American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

September 28, 2023

The Honorable Bill Cassidy, M.D.
Senate Committee on Health, Education, Labor and Pensions
United States Senate
Washington, DC 20510

Re: Request for Information on Health Data Privacy

Dear Senator Cassidy:

On behalf of the nearly 5,000 member hospitals, health systems and other health care organizations, and our clinician partners — including more than 270,000 affiliated physicians, 2 million nurses and other caregivers — and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) appreciates the opportunity to comment on your request for information (RFI) on data privacy and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

America's hospitals and health systems are committed to safeguarding the privacy of their patients' medical information. The AHA and its members believe that the current HIPAA rules generally offer an effective framework that restricts covered entities, like hospitals and other health care providers, from sharing patients' protected health information (PHI) without creating significant impediments to the robust use and disclosure of information necessary to support high-quality care. In addition, the decades-old HIPAA framework is now so sufficiently embedded in law and practice that any fundamental revisions would create more challenges than benefits. For these reasons, the AHA does not believe that Congress should make any major revisions to HIPAA at this time. That being said, two specific issues would benefit from congressional attention.

First, in December 2022, the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) issued a new rule regarding the use of so-called "online tracking technologies," *i.e.*, technologies that are used to collect and analyze

information about how users interact with regulated entities' websites.[1] As explained below, this rule is flawed as a matter of law and harmful as a matter of policy. As a result of the OCR rule, hospitals and health systems can no longer rely on a broad array of third-party technologies — from Google Analytics to YouTube or other video applications — that help them provide their communities with reliable health care information. Not only does this OCR rule violate HIPAA and its implementing regulations, but it inflicts meaningful harm on patients and public health. **Congress should urge OCR to withdraw the rule immediately.**

Second, hospitals and health systems currently face a patchwork of state and federal privacy requirements, which creates unnecessary regulatory burdens. The AHA has long advocated that HIPAA's requirements be the uniform, nationwide standard for protecting the privacy and security of all patient information. Because the HIPAA framework is both effective and entrenched, Congress should enact full federal preemption for HIPAA.

OFFICE OF CIVIL RIGHTS DECEMBER 2022 GUIDANCE

HIPAA and its implementing regulations "strike a balance."[2] The law "protects the privacy of people who seek care and healing," while "permit[ting] important uses of information."[3] Hospitals and health systems have long honored the balance that HIPAA strikes and take seriously their obligation to safeguard the privacy of patient records and billing statements. At the same time, they have embraced the federal government's encouragement to share non-private, health-related information when it can improve public health.

In December 2022, however, OCR precipitously upended the balance that HIPAA strikes, contravening its own efforts to encourage hospitals to share non-private healthcare information with the public. Without consulting health care providers, third-party technology vendors, or the public at large, the agency issued a sub-regulatory guidance document that has had profound effects on hospitals, health systems and the communities they serve. In this new rule, OCR took the position that when an online technology connects (1) an individual's IP address with (2) a visit to a public webpage that addresses specific health conditions or health care providers, that combination of information is subject to restrictions on use and disclosure under HIPAA. Thus, website visitors' IP addresses are protected even if they are not actually seeking medical care. In OCR's misguided view, the same HIPAA protections apply if visitors search for a medical service for a friend or relative; if they are seeking general health information

---

[1] United States Department of Health and Human Services, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html#ftnref22
[2] United States Department of Health and Human Services, Summary of the HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.
[3] *Id*.

(e.g., information about flu season or symptoms of an unknown illness); or if they are conducting academic research for a study of data on hospitals' websites. OCR's new rule violates HIPAA and its regulations. In fact, courts have already concluded that the interpretation of individually identifiable health information (IIHI) offered by HHS in its guidance "goes well beyond the meaning of what the statute can bear."[4]

Just as problematic for purposes of this RFI, OCR's new rule is simply bad public policy. As part of their information-sharing efforts, hospitals and health systems use a variety of third-party technologies to enhance their websites. Examples include:

- **Analytics tools** convert web users' interactions with hospital webpages into critical data, such as the level and concentrations of community concern on medical questions, or the areas of a hospital website on which people have trouble navigating. These tools allow hospitals to more effectively allocate resources and help community members to more easily find the health care information that they are seeking.
- **Video technologies** allow hospitals to offer a wide range of information to the public, including videos that educate the community about particular health conditions.
- **Map and location technologies** enable the provision of better information about where health care services are available, including embedded applications that provide bus schedules or driving directions to and from a community member's location.

