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

May 22, 2023

Melanie Fontes Rainer
Director, Office for Civil Rights
Department of Health and Human Services
Hubert H. Humphrey Building
200 Independence Avenue, S.W., Room 515F
Washington, DC 20201

Re: HIPAA Privacy Rule to Support Reproductive Health Care Privacy; 88 Fed. Reg. 23506 (RIN 0945–AA20) (April 17, 2023)

Dear Director Fontes Rainer:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinical 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) strongly supports the Office of Civil Rights' (OCR) proposed rule. The AHA agrees with OCR that a "positive, trusting relationship between individuals and their health care providers is essential to an individual's health and well-being."[1] **The proposed rule will enhance provider-patient relationships by providing heightened privacy protections for information about care that is lawful under the circumstances in which it is provided, but may nonetheless get swept up in criminal, civil or administrative investigations**.

At the same time, the AHA has serious concerns about a recent, related OCR policy: the December 2022 guidance on the "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates" (hereinafter "Online Tracking Guidance"). This guidance — ostensibly issued with the same worthy goal in mind as the proposed rule — is too broad and will result in significant adverse consequences for hospitals, patients and the public at large. **In particular, by treating a mere IP address as protected health information under HIPAA, the Online Tracking Guidance will <u>reduce</u> public access to credible health information.**

[1] 88 C.F.R. 23506, 23508.

As you finalize the proposed rule, the AHA urges you to (1) consider whether the Online Tracking Guidance remains necessary in light of the heightened privacy protections in the proposed rule; (2) if OCR continues to believe that some form of the Online Tracking Guidance remains necessary, amend that guidance to better reflect the realities of online activity by hospitals and health systems; and (3) potentially seek public comment before reissuing it.

OCR Should Finalize the Proposed Amendments to Its Privacy Rule

The proposed rule rests on a series of unobjectionable principles, all of which are clearly and concisely set forth on page 23508:

- "The prospect of releasing highly sensitive [protected health information (PHI)] can result in medical mistrust and the deterioration of the confidential, safe environment that is necessary to quality health care, a functional health care system, and the public's health generally."

- "If individuals believe that their PHI may be disclosed without their knowledge or consent to initiate criminal, civil, or administrative investigations or proceedings against them or others based primarily upon their receipt of lawful reproductive health care, they are likely to be less open, honest, or forthcoming about their symptoms and medical history. As a result, individuals may refrain from sharing critical information with their health care providers, regardless of whether they are seeking reproductive health care that is lawful under the circumstances in which it is provided."

- "If an individual believes they cannot be honest about their health history, the health care provider cannot conduct an appropriate health assessment to reach a sound diagnosis and recommend the best course of action for that individual."

- "Heightened confidentiality and privacy protections enable an individual to develop a trust-based relationship with their health care provider and to be open and honest with their health care provider. That health care provider is then more likely to provide a correct diagnosis and aid the individual in making informed treatment decisions."

- "[A]n individual's lack of trust in their health care provider to maintain the confidentiality of the individual's most sensitive medical information and a lack of trust in the medical system more generally may have significant repercussions for the public's health more generally. Individuals who are not candid with their health care providers about their reproductive health care may also withhold information about other matters that have public health implications."

The AHA's hospital and health system members agree with these propositions. Lawful medical care should not carry adverse legal consequences. Patients and providers should not have to risk government enforcement action based on care that is permissible where it is provided. Accordingly, the AHA strongly supports policies that reduce the risk of inappropriate enforcement and thus foster trust within the patient-provider relationship.

The proposed rule advances these important goals by making only modest changes to the Privacy Rule. By simply requiring requesters to attest to the fact that they are not seeking to use health information to investigate or penalize the lawful provision of health care, the proposed rule appropriately balances patient/provider privacy with the government's occasional need for health information. The AHA welcomes these commonsense amendments to the Privacy Rule.

In addition, the proposed rule correctly ensures that hospitals and health systems are <u>not</u> required to investigate the accuracy of an attestation.[2] Any final rule should reiterate — indeed, emphasize — that hospitals and health systems will not be burdened by having to question the validity of an attester's statements, so long as those statements are objectively reasonable.

