

June 14, 2023

The Honorable Xavier Becerra  
Secretary  
U.S. Department of Health and Human Services  
200 Independence Avenue, SW  
Washington, DC 20201

Re: HIPAA Privacy Rule To Support Reproductive Health Care Privacy (RIN: 0945-AA20)

Dear Secretary Becerra:

On behalf of the physician and medical student members of the American Medical Association (AMA), I am pleased to offer our comments on the Notice of Proposed Rulemaking entitled, “HIPAA Privacy Rule To Support Reproductive Health Care Privacy,” (NPRM) published by the Office for Civil Rights (OCR), Office of the Secretary, Department of Health and Human Services. While the AMA appreciates the efforts to protect the privacy of reproductive health care information, we encourage OCR to apply these protections more broadly and to further align HIPAA with the approach recently proposed in the agency’s NPRM on Confidentiality of Substance Use Disorder (SUD) Patient Records (Part 2 NPRM).<sup>1</sup> In so doing, the compliance burden would be more appropriately redistributed from resting entirely on the shoulders of health care providers, and would be shared by those requesting this sensitive data.

### ***Scope of Proposed Protections***

#### **a. Definition of Information Subject to the Proposed Prohibition**

AMA has extensive policy advocating for maintaining the privacy of patient information,<sup>2</sup> the preservation and expansion of access to reproductive health services,<sup>3</sup> and for the protection of physicians who provide reproductive health care and patients who receive such care.<sup>4</sup>

---

<sup>1</sup> Confidentiality of Substance Use Disorder (SUD) Patient Records, 87 Fed. Reg. 74216, 74253 (proposed December 2, 2022).

<sup>2</sup> [3.1.1 Privacy in Health Care; Patient Privacy and Confidentiality H-315.983](#); [Police, Payer, and Government Access to Patient Health Information H-315.975](#); [Confidentiality and Privacy Protections Ensuring Care Coordination and the Patient-Physician Relationship H-315.964](#); [Right to Privacy in Termination of Pregnancy H-5.993](#).

<sup>3</sup> [Preserving Access to Reproductive Health Services D-5.999](#); [Expanding Support for Access to Abortion Care D-5.996](#); [Support for Access to Preventive and Reproductive Health Services H-425.969](#).

<sup>4</sup> [Violence Against Medical Facilities and Health Care Practitioners and Their Families H-5.997](#); [Oppose the Criminalization of Self-Managed Abortion H-5.980](#); [Support for Physicians Practicing Evidence-Based Medicine in a Post Dobbs Era D-5.998](#).

Our policy further supports extending this protection to other sensitive medical information.<sup>5</sup> In response to OCR’s request for comment on the definition of “Reproductive Health Care” and whether OCR should prohibit uses or disclosures of highly sensitive protected health information (PHI), we urge the agency to broaden the definition of patient information that will be afforded additional protections under these proposals.

Vulnerable patient groups are increasingly being targeted by state legislation that aims to curtail their rights to access evidence-based health care.<sup>6</sup> Physicians providing evidence-based health care to these individuals are fellow targets with their patients, of restrictive state laws which seek to inappropriately interfere in the patient-physician relationship.

The need to apply heightened protections to special categories of PHI must be balanced with the competing priority of facilitating the flow of data to support optimal health outcomes, especially in the face of rising U.S. maternal mortality rates, which are disproportionately high for Black women.<sup>7</sup>

In order to continue the support of beneficial data sharing while protecting patients and medical providers from those who seek to use an individual’s PHI in civil or criminal proceedings, AMA suggests that the proposed definition of Reproductive Health Care be broadened to include other types of sensitive medical information which may subject the patient or care provider to civil or criminal liability. Thus, the proposed definition at 42 CFR § 160.103 would be:

“*Sensitive Personal Health Care* means care, services, or supplies related to the health of the individual which could expose any person to civil or criminal liability for the mere act of seeking, obtaining, providing, or facilitating such health care.”

The above definition would protect reproductive health care information as well as gender-affirming care and provide a federal baseline of protection for any health care that becomes the target of states that seek to inappropriately interfere in the patient-physician relationship. Because the above definition would define the scope of data protected by the proposed prohibition on disclosures for civil or criminal proceedings, it would serve to shield patients and providers who receive and render health care, while leaving the flow of data for all other purposes, unimpeded. Throughout the NPRM proposals, where “reproductive health care” appears, the phrase “sensitive personal health care” could be substituted seamlessly.