If the OCR's new rule is permitted to stand, hospitals and health systems will be forced to restrict the use of valuable third-party technologies like these.

This issue is further exacerbated due to third-parties that decline to sign business associate agreements (BAAs) that would commit them to protecting private patient information. Hospitals and health systems are caught between OCR enforcement and these third-party vendors. Community members and public health are ultimately suffering the consequences of not having the most reliable health information available to them because hospitals and health systems cannot risk the serious consequences that flow from OCR's unlawful rule, including HIPAA enforcement actions, class action lawsuits or the loss of significant investments in existing websites.

Despite repeatedly raising concerns about this guidance and explaining why it should be withdrawn, OCR moved forward with its new rule, threatening serious consequences against hospitals that violate it. In July 2023, OCR and the Federal Trade Commission

---

[4] *Kurowski v. Rush Sys. for Health*, 2023 WL 4707184, at *4 (N.D. Ill. July 24, 2023); *see Smith v. Facebook*, 745 F. App'x 8, 9 (9th Cir. 2018) (similarly concluding that "the connection between a person's browsing history" on "publicly accessible websites" and "his or her own state of health is too tenuous" to implicate HIPAA)

wrote to approximately 130 hospital systems and telehealth providers "strongly encouraging" them "to review" and "take actions" in light of its December 2022 bulletin.[5] OCR further warned that it is "closely watching developments in this area."[6] And in a press release accompanying these warning letters, OCR stated that it is "concerned" that hospitals' use of these technologies results in "impermissible disclosures of health information" — an issue that OCR "will use all of its resources to address."[7] The press release noted, moreover, that since issuing the rule in December 2022, "OCR has confirmed its active investigations nationwide to ensure compliance with HIPAA."[8] And several months later, on Sept. 1, 2023, OCR publicly released the names of all hospitals and health systems that received its warning letter.

Congress does not need to amend HIPAA as the statute already bars OCR's new rule. AHA urges Congress to make clear to OCR that the agency should withdraw the rule immediately. AHA recommends that Congress should consider exploring how to better require entities not covered by HIPAA to protect patient privacy, especially those third-party entities that decline to sign BAAs to ensure patient privacy.

PREEMPTION

While generally preempting contrary state law, HIPAA does not preempt state law that is "more stringent" than the requirements that it mandates.[9] Specifically, state law is not preempted where: (1) state law is contrary to HIPAA; (2) relates to matters of IIHI; and (3) is more stringent than the HIPAA requirements.[10]

For all the strengths of the existing HIPAA framework, its approach to preemption has proven to be problematic. It creates unnecessary regulatory burdens on hospitals and health systems, forcing them to satisfy a myriad of legal requirements that raise compliance costs and divert limited resources that could be used on patient care. In addition, the existing state and federal patchwork of health information privacy requirements remain a significant barrier to the robust sharing of patient information necessary for coordinated clinical treatment. For instance, the patchwork of differing requirements poses significant challenges for providers' use of a common electronic health record that is a critical part of the infrastructure necessary for effectively coordinating patient care and maintaining population health.

---

[5] *HHS Office for Civil Rights and the Federal Trade Commission Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, at https://www.hhs.gov/about/news/2023/07/20/hhs-office-civil-rights-federal-trade-commission-warn-hospital-systems-telehealth-providers-privacy-security-risks-online-tracking-technologies.html.
[6] *Id*.
[7] *Id*.
[8] *Id*.
[9] 42 U.S.C. §§ 1320d-2, 1320(d)(7).
[10] *See* 45 C.F.R. § 160.202.

If Congress were to make any changes to HIPAA, it should address this problem and enact a full preemption provision. HIPAA is more than sufficient to protect patient privacy and, if interpreted correctly, it strikes the appropriate balance between health information privacy and valuable information-sharing. Varying state laws only add costs and create complications for hospitals and health systems. **As such, the AHA reiterates its long-standing recommendation that Congress strengthen HIPAA preemption**.

The AHA appreciates the opportunity to share comments regarding health data privacy. We look forward to working with you to ensure hospitals and health systems have the tools they need to continue to ensure the privacy of their patients' medical information.

Sincerely,

/s/

Stacey Hughes
Executive Vice President