulletin states that information collected through tracking technologies on covered entity websites, mobile applications, or patient portals may include personally identifiable health information, which qualifies as protected health information (PHI) under HIPAA if created or received by a HIPAA-covered entity or its business associate. The bulletin also warns that using or sharing such information without the site visitor's consent may constitute unauthorized uses or disclosures of PHI.

DEFINING PHI IN THE DIGITAL SPACE

As noted in the Bulletin, the term *PHI* refers to individually identifiable information created or received by a HIPAA-covered entity that "relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."[1]

NANCY L. PERKINS, JD, MPP
- Counsel, Arnold & Porter, Washington, DC
- nancy.perkins@arnoldporter.com
- Financial disclosure: None

Tracking technologies typically collect information about the device an individual uses to connect to a website, such as a device ID or an Internet Protocol (IP) address. In its bulletin, the OCR asserted that this identifiable information, when combined with information about the individual's visit to certain covered entity websites, constitutes PHI under HIPAA because it indicates that the individual has requested, received, or will receive health care services or benefits from the covered entity operating the website.

For example, the OCR considers the history of an individual's browsing on a health care provider's website—such as visiting an ophthalmology practice's website to learn about cataract surgery or gather information on refractive surgery providers—to be PHI. Such information demonstrates that the individual has requested, received, or will receive health care services from that practice. The bulletin warns that, if this information is shared without the individual's authorization, the covered entity may be liable for violating HIPAA's general prohibition on disclosing PHI without proper authorization.

CONTROVERSY OVER THE OCR'S BULLETIN

Joint Communication From the OCR and Federal Trade Commission

Six months after issuing the bulletin, the OCR, together with the Federal Trade Commission (FTC), sent a joint letter to approximately 130 hospitals, telehealth providers, health app developers, and other health care industry entities. The letter warned of the "serious privacy and security risks" associated with collecting information through online tracking technologies integrated into their websites and mobile applications.[2]

Lawsuit Challenging the Bulletin

In response, in November 2023, the American Hospital Association, the Texas Hospital Association, Texas Health Resources, and the United Regional Health Care System filed a lawsuit against the OCR in the US District Court for the Northern District of Texas. The lawsuit challenged the OCR's authority to issue the bulletin and enforce the HIPAA Privacy Rule based on the Bulletin. The plaintiffs argued that the OCR erred in declaring that information collected via tracking technologies on HIPAA-regulated entities' unauthenticated public web pages (UPWs)—web pages that do not require visitor verification or login credentials—constitutes PHI.

For example, the plaintiffs contended that, even if an IP address of a visitor to a health-related UPW could be reliably associated with a specific individual, the combination of the IP address and the web page visit could not reasonably be assumed to reflect information about the individual's health, health care, or payment for health care. The plaintiffs noted that visits to UPWs might occur for reasons unrelated to personal health, such as academic or journalistic research, general curiosity about health-related topics in the news, or even accidental clicks on links. They asserted that the OCR's categorical characterization of information collected through certain tracking technologies as PHI lacks sufficient factual and legal basis.

The OCR's Revised Bulletin

Following an initial briefing, both parties filed motions for summary judgment. Shortly before its summary judgment brief was due, the OCR issued a revised bulletin suggesting that user information collected on UPWs could be considered PHI if the individual's reason for visiting the web page was related to personal health care. The OCR posted the revised bulletin with a disclaimer stating, "The contents of this document do not have the force and effect of law and are not meant to bind the public in any way." Consistent with this disclaimer, the OCR argued that the bulletin could not be challenged in court because it was not a "final agency action" subject to judicial review.

Judicial Response

The judge presiding over the case disagreed with the OCR's interpretation of its revised Bulletin.[3] The judge determined that the revised Bulletin provides guidance about mandatory legal obligations and therefore imposes substantive legal obligations. As such, the Bulletin qualifies as a "final agency action" and is subject to judicial review.

On the substantive content of the Bulletin, the judge ruled that the OCR exceeded its authority under HIPAA by stating that information collected through tracking technologies on HIPAA-regulated entities' UPWs constitutes PHI. The judge reasoned that, although an IP address can be considered identifiable information, there is no justification for concluding that health-related browsing information from a UPW linked to an IP address qualifies as health information about the individual associated with that IP address. The judge therefore found that the combination of an individual's IP address and their visit to a HIPAA-covered entity's UPW cannot automatically be classified as PHI under HIPAA.