---

<sup>5</sup> [Code of Medical Ethics - Privacy, Confidentiality & Medical Records \(3.2 Confidentiality\)](#); [HIV/AIDS Reporting, Confidentiality, and Notification H-20.915](#); [Discrimination and Criminalization Based on HIV Seropositivity H-20.914](#); [Medical Spectrum of Gender D-295.312](#); [Opposing Mandated Reporting of People Who Question Their Gender Identity H-65.959](#); [Health Care Needs of Lesbian, Gay, Bisexual, Transgender and Queer Populations H-160.991](#); [Support of Human Rights and Freedom H-65.965](#); [Preventing Anti-Transgender Violence H-65.957](#); [Code of Medical Ethics - Physicians & the Health of the Community \(8.5 Disparities in Health Care\)](#).

<sup>6</sup> The Human Rights Campaign has declared a National State of Emergency for LGBTQ+ Americans as over 75 anti-LGBTQ bills have been signed into law in 2023, doubling the number passed in 2022, which had set a previous record. <https://www.hrc.org/campaigns/national-state-of-emergency-for-lgbtq-americans>, accessed June 7, 2023.

<sup>7</sup> *The U.S. Maternal Mortality Crisis Continues to Worsen: An International Comparison*, The Commonwealth Fund December 1, 2022, available at: <https://www.commonwealthfund.org/blog/2022/us-maternal-mortality-crisis-continues-worsen-international-comparison>.

b. The HIE Problem

The operations of health information exchanges (HIEs)<sup>8</sup> have emerged as a significant privacy concern. The AMA has heard from numerous physicians that PHI regarding lawfully rendered health care is crossing state lines and being used against patients in states where those services are prohibited.

- A health center that is setting up reproductive health care services recently expressed concern regarding a large electronic health record (EHR) developer, one of the largest providers of health information technology, sharing this information if their patient left California, as many of their patients are migrant workers.
- Individual providers and small clinics have limited powers of negotiation or influence over EHR developers. EHR developers are reluctant to support physicians in protecting certain medical information—even to meet patients’ preferences.
- The patient and provider community are concerned that many EHRs and HIEs share information with non-covered entities such as social services. Several have voiced concern that patient PHI is disseminated unsolicited, to venues that put patients, and possibly care providers, at risk.
- Medical providers may resort to encouraging patients not to sign up for the large EHR developer’s national data exchange network (or to turn off the sharing they may have now) which will block all their data from being shared.

The confusion is exacerbated by the fact that HIEs are generally not HIPAA covered entities, *unless* they perform certain functions requiring access to PHI, which make them a business associate subject to the HIPAA Privacy Rule.<sup>9</sup>

Clarifying guidance is urgently needed to stem eroding confidence in the patient and provider community that PHI will not be shared beyond the wishes of, and to the detriment of, the patient and physician. Successful implementation of these proposals will depend upon vigorous and intentional efforts to educate patients and providers on practical compliance measures, so that data sharing is not frozen in fear of triggering penalties under a complex and confusing regulatory scheme.

OCR has made one statement that would be difficult to overemphasize: “Covered entities **may** provide greater protections than required by the Privacy Rule. (emphasis in the original)<sup>10</sup>

---

<sup>8</sup> HIEs, sometimes referred to as Health Information Exchange Organizations or “HIOs,” are entities that assist in the sharing and exchanging of medical information between healthcare providers and other authorized individuals/entities. *What is an HIE/HIO?*, Valley Health System, <https://www.valleyhealth.com/health-information-exchange#:~:text=A%20Health%20Information%20Exchange%20or,important%20medical%20information%20about%20you>, accessed May 31, 2023. Note that HHS-OCR uses the term HIO to denote a “health information organization,” (see footnote 9, *infra*) adding to the definitional ambiguity associated with these entities and the privacy rules which apply to them.

<sup>9</sup> See, e.g., *The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment*, published by HHS-OCR: <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/introduction.pdf>, accessed May 31, 2023.

<sup>10</sup> Webinar: “Protecting the Privacy of Reproductive Health Information Post Dobbs,” Slide 25, presented by HHS-OCR, hosted by American Health Lawyers Association, May 31, 2023. Available at: <https://educate.americanhealthlaw.org/local/catalog/view/product.php?productid=1062>.

