



Association of  
American Medical Colleges  
655 K Street, N.W., Suite 100, Washington, D.C. 20001-2399  
T 202 828 0400  
www.aamc.org

Submitted via [www.regulations.gov](http://www.regulations.gov)

May 6, 2021

Robinsue Frohboese  
Acting Director and Principal Deputy  
Office for Civil Rights  
U.S. Department of Health and Human Services  
Attention: HHS-OCR-0945-AA00  
Hubert H. Humphrey Building  
200 Independence Avenue SW  
Washington, DC 20201

**RE: Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement [RIN 0945-AA00]**

Dear Acting Director Frohboese:

The Association of American Medical Colleges (AAMC) appreciates the opportunity to respond to the Office for Civil Rights (OCR) notice of proposed rulemaking entitled “Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement,” 86 *Fed. Reg* 6446 (January 21, 2021).

The AAMC is a not-for-profit association dedicated to transforming health through medical education, patient care, medical research, and community collaborations. Its members are all 155 accredited U.S. and 17 accredited Canadian medical schools; more than 400 teaching hospitals and health systems, including Department of Veterans Affairs medical centers; and more than 70 academic societies. Through these institutions and organizations, the AAMC leads and serves America’s medical schools and teaching hospitals and their more than 179,000 full-time faculty members, 92,000 medical students, 140,000 resident physicians, and 60,000 graduate students and postdoctoral researchers in the biomedical sciences.

AAMC member hospitals and health systems have been leaders in ensuring that patient information is protected and are committed to ensuring use of such information is consistent with federal and state privacy laws. Teaching hospitals and health systems are invested in the transformation to delivering value-based health care and recognize the role of health information exchange and patient engagement in that effort. The AAMC supports policies to improve patient engagement in their care and remove obstacles to efficient care coordination and case management while preserving the privacy of patients’ protected health information (PHI).

The AAMC believes removing barriers to the exchange of health information for coordinating care among providers, payers, and others involved in meeting patients’ health-related needs will have a positive impact on patient care and health outcomes. To that end, we strongly support giving patients greater access to and control over their own health records. However, we remain deeply concerned about the increasing role of non-HIPAA entities, such as personal health application (PHA) developers, in accessing and using sensitive information about patient’s health. Until such entities are subject to privacy and security standards commensurate with HIPAA rules, there is a real threat that the lack of appropriate patient privacy protections will erode any gains in patient engagement.

We believe many of the proposed changes, such as those clarifying and incrementally expanding permitted disclosures of PHI to facilitate individual care coordination and case management, will have a positive impact on patient care and health outcomes. We commend HHS for its efforts to reduce regulatory burden where there are no offsetting patient benefits or protections, such as the proposed elimination of the written acknowledgement of the Notice of Privacy Practices (NPP).

Finally, the AAMC asks HHS to better harmonize rules addressing access to health data and interoperability, including regulations under HIPAA, the ONC interoperability and information blocking regulations, and 42 CFR Part 2. While we understand that there are different statutory authorities for these rules, a common regulatory framework (including terms and definitions) will improve compliance and reduce operational burden on providers subject to these rules and reduce confusion for patients. Complying with the many new data exchange requirements is already a daunting task for most health organizations at a time when resources are stretched thin due to the ongoing COVID-19 public health emergency. While complete harmonization may not be possible due to legislative constraints, we urge HHS to provide detailed and integrated guidance to providers that accounts for the different HHS rules governing health information exchange that providers may be subject to.

The following represents a summary of our comments:

- ***Individual Right of Access Definitions for Electronic Health Records (EHRs) and Personal Health Care Applications (PHAs or Apps)***: Definitions should be consistent with the HITECH Act, limited to clinical records maintained by health care providers and, in regard to PHAs, created for individual use for health care purposes.
- ***Individual Right of Access and Privacy of Information in Apps***: Transmission of PHI should be limited to apps whose third-party vendor has been certified as meeting minimum privacy and security standards.
- ***Individual Right of Access and Right to Inspect***: Right should be balanced and allow providers to establish reasonable parameters for patients to capture their PHI in person.
- ***Individual Right of Access and Timelines for Response***: Timeliness requirements should appropriately reflect current guidance of “as soon as practicable,” but maintain existing 30-day maximum time frame for outlier requests and extensions.
- ***Individual Right of Access and the Prohibition of Unreasonable Measures***: Standard should be based upon OCR’s 2016 Access Guidance.
- ***Individual Access Right to Direct Copies to Third Parties***: The Requestor-Recipient role should permit providers discretion to fulfill the request and to require requests be made in writing, and that Disclosers be allowed to rely on the Requestor-Recipient’s verification of the identity of the individual making the request.
- ***Individual Right of Access Fees***: Permitted fees for third-party requests for physical copies for non-health care purposes should include labor and other related costs.
- ***Proposals to Support Care Coordination and Case Management***: Proposals to improve coordinated care for patients should be finalized. Regarding the proposal to expressly allow for disclosures to social services agencies and community-based organizations, HHS should provide greater specificity to better balance individual privacy with expanded care coordination.
- ***Disclosures to Support Patients with Substance Use Disorder, Experiencing Serious Mental Illness, and in Emergency Circumstances***: The adoption of the “good faith belief” and “serious and reasonably foreseeable” standards should be adopted to facilitate disclosures in the best