Relatedly, the AHA would welcome other measures that would reduce the burden on hospitals and health systems. For example, the AHA would support OCR creating a model attestation form, coupled with a guarantee that a provider's good faith reliance on such a form is objectively reasonable. It also may be helpful to require requesters to attach the relevant legal process (*e.g.*, a subpoena or administrative order) to that attestation to provide further assurance that the request is legitimate. Similarly, OCR specifically sought comment on whether "requesters of PHI should be required to name the individuals whose PHI they are requesting, or if describing a class of individuals whose PHI is requested is sufficient."[3] Allowing bulk requests would not only increase costs and burdens for covered entities, but they would raise unique privacy concerns about why any requester would seek so much information. Therefore, to minimize administrative burdens on hospitals and to ensure a reasonable scope for requests (and, in turn, attestations), the AHA would support a requirement for individualized requests.

OCR Should Suspend or Amend Its December 2022 Online Tracking Guidance

---

[2] *Id*. at 23536 ("The Department does not propose to require a regulated entity to investigate the validity of an attestation provided by a person requesting a use or disclosure of PHI; rather, a regulated entity would be able to rely on the attestation provided that it is objectively reasonable under the circumstances for the regulated entity to believe the statement required by 45 CFR 164.509(c)(1)(iv) that the requested disclosure of PHI is not for a purpose prohibited by 45 CFR 164.502(a)(5)(iii).").
[3] *Id*. at 23536.

In December 2022, OCR issued guidance regarding the use of online tracking technologies, *i.e*., technologies that are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications. The AHA understands that this guidance may have been motivated — at least in part — by the same concerns as the proposed rule.[4] **Regrettably, the Online Tracking Guidance errs by defining PHI too broadly — specifically, to include all IP addresses.[5] As a result, the guidance will inadvertently impair access to credible health information. It should be suspended or amended immediately.**

Americans are increasingly reliant on digital platforms for health information. According to a March 2023 report by the National Quality Forum, "[a]pproximately 74 percent of surveyed Americans use search engines to start their patient journey."[6] But online health information "can be disconcerting, confusing, and even misleading, leaving the onus on the consumer to decipher the information."[7] And as Surgeon General Vivek H. Murthy recently explained, "Health misinformation is a serious threat to public health. It can cause confusion, sow mistrust, harm people's health, and undermine public health efforts. Limiting the spread of health misinformation is a moral and civic imperative that will require a whole-of-society effort."[8]

It is therefore critical that consumers who use the internet to obtain health information visit trustworthy, helpful and accurate sources. Hospitals and health systems play an important role in this regard. Our members' digital platforms are typically the best sources of health information. For this reason, Surgeon General Murthy specifically recommended that medical professionals, like our hospital and health system members, use "technology and media platforms to share accurate health information with the

---

[4] *See, e.g*., 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 ("Examples of unauthenticated webpages where the HIPAA Rules apply include … [t]racking technologies on a regulated entity's unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage."); *id*. ("For example, the HIPAA Rules apply to any PHI collected by a covered health clinic through the clinic's mobile app used by patients to track health-related variables associated with pregnancy (e.g., menstrual cycle, body temperature, contraceptive prescription information).").

[5] As you know, an IP address is simply a long string of numbers assigned to every device connected to a network that uses the Internet. Critically, the IP address identifies the computer, smart phone, tablet or other device, whether it is in someone's home, office, a public library, apartment building or somewhere else. As such, that device could be associated with a particular person or it could be shared by many different people.

[6] National Quality Forum, *Issue Brief: Improving the Accessibility of High Quality Online Health Information* 1 (Mar. 14, 2023), https://www.einnews.com/pr_news/622101919/high-quality-health-info-online-must-be-accessible-says-issue-brief-from-nqf-with-support-from-youtube-health (hereinafter National Quality Forum Study).

[7] *Id*.

[8] Vivek H. Murthy, *Confronting Health Misinformation: The U.S. Surgeon General's Advisory on Building A Healthy Information Environment* 2 (2021), https://www.hhs.gov/sites/default/files/surgeon-general-misinformation-advisory.pdf.

public."[9] What's more, the AHA is well-aware that a "wide gap in accessibility exists between the information from credible sources and the information that consumers find, understand, and use" for "consumers affected by digital access, health literacy, and other factors related to health equity and disparities."[10] Through the use of their websites, apps and other digital platforms, hospitals and health systems are able to reach underserved communities that would not otherwise have access to reliable health information.