Unfortunately, that message is often lost in efforts to avoid noncompliance with HIPAA and the Information Blocking Rules, as discussed below.

The AMA is committed to assisting with educational efforts, not only with respect to the mechanics of information sharing permitted under the law, but also on the benefits to patients of the new protections to increase their confidence in sharing full information with their care provider. Part of this educational campaign should be aimed at ensuring patients understand the implications of the forthcoming Final Rule.

*New Category of Prohibited Uses and Disclosures Introduces Unprecedented Provider Liability*

As written, the proposed prohibition at §164.502(a)(5)(iii) states that a covered entity may not use or disclose PHI for a criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating reproductive health care (we suggest “sensitive personal health care,” as discussed above). This proposal would render a provider liable for a HIPAA violation that they are powerless to prevent, as the covered entity would be responsible for the actions of the PHI recipient when that recipient uses the PHI for a prohibited purpose. The PHI recipient, in turn, may not have the present intention to use the PHI for a prohibited purpose and may not decide until later to use the PHI against the patient, provider, or other individual. In such a case the provider is nonetheless liable for violating HIPAA because their PHI disclosure was ultimately used for a civil or criminal proceeding against an individual.

A further problem with the proposed prohibition under §164.502(a)(5)(iii)(C) is that it obligates medical providers to undertake the impossible task of determining whether care previously provided by another covered entity, which appears in their patient’s medical record, was lawfully provided. Per §164.502(a)(5)(iii)(C) if the prior care was lawfully provided, then the PHI is protected from disclosure and if it was not, the protection does not apply. A physician whose patient presents with complications from a terminated pregnancy, for example, must go through an independent investigation to determine where that event occurred, and a subsequent legal analysis to determine whether the care provided was lawful. This approach is patently impossible and an inappropriate delegation of duties to medical professionals. The above scenarios represent unintended but serious consequences of holding covered entities solely responsible for post-disclosure uses of PHI by others.

To address this issue, AMA suggests a two-part approach:

First, OCR should clarify that a covered entity has the right to require an attestation, as otherwise provided for in this NPRM and as discussed below, **at their discretion**, and to decline any request for PHI when the requester refuses to provide the attestation. This practice would not impede the beneficial flow of patient data, as the attestation to be provided is a low threshold—simply, that the PHI will not be used against an individual “for the mere act of seeking, obtaining, providing or facilitating” sensitive personal health care.<sup>11</sup> If medical providers are to be held liable for HIPAA violations based on the actions of a third party, then they need to be equipped with the right to require an attestation that the party requesting PHI, will not use it for a prohibited purpose under the proposed regulations.

---

<sup>11</sup> Proposed 42 CFR §164.502(a)(5)(iii)(D) states a rule of construction clarifying that an otherwise permitted use or disclosure of PHI is not prohibited by this section “unless such use or disclosure is primarily for the purpose of investigating or imposing liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care [AMA suggests ‘sensitive personal health care’].” HIPAA Privacy Rule To Support Reproductive Health Care Privacy, 88 Fed. Reg. 23506, 23553 (proposed April 17, 2023).

Secondly, to appropriately allocate responsibility for HIPAA compliance for these PHI disclosures, we strongly recommend that in addition to giving covered entities the right to require an attestation at their discretion, that OCR clarify that **a covered entity will only be found in violation of the proposed prohibited disclosure if the covered entity had contemporaneous actual knowledge** that the PHI being requested was “for the purpose of investigating or imposing liability on any person for the mere act of seeking, obtaining, providing, or facilitating”<sup>12</sup> sensitive personal health care. The “actual knowledge” criterion was articulated in the NPRM proposals addressing defective attestations,<sup>13</sup> and is also appropriately incorporated as suggested here, in an assessment of whether a covered entity violated the proposed prohibition on PHI disclosure.

As in the above discussion, the party who is requesting PHI is in the best position to determine how it will be used, and whether that use is permitted under the proposed rule; accordingly, a covered entity must be given the right to require an attestation from the person seeking the PHI disclosure.

For these reasons, AMA strongly recommends that **OCR provide covered entities with the right to require an attestation at their discretion and to clarify that covered entities will not be in violation of a prohibited disclosure unless they had actual knowledge**. To impose any other liability scheme for the subject PHI disclosures, amounts to imposing vicarious liability on a medical provider for the actions of a third party.