interests of patients and communities. HHS should also work to harmonize substance-used disorder disclosure standards under HIPAA and 42 CFR Part 2.

- ***Notice of Privacy Practices (NPP) Requirements:*** Proposal to eliminate the written acknowledgement requirement in recognition of the lack of patient benefit and the significant paperwork burden on covered entities should be finalized.

#### INDIVIDUAL RIGHT OF ACCESS (45 CFR 164.524)

##### ***The Definition of “Electronic Health Record (EHR)” Should Be Consistent with the HITECH Act and Limited to Clinical Records Maintained by Providers That Have a Direct Treatment Relationship with Patients***

HHS proposes to define EHR for the purposes of the Privacy Rule to include the clinical and billing records of a health care provider that has a direct relationship with patients. This definition goes beyond the clear language and intent of the HITECH Act, which states “[t]he term ‘electronic health record’ means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.”<sup>1</sup> Expanding the definition of EHR to include billing records would impose a significant burden on health care providers as such records generally do not reside in EHR systems and would require combining the records from disparate systems, often in different formats and using different software. This would be operationally challenging and is contrary to Congressional intent in the HITECH Act provision. For similar reasons, the AAMC does not support defining an EHR as an electronic designated record set (DRS), since it was precisely this unsupported broadening of the definition from the HITECH Act that the courts vacated in *Ciox Health, LLC v. Azar et al.*<sup>2</sup> Instead, **the AAMC supports a definition of EHR consistent with statute, that is clearly limited to structured clinical records of direct treatment providers.**

##### ***“Personal Health Application (PHA)” Should be Defined as an Application Created for Individual Use for Health Care Purposes***

HHS proposes to define PHA as “an electronic application used by an individual to access health information about that individual...controlled by or primarily for the individual, and not by or primarily for a covered entity or another party such as the application developer.”<sup>3</sup> This definition is intended to clarify that the PHA is an expansion of an individual’s access rights. The proposed definition is very expansive, and while HHS states that it is intended to be consistent with the HITECH Act, it goes well beyond the definition in that legislation. The AAMC does not agree that disclosure of PHI through a PHA is a clarification of an individual’s right of access, because a PHA necessarily involves disclosures to the third-party vendor operating the PHA.

HHS OCR has previously made clear through a series of FAQs<sup>4</sup> that transmission of PHI to a health application is a transmission to a third party. HHS states in its discussion of PHAs that these are simply a

---

<sup>1</sup> See 42 U.S.C 17921(5).

<sup>2</sup> See No. 18-cv-0040 APM (D.D.C. January 23, 2020).

<sup>3</sup> 86 *Fed. Reg.* 6446, 6457.

<sup>4</sup> See “[The Access right, health apps and APIs](#)” on OCR’s website, which includes [this FAQ](#), which states (emphasis added):

mechanism for individuals to access their own PHI. Nonetheless, in its request for comments, HHS effectively acknowledges that this is not the case when it asks whether covered entities (CEs) should be required to educate or warn individuals seeking to use PHAs that they are transmitting PHI to an entity that is not covered by the HIPAA Rules. In fact, the proposed definition of a PHA is so broad that vendors acting on behalf of non-health entities, such as attorneys and insurance companies, are already offering portals by which they may obtain medical records for non-health care purposes for free and without patient authorization by utilizing the PHA mechanism.<sup>5</sup> This is especially concerning in light of HHS' recent steps to greatly increase health data exchange through its information blocking and interoperability rules, which will facilitate the flow of vast amounts of health records from HIPAA entities to non-HIPAA entities that today face few, if any, impediments to commercially exploiting that data. **The AAMC recommends that the definition be limited to applications created for individual use specifically for health care purposes to avoid abuse of access rights by non-health care third parties.**