The judge also rejected the OCR's argument that user information collected on UPWs constitutes PHI if the individual's purpose for visiting the website relates to their own health care. The judge found that such an approach would make the determination of whether information is PHI based on a subjective assessment of the "purpose and intent" of the website visitor. The judge concluded that, because HIPAA-regulated entities have no practical means of discerning the purpose or intent behind a visitor's use of an unauthenticated website or whether it pertains to the individual's health care, the OCR's focus on visitor intent lacks legal justification.

Outcome and Current Status

The judge vacated only the portion of OCR's Bulletin addressing the use of tracking technologies on UPWs. The OCR subsequently filed a notice of appeal to the US Court of Appeals for the Fifth Circuit to challenge the district court's order. However, 10 days later, the agency voluntarily withdrew

the appeal. As of this writing, the OCR has not removed the Bulletin from its website. Instead, the OCR references the court order and states that the US Department of Health and Human Services "is evaluating its next steps in light of that order."[1]

CONSIDERATIONS FOR OPHTHALMOLOGY PRACTICES

Third-Party Tools and Data Disclosure

The OCR Bulletin remains in effect as it pertains to the use and disclosure of information collected through tracking technologies on authenticated parts of a website, mobile app, or portal. Accordingly, ophthalmology practices with websites, mobile applications, or patient portals should carefully evaluate the types of tracking technologies implemented on these platforms. The review should specifically consider whether PHI is being used or disclosed via tracking technologies, including tools provided by third parties such as advertising or social media companies, in ways that may require patient authorization.

Patient Authorization and Privacy Protections

Ophthalmologists should be aware that, citing concerns about transparency and privacy, the FTC and private parties have challenged the use of certain tracking technologies on health-related websites. The FTC has settled claims in cases involving companies such as BetterHelp,[4] Monument,[5] Cerebral,[6] and GoodRx.[7] Recently, GoodRx also agreed to settle similar claims brought in a consolidated class action in the US District Court for the Northern District of California.[8]

MITIGATING RISKS IN A CHANGING LANDSCAPE

Although the change in federal administration may reduce the likelihood of federal enforcement actions, private litigants and some state authorities are likely to continue advocating for stronger protections of individual privacy. Vigilance in safeguarding the privacy and security of patient information, whether collected online or offline, therefore remains essential. ■

1. Office for Civil Rights, US Department of Health and Human Services. Use of online tracking technologies by HIPAA covered entities and business associates. Updated June 26, 2024. Accessed January 13, 2025. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html
2. Office for Civil Rights, US Department of Health and Human Services, and Federal Trade Commission. Letter re: use of online tracking technologies. Published July 20, 2023. Accessed January 13, 2025. https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf
3. *American Hospital Association v Becerra*, 4:23-cv-01110-P (ND Tex. June 20, 2024). Accessed January 13, 2025. https://casetext.com/case/am-hosp-assn-v-becerra
4. Federal Trade Commission. FTC gives final approval to order banning BetterHelp from sharing sensitive health data for advertising, requiring it to pay $7.8 million. July 14, 2023. Accessed January 23, 2025. https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising
5. Federal Trade Commission. Alcohol addiction treatment firm will be banned from disclosing health data for advertising to settle FTC charges that it shared data without consent. April 11, 2024. Accessed January 23, 2025. https://www.ftc.gov/news-events/news/press-releases/2024/04/alcohol-addiction-treatment-firm-will-be-banned-disclosing-health-data-advertising-settle-ftc
6. Federal Trade Commission. Proposed FTC order will prohibit telehealth firm Cerebral from using or disclosing sensitive data for advertising purposes, and require it to pay $7 million. April 15, 2024. Accessed January 23, 2025. https://www.ftc.gov/news-events/news/press-releases/2024/04/proposed-ftc-order-will-prohibit-telehealth-firm-cerebral-using-or-disclosing-sensitive-data
7. Federal Trade Commission. FTC enforcement action to bar GoodRx from sharing consumers' sensitive health info for advertising. February 1, 2023. Accessed January 23, 2025. https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising
8. Consolidated Class Action Complaint. Case No. 3:23-cv-00501-AMO. United States District Court for the Northern District of California. 2023. https://www.classaction.org/media/doe-et-al-v-goodrx-holdings-inc-et-al.pdf