The Online Tracking Guidance aggravates the risk of health misinformation by treating a mere IP address as a unique identifier under HIPAA. In particular, the guidance errs by concluding that IP addresses constitute PHI *whenever* they are shared with a third party, regardless of the context surrounding when someone visits a regulated entity's website. Under the guidance, an IP address is protected even if consumers are not actually seeking medical care. The same HIPAA protections apply if a consumer is searching for a physician or medical service, seeking general health information (*e.g*., information about vaccines, flu season, or symptoms of an unknown illness), or merely looking for information about visiting hours, facility locations, cafeteria menus or any of the multitude of reasons one might go to a hospital's website. In addition, an IP address is treated as HIPAA-protected even though that address provides no indication whatsoever whether the person using that computer is a potential patient, a friend or relative of that patient, or just a curious online visitor.

Critically, if an IP address, in and of itself, is treated as a unique identifier under HIPAA, hospitals and health systems will be forced to restrict the use of certain technologies that help improve community access to health information. For example, many hospitals use valuable online tools that sometimes require them to provide IP addresses to third-party vendors, including:

- **Analytics technologies.** These tools capture and report upon key events such as webpage views and clicks. Analytics technologies allow hospitals to optimize their online presence to reach more members of the community, including members of the community most in need of certain healthcare information. And beyond healthcare information, analytics tools allow hospitals to actually reach more patients and expand access to underserved communities. For example, depersonalized IP address data may be used to predict a geographic area's needs. This allows hospitals to expand services (*e.g*., OB/GYN, children's services, or other specialties) to new areas, including areas and populations that have been historically underserved. As such, the guidance will limit access to quality care by impairing the ability of

[9] *Id*. at 10; *see id*. ("[P]rofessional associations can equip their members to serve as subject matter experts for journalists and effectively communicate peer-reviewed research and expert opinions online.")
[10] National Quality Forum Study at 1.

health systems to understand and predict the real demand for services in their communities.

- **Translation services.** Some hospitals contract with third parties to translate parts of their websites, so that non-English speakers can access vital healthcare information. Failure to optimize these translation services will hit vulnerable communities, who are already heavily impacted by health misinformation.
- **Map and location applications.** Some hospitals use third-party services to provide better information about where healthcare services are provided.
- **Social Media.** Some health systems use social medial tools to drive traffic to websites containing trustworthy sources of information. Americans heavily rely on social media platforms for health information. These platforms are typically free to use, which makes them accessible to people of all income levels. Likewise, many social media platforms require only a mobile phone, not a computer. Users of social media include: 69% of those making an annual household income of $30k or less; 64% of those with high school education or less; 80% of the Hispanic population and 77% of the black population.[11] These populations will be particularly disadvantaged if hospitals and health systems can no longer rely on social media to put out credible health information.

Hospitals can only use these technologies with the help of third party vendors. But those vendors often refuse to comply with the Online Tracking Guidance because they are not subject to HIPAA's strictures. Hospitals are now caught in the middle. **The Online Tracking Guidance puts hospitals and health systems at risk of serious consequences — including class action lawsuits,[12] HIPAA enforcement actions, or the loss of tens of millions of dollars of existing investments in existing websites, apps and portals — for a problem that ultimately is <u>not</u> of their own making.**

Take, for example, Google Analytics. In response to the Online Tracking Guidance, Google refuses to enter into any business associate agreements and that covered entities should simply stop using Google Analytics.[13] Prior to this, many hospitals had

---

[11] Pew Research Center, Social Media Fact Sheet (Apr. 7, 2021), *at* https://www.pewresearch.org/internet/fact-sheet/social-media/?tabId=tab-ad42e188-04e8-4a3c-87fb-e101714f1651

[12] In recent months, plaintiffs' attorneys have used the Online Tracking Guidance against regulated entities and in groundless class action litigation. This is particularly problematic during a time of decreased reimbursements, increased labor costs and supply chain shortages.