***Transmission of PHI Through a PHA Should Only Be Allowed Where the Third-Party Vendor Has Been Certified by an Independent Organization as Meeting Minimum Privacy and Security Standards***

As previously noted, HHS seeks comment on whether CEs should be required to educate or warn individuals seeking to use PHAs that they are transmitting PHI to an entity not covered by the HIPAA privacy rules. Such a requirement places the burden of privacy on individuals to ensure that their data remains protected and is likely insufficient to mitigate harm. It also puts CEs in a precarious position of gatekeeping information individuals may rely on for self-evaluations of third-party vendors while also not wanting such education or warnings to be viewed as discouraging the individual rising to a level deemed information blocking.

The onus should be placed on PHA vendors to be certified by an independent organization that they meet minimum privacy and security standards before they may offer PHAs to individuals. This is similar to the approach taken by the Centers for Medicare and Medicaid Services (CMS) with the Blue Button initiative. Requiring certification by independent industry-based organizations would address HHS concerns that it does not have jurisdiction over non-HIPAA entities, since the HHS requirement would apply to CEs to only allow the PHAs of certified PHA vendors to be used to access PHI. The actual certification process could be provided by independent industry-based organizations, such as HITRUST and the CARIN Alliance, among others that are on a list of certifying organizations approved by HHS. HHS could require that the certifying organization verify that the PHA operator at least meets certain

---

***What liability does a covered entity face if it fulfills an individual's request to send their ePHI using an unsecure method to an app?***

*Under the individual right of access, an individual may request a covered entity to direct their ePHI to a third-party app in an unsecure manner or through an unsecure channel. See 45 CFR 164.524(a)(1), (c)(2)(ii), (c)(3)(ii). For instance, an individual may request that their unencrypted ePHI be transmitted to an app as a matter of convenience. In such a circumstance, the covered entity would not be responsible for unauthorized access to the individual's ePHI while in transmission to the app. With respect to such apps, the covered entity may want to consider informing the individual of the potential risks involved the first time that the individual makes the request.*

<sup>5</sup> See CVN Blog "[Federal Plan to Overhaul Medical Records Rules Promises Big Changes for Law Firms](#)," Stating "[The] streamlined process means attorneys receive medical records more quickly and without the high fees charged by document centers....Attorneys sign up with ChartSquad for free and refer their clients to the company's easy-to-use online portal. Clients then request their medical records through the company's easy-to-use app and elect to share their records with whomever they choose, including their attorneys. ChartSquad does the rest, updating clients as records are delivered." December 23, 2020 (last accessed April 13, 2021).

minimum privacy and security standards, such as those specified in the suggested privacy attestation referred to by the HHS Office of the National Coordinator of Health Information Technology (ONC) in the preamble to its Cures Act rule.<sup>6</sup>

Furthermore, there is deep concern about the security application programming interfaces (APIs), which often serve as the transmission mechanism to move information from a CE to a PHA. A recent report found that PHAs are susceptible to hacking and leaks of PHI through the APIs themselves.<sup>7</sup> The Office of the National Coordinator for Health IT (ONC) has finalized rules to require the use of open, standardized APIs to encourage secure access to data, including HL7 Fast Healthcare Interoperability Resources (FHIR) API Capability as a criterion for EHR certification by the end of 2022, and additional capability by the end of 2023. The AAMC asks HHS to exercise caution during the period that these secure API capabilities are implemented and deployed to ensure that patient privacy is not at risk.

**In light of these concerns, the AAMC recommends HHS limit transmission of PHI through PHAs to those that do not permit third-party access to the information and that meet independent certification to minimum standards for privacy and security.** Requiring a certification to transmit PHI through the PHA would provide patients with meaningful privacy protections which is preferable to merely ensuring that PHI flows only to entities that are known to have in place minimum privacy and security protections. Additionally, HHS should consider include in regulation its current guidance about when a CE does and does not remain liable for a PHA's use or disclosure of the PHI it receives.<sup>8</sup>

***Allowing Patients to Capture Their PHI in Person Must Be Paired with Allowing Covered Entities to Establish Reasonable Parameters That Balance Several Competing Needs***

HHS proposes a new access right that would allow an individual to take notes, videos, and photographs, and use other personal resources to view and capture PHI. HHS states that it does not believe that such a right would be inconsistent with federal and state recording laws or intellectual property rights protections.