Finally, in addition to a clear statement that only those covered entities with actual knowledge that the requested PHI was for a prohibited purpose will be liable for violating the proposed prohibition of PHI disclosure, it will be necessary for HHS to clarify that the covered entity’s right to require an attestation at their discretion, and to deny the request for PHI absent an attestation, will not constitute prohibited Information Blocking under regulations promulgated by the Office of the National Coordinator for Health Information Technology (ONC).<sup>14</sup>

As this NPRM and the recent ONC proposed rule on interoperability and information sharing<sup>15</sup> were published within a two-day period, confusion over compliance requirements is rampant in the regulated community, as one would expect. The AMA requests that OCR encourage ONC to echo OCR’s clarifying guidance to assuage concerns in the regulated community that complying with one HHS agency’s regulations will not incur a violation of another HHS agency’s regulations. The confusion that already exists exacerbates the tremendous potential that the proposals outlined in this NPRM have, to create logjams in data sharing to the detriment of patient care, as discussed below.

To streamline the beneficial flow of patient data, covered entities must be allowed to request an attestation such as that described in the NPRM from every person who requests that they disclose PHI, as noted above. This approach would allow the attestation to be incorporated into workflow processes without impeding information sharing, as the only entities who will be delayed or denied receiving the PHI they seek, are those who request PHI to use against an individual for the mere fact of providing, receiving, or facilitating

---

<sup>12</sup> Ibid.

<sup>13</sup> *Id.*, at § 164.509(b)(2)(iv).

<sup>14</sup> In recognition of OCR’s usual practice of declining to comment on regulations promulgated by another agency, a clear statement that a covered entity will be acting lawfully by declining a PHI request from any person that declines to provide an attestation under this NPRM, and will not, on that basis, be found to have violated any Departmental regulations, could go a long way to reassure covered entities that they can act in good faith with impunity, when they request the attestation and decline the PHI disclosure when it is not forthcoming.

<sup>15</sup> Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing, 88 Fed. Reg. 23746 (proposed April 18, 2023).

sensitive personal health care; those, and only those persons, would be unable to attest that their purpose is not prohibited by the proposed rule.

#### *Attestation Requirement*

Just as the proposed prohibited disclosure discussed above, should reallocate responsibility for the subsequent use of information to the requester of PHI who will use it, rather than the covered entity who must rely on the requester's representations as to their intended use, the proposals regarding attestation requirements for law enforcement and civil proceedings (among specified others)<sup>16</sup> present an inappropriate compliance burden for covered entities.

Under this proposal, a covered entity that receives a request for PHI "potentially related to reproductive health care" must obtain a signed attestation that the use or disclosure is not for a prohibited purpose (which is, that the PHI will not be used against an individual "for the mere act of seeking, obtaining, providing or facilitating" sensitive personal health care).

This proposal again demonstrates the difficulty faced by a medical provider who must determine whether a PHI request is "potentially related" to sensitive personal health care. If so, an attestation is required. If not, the disclosure, if otherwise permissible, is allowed.

Resolving this problem presents another opportunity to further align 42 CFR Part 2, regarding privacy of substance use disorder (SUD) patient records, with HIPAA. The alignment of these two statutory regimes is a long-standing objective of HHS and is widely supported by the patient and provider community.

A salient feature of 42 CFR Part 2, is that it is worded so as to protect patient information without specifying in each instance who the actor is in each scenario, for example: "A court order under the regulations of this part may authorize disclosure of confidential communications made by a patient . . . only if the disclosure is necessary to protect against an existing threat to life or serious bodily injury . . ." (42 CFR § 2.63 – Confidential communications).

This is a useful approach to apply heightened protections to sensitive personal medical information, as contemplated in the NPRM under consideration; the restriction applies to the document (for Part 2, a court order, for this NPRM, it would be the attestation), rather than an approach that focuses entirely on covered entities.