[13] *See* HIPAA and Google Analytics, *at* https://support.google.com/analytics/answer/13297105?hl=en ("Can Google Analytics be used in compliance with HIPAA? … Google makes no representations that Google Analytics satisfies HIPAA requirements and does not offer Business Associate Agreements in

made the reasonable choice of working with Google to reach more consumers with better-designed websites and better-presented health information. Now, the Online Tracking Guidance has caused Google (and many other similar vendors) to abandon support of hospitals and health systems, while presumably not abandoning support of more questionable sources of health-related "information" that are not subject to HIPAA.

We respectfully request that OCR address this situation — particularly in light of the proposed rule:

- *First*, we ask OCR to consider whether the Online Tracking Guidance is necessary if the proposed rule is finalized. If, as AHA believes, that guidance is no longer necessary, OCR should suspend it immediately.

- *Second*, if OCR concludes otherwise, we ask that OCR amend that guidance to make clear that (1) IP addresses alone do not qualify as unique identifiers under HIPAA because they do not individually identify a person; or (2) if OCR nonetheless wishes to protect IP addresses, it do so only for IP addresses provided via authenticated (*i.e*., nonpublic) webpages like password-protected patient portals that are more likely to contain private personal health information. With these minor amendments, hospitals would be able to provide necessary health information and education to their communities, while protecting privacy consistent with HIPAA's goals.

- *Third*, if OCR is unwilling to make these simple changes to its Online Tracking Guidance, it should seek public comment via an RFI or notice-and-comment rulemaking (rather than issuing sub-regulatory guidance that did not benefit from *any* input by regulated entities). This is a complex subject, with legal, technological and practical nuances. OCR would benefit greatly from public participation. *See generally* Memorandum from Barack Obama, President of the U.S., to the Heads of Executive Departments and Agencies (Jan. 21, 2009) ("Public engagement enhances the Government's effectiveness and improves the quality of its decisions. Knowledge is widely dispersed in society, and public officials benefit from having access to that dispersed knowledge.")

- *Fourth*, because any issues related to the release of IP addresses to third parties is ultimately caused by the decisions of third-party vendors, it seems more suited to regulation by the Federal Trade Commission — not OCR. As the proposed rule itself notes, "the Federal Trade Commission (FTC) has recognized that

---

connection with this service."); *cf*. Geoffrey A. Fowler, Google promised to delete sensitive data. It logged my abortion clinic visit, *Washington Post* (May 9, 2023), *at* https://www.washingtonpost.com/technology/2023/05/09/google-privacy-abortion-data/ ("Google offered a partial solution: It would proactively delete its trove of location data when people visited "particularly personal" places, including abortion clinics, hospitals and shelters. Nearly a year later, my investigation reveals Google isn't doing that in any consistent way.").

> information related to personal reproductive matters is 'particularly sensitive.'… As a result, the FTC has committed to using the full scope of its authorities to protect consumers' privacy, including the privacy of their health information and other sensitive data."[14] Here, OCR should work with the FTC to identify and regulate third parties that refuse to protect health information, rather than putting hospitals to the Hobson's Choice created by the December 2022 Online Tracking Guidance.

The AHA remains eager to discuss our members' concerns about the Online Tracking Guidance at your earliest convenience. In the meantime, as noted above, the AHA supports the related privacy protections set forth in the proposed rule. We appreciate your consideration.

Sincerely,

/s/

Melinda Reid Hatton
General Counsel and Secretary

---

[14] 88 C.F.R. at 23510 (quoting Kristin Cohen, ''Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data,'' Federal Trade Commission Business Blog (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-healthand-other-sensitive-information-ftc-committedfully-enforcing-law-against-illegal); *see* FACT SHEET: President Biden to Sign Executive Order Protecting Access to Reproductive Health Care Services (July 8, 2022), *at* https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/08/fact-sheet-president-biden-to-sign-executive-order-protecting-access-to-reproductive-health-care-services/ ("The President's Executive Order takes additional steps to protect patient privacy, including by addressing the transfer and sales of sensitive health-related data, combatting digital surveillance related to reproductive health care services, and protecting people seeking reproductive health care from inaccurate information, fraudulent schemes, or deceptive practices. … The President has asked the Chair of the Federal Trade Commission to consider taking steps to protect consumers' privacy when seeking information about and provision of reproductive health care services. The President also has directed the Secretary of HHS, in consultation with the Attorney General and Chair of the FTC, to consider options to address deceptive or fraudulent practices, including online, and protect access to accurate information.").