The AAMC supports efforts to make health records accessible to patients, especially in light of the current COVID-19 public health emergency, where patients are often not allowed to bring a family member to appointments and might find it challenging to capture the information communicated during the visit. **We support the proposal in concept, but urge HHS to allow providers sufficient flexibility in implementation to ensure that the right is exercised in a way that is within resource capacity and not detrimental to delivering care, does not disrupt clinical workflow, and does not impinge on the rights of others.** Video recording in a hallway, waiting room, or other public spaces does not ensure the privacy of other patients. Thus, CEs must be able to reasonably restrict in these areas or situations. In addition, some patients may seek to record or video entire appointments or procedures, including the voices and images of physicians and staff. This would infringe on the privacy of the health care staff who would have no control over their own information captured by patients in a non-public setting. Finally, in some states this would violate state recording laws unless the physician and staff consented to the recording, and it would not be clear which law would prevail in that situation. **We recommend that HHS**

---

<sup>6</sup> 85 *Fed. Reg.* 25642 (May 1, 2020)

<sup>7</sup> See FierceHealthcare article "[Mobile health apps leak sensitive data through APIs, report finds](#)," describing recent report by Alissa Knight entitled "[All That We Let In](#)," February 24, 2021 (last accessed March 9, 2021).

<sup>8</sup> See OCR Guidance, "[The access right, health apps, & APIs](#)," January 6, 2021 (last accessed May 4, 2021).

**state clearly in the regulation that CEs are permitted to impose reasonable limits on the exercise of this right.**

***Support Revision of Timeliness Requirements to “As Soon as Practicable,” But Maintain Existing 30-Day Maximum Time Frame for Responding to Individual Request for Access and Extensions***

The Privacy Rule establishes a timeliness requirement for responding to an individual’s right to access to obtain a copy of his or her PHI such that a CE must provide access no later than 30 days following receipt of a request. The current timeliness requirement allows for one 30-day extension provided that the CE provides a written statement of the reasons for such delay and the date by which it will complete any action on the request. HHS proposes to amend the timeliness requirement to mandate that CEs provide copies of PHI as soon as practicable, but not later than 15 days, with the possibility of a one-time 15-day extension so long as the CE has established policies to address urgent or high-priority requests (which OCR does not define). This 15-day timeframe would apply to both individual requests and requests by an individual to direct copies of PHI to third parties.

**We support requiring providers to respond to access requests as soon as practicable.** AAMC members make every effort to respond promptly to requests, in compliance with HIPAA, state and other legal requirements. HHS OCR has been clear that the 30-day period to respond to a request is the “outer time limit for providing access” and that it expects CEs “should be able to respond to requests for access well before the 30 day outer limit.”<sup>9</sup> While many requests may be responded to within 15 days, some requests require a laborious and time-consuming process to fulfill. For example, our members maintain some records from legacy systems which primarily reside in offsite archives. Similarly, it is neither simple nor straightforward to produce some types of electronically maintained records in a form that is readable. Imaging data is particularly problematic in this regard and can require significant effort to create a useful version. Furthermore, assessing differing timeliness standards based on an assessment of urgency of the request would be complicated and burdensome to administer without clear definition from HHS. Such a policy would intrude on the privacy of patients, and place providers in the untenable position of having to make subjective judgments to rank individual requests and the veracity of requesters.

HHS proposes additional requirements that, if finalized, will add to the complexity of individual requests and could potentially necessitate more than 15 days for response. Shortening the time limit in addition to expanding the right of access will require additional staffing and retraining. Therefore, the AAMC does not support reducing the outer time frame or extension time frame to 15 days. Additionally, the ability to extend the time frame for a response should not be conditioned on a policy to address high priority or urgent requests, as this could have unintended negative consequences. **We recommend that HHS amend the regulation to the “as soon as practicable” standard, but also retain the existing provision allowing covered entities a one-time extension of up to 30 days provided that the individual is notified before the end of the initial time frame of the reason for the extension and the date the information will be provided.**

---

<sup>9</sup> HHS Office for Civil Rights, [Guidance: Individuals’ Right under HIPAA to Access their Health Information](#) (last accessed March 3, 2021).