For individuals requesting PHI under proposed § 164.509 where an attestation is required, which includes law enforcement, judicial and administrative proceedings, health oversight activities and disclosures to coroners and medical examiners, **OCR would be well advised to trade the cumbersome and unworkable approach of requiring medical providers to ascertain motive and require an attestation, for the streamlined approach that Part 2 uses, imposing the requirement to provide an attestation on the requester seeking patient information.**<sup>17</sup>

---

<sup>16</sup> Proposed 42 CFR § 164.509(a) provides that a covered entity may not disclose certain PHI, without first obtaining an attestation that it is valid under these proposals, for health oversight activities, judicial and administrative proceedings, law enforcement purposes, or disclosures to coroners and medical examiners.

<sup>17</sup> See 42 CFR § 2.65 – Procedures and criteria for orders authorizing use and disclosure of records to criminally investigate or prosecute patients. Substituting the references to court orders under Part 2, with references to an attestation under the current proposal, an alternative for proposed 45 CFR § 164.509 would read:

Again, the twin objectives of public health stakeholders are to protect the privacy of sensitive medical information while facilitating the free flow of beneficial data for patient care. It is indisputable, and will be further elaborated below, that an approach which requires providers to segregate all patient data at a granular level, to categorize each requester of PHI, to ascertain the motives of each requester and in some cases, require documentation as to their intentions, and then to disclose or retain patient data on a nearly case-by-case basis under the threat of penalties for guessing wrong, is a recipe that pours concrete on the flow of patient data that the last ten years of federal regulations have sought to foster. This is the future of health care, should the proposals be finalized as written because providers cannot comply and may be risk-averse enough to withhold all data.

**For these reasons, the AMA strongly recommends that OCR place responsibility for the use of patient data on the shoulders of those who intend to use it.** We believe that by requiring those enumerated types of requesters (law enforcement, etc.) to be responsible for proactively attesting that they will not use the PHI for a prohibited purpose, is essential to returning confidence to care providers that they will not be held in violation of federal law for the actions of others, if a disclosure they made in good faith ends up being used for a prohibited purpose. This is the first prong of a much needed two-prong approach.

The second prong of the approach, as outlined above, is to equip covered entities with the right to require an attestation at their discretion, as they will never be entirely sure what the requester intends or will do in the future.

By adopting both aspects of this approach, a covered entity will have the option to implement a workflow that, **in each instance of PHI disclosure, will require an attestation.** It will be required for each of the four special categories of requestors discussed above, and a covered entity may *choose* to require an attestation from all other requesters. There will be some start-up costs and workflow adjustments, yet this approach is **incomparably easier and less expensive while inestimably more likely to achieve the goals of protecting privacy and facilitating the beneficial sharing of patient information.**

*Technical Challenges and Limitations - Do regulated entities have the technical ability to differentiate between types of PHI in their electronic record systems and apply special protections to a new category of “highly sensitive PHI?”*

Expanding the access to health information is essential to support patient-centered clinical care. The AMA is a strong advocate for patient access to their medical records. Empowering patients and including them as a partner in care decisions has been shown to improve the patient-physician relationship and improve outcomes. Our ability to collect and track health and wellness data has benefited a growing population of users across the United States. Physicians and care teams can more closely monitor known conditions, identify early signs of diseases, and proactively engage with patients. Likewise, patients are better enabled to manage their own care and make informed decisions.

---

Any person requesting the use or disclosure of protected health information (PHI) for purposes specified in §164.512(d), (e), (f), or (g)(1) must provide to the covered entity, an attestation that the PHI will not be used for purposes specified in §164.502(a)(5)(iii)(1) or (2).

This alternative wording would require any person requesting PHI for purposes of health oversight activities, judicial and administrative proceedings, law enforcement, or for coroners or medical examiners, to proactively attest that the PHI will not be used for a criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating sensitive personal health care.

However, as more data are collected and exchanged, there is a lack of meaningful controls for patients to express their preferences and direct the access, exchange, or use of their personal health information. For years, the AMA has called on policymakers and health IT vendors to expeditiously work to create technology and policies that allow for “equitable interoperability”—that is, information exchange that empowers and does not disadvantage individuals. Further, ONC is proposing to expand the United States Core Data for Interoperability (USCDI) to include new data elements. These elements include social determinants of health information (SDOH). The USCDI will act as the basis for all health information exchange across the nation and is required in Centers for Medicare & Medicaid Services (CMS) programs. Additionally, ONC’s Information Blocking polices require that all patients’ electronic health information (EHI) must be made available for access, exchange, or use. It is also important to note that in ONC’s 21st Century Cures Act Final Rule,<sup>18</sup> the agency joined together the terms “health information network” and “health information exchange” as one of the three categories of “actors” that are regulated by the information blocking section of that regulation. As noted above, the proliferation of terms regarding the subjects of various privacy restrictions has been a source of confusion in the regulated community who could benefit from clear implementation guidance and outreach.

Together, federal USCDI and EHI requirements will vastly increase the volume and velocity of patient medical record exchange. Misuse of this information can jeopardize patient care and wellness. When accessed by state administrators and law enforcement, e.g., information related to reproductive health, EHI can be used against individuals—threatening their civil liberties. There is a strong need to protect patients’ sensitive personal health information—as both a foundation for health equity but also to mitigate the risk of negative impacts to individuals resulting from the disclosure of their information.

The ability for an individual to manage their data at a granular level, e.g., controlling elements of their record such as specific lab values or medications, can be a powerful mechanism to protect their medical information. Allowing some, but not all, of their information to be accessible or transmitted to another entity can give patients the confidence to continue to share personal information with their physician. In a 2022 survey of 1000 patients, 92 percent of patients believe that privacy is a right and nearly 75 percent of patients are concerned about protecting the privacy of their health data. Almost 80 percent of patients want to be able to “opt-out” of sharing some or all of their health data. Over one-half of surveyed patients stated that they are very or extremely concerned about negative repercussions related to insurance coverage, employment or opportunities for health care resulting from access to their health data.<sup>19</sup>

Yet, lacking adequate tools for granular segmentation of sensitive data, health care organizations resort to imprecise automated or manual processes to withhold sharing for broad patient populations. Physicians’ EHR systems lack the capabilities to support granular segmentation of sensitive data and the ability for physicians to accommodate patients’ expressed preferences to share their records. The AMA is strongly supportive of recent ONC proposals to require that EHR developers provide enhanced controls for sensitive data. However, as proposed, ONC’s EHR requirements would not go into effect until January 2026. Even then, it is unclear how effective these controls will be. There will continue to be a gap in certified EHRs’ abilities to protect patients’ sensitive data for years to come. Lacking these controls—and the trust that their data will be protected—patients with stigmatized or sensitive medical conditions may be less likely to consent to having their data recorded in the EHR and shared. OCR must consider the real-

---

<sup>18</sup> 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25642, 25794, third column (published May 1, 2020).

<sup>19</sup> *Patient perspectives around data privacy*, American Medical Association in partnership with Savvy Cooperative®, available at: <https://www.ama-assn.org/system/files/ama-patient-data-privacy-survey-results.pdf>.



The Honorable Xavier Becerra

June 14, 2023

Page 9

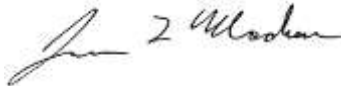
world limitations of EHR technology and craft policies that account for physicians' inability to withhold certain medical information from access, exchange, or use.

### **Conclusion**

Trust is the foundation of the patient-physician relationship; AMA strongly supports and encourages OCR's efforts to protect sensitive patient information, which is essential to this trust. PHI is best protected by allocating responsibility for its use, to those who intend to use it. Well-intentioned proposals that task covered entities with infeasible segmentation and retention unsupported by current technologies, seem doomed to freeze information sharing. We believe that the suggestions outlined above will empower covered entities to share essential data for patient treatment, build the trust of patients and providers in the area of patient privacy, and appropriately restrain the flow of personal details from those who would seek to use lawfully obtained health care to punish patients, providers, and supportive members of the community. Giving covered entities the right to require a discretionary attestation, together with a requirement that law enforcement and other requestors proactively provide an attestation as to their use of the PHI, is the most seamless approach to protecting sensitive personal health care information while facilitating the free flow of beneficial medical data. AMA believes implementing the above suggestions will free up the flow of much needed data to optimize patient care.

Thank you for the opportunity to provide comments on this proposal. Please contact Margaret Garikes, Vice President, Federal Affairs at [margaret.garikes@ama-assn.org](mailto:margaret.garikes@ama-assn.org) or 202-789-7409 with any questions or concerns.

Sincerely,

A handwritten signature in black ink, appearing to read "James L. Madara". The signature is fluid and cursive, with the first name "James" being the most prominent part.

James L. Madara, MD