***Prohibition on Covered Entities Imposing Unreasonable Measures Should Use OCR's 2016 Access Guidance***

HHS proposes to prohibit CEs from imposing unreasonable measures that impede individuals from access when a measure that is less burdensome for the individual is practicable for the entity. **The AAMC supports prohibiting the imposition of unreasonable measures that serve as barriers to, or unreasonably delay a patient from, obtaining access to their health records.** However, in order to allow CEs to establish uniform protocols that can apply to all requests, **we recommend that the regulation follow the wording of the 2016 Access Guidance,<sup>10</sup> which we believe more appropriately balances the burdens of individuals and CEs and allows CEs to establish and implement uniform policies across the organization.** Specifically, the 2016 Guidance prohibits unreasonable measures that “serve as barriers to or unreasonably delay” an individual from obtaining access and encourages CEs to offer multiple options for requesting access. Adopting the language of the 2016 Guidance in regulation would facilitate uniform policies and workforce training across the CE and help ensure that individual requests are handled quickly and efficiently.

***Health Care Providers Should be Permitted to Require That Individual Requests to Direct Copies of PHI to Third Parties Be in Writing***

HHS proposes to require covered health care providers to respond to oral requests by patients to direct an electronic copy of PHI in an EHR to a third party designated by the patient when the request is “clear, conspicuous and specific” as required by the HITECH Act. The AAMC supports efforts to facilitate patients’ access to their information, but not in a manner that could increase privacy risks and create misunderstandings with providers. In some circumstances, responding to oral requests could improve processing times, such as when a patient makes a request at the point-of-care following an in-person visit, and with staff trained to document such a request. Errors, misunderstandings and misdirected data are much more likely to occur when relying on an oral request. Additionally, the AAMC is concerned that the requirement that requests be “conspicuous,” is at odds with application to the spoken word. **Considering these challenges, we recommend that HHS allow health care providers to accept oral requests at their discretion and them to require that individual requests to direct PHI to a third party be in writing.**

***Requestor-Recipients Should Be Allowed to Exercise Reasonable Judgment When Determining Whether to Act on an Individual's Direction to Request PHI from a Provider Holding PHI in an EHR***

HHS proposes to require that an individual may direct, orally or in writing, that his or her covered health care provider or health plan, as a “Request-Recipient,” obtain an electronic copy of PHI in an EHR from one or more covered health care providers, as a “Discloser.”

The AAMC supports efforts to improve the sharing of PHI between health plans and providers to facilitate care coordination and case management. However, **we are concerned that mandating, rather than permitting, this type of data exchange could have unintended negative consequences to patients as well as CEs.** This is particularly the case if the PHI is required to be disclosed based solely on an oral request, and without any input from the Receiver-Recipient as to whether it needs all of the requested records, already has some or all of the requested records or has determined what it would do with the records.

---

<sup>10</sup> HHS Office for Civil Rights, [2016 Guidance on Access Rights](#) (last accessed April 20, 2021).

While the disclosure would be to another CE, this does not eliminate the risks to privacy, security, and potentially even health care delivery, from the unplanned receipt of significant amounts of health data. CEs may not have the resources to store the data or resolve inconsistencies with, or duplication of, data they already hold, with the result that the data could be housed in temporary storage making it more vulnerable to breaches. The minimum necessary and data minimization principles, now uniformly embraced in privacy legislation and as best practices, seek to reduce these very real privacy risks and would be blunted by this proposal. **We urge HHS to modify the Requestor-Recipient request requirement to allow Requestor-Recipients to exercise reasonable judgment in deciding whether to act on such an individual request.** This decision would be based on the nature of the data requested, the data the Requestor-Recipient already holds, its ability to integrate and use the data, and other relevant factors.

***Disclosers Responding to Requestor-Recipient Access Requests Should be Allowed to Rely on the Requestor-Recipient's Verification of the Identity of Individual***

If HHS finalizes its proposal to create the Requestor-Recipient and Discloser roles under the individual right of access, **the AAMC recommend HHS expressly allow Disclosers to rely on the Requestor-Recipient's verification of the identity of the individual directing the request.** This will assist in more timely responses to the Requestor-Recipient by avoiding delays to confirm the request with the individual and otherwise frustrate the seamless information exchange intended by this new individual right of access.

***Permitted Fees for Third Party Requests for Physical Copies of PHI for Non-Health Care Purposes Should Include Labor and Other Related Costs***

Currently, the HIPAA Privacy Rule allows covered entities to charge a reasonable, cost-based fee to fulfill access requests from individuals for copies of their PHI, referred to as "the patient rate." Allowable fees are limited to the costs of (i) labor for copying (whether the PHI is in paper or electronic form), (ii) supplies for creating the paper copy or electronic media, (iii) postage, and (iv) preparing any agreed-upon summary or explanation of the requested PHI. For patient requests for their PHI, the allowable fees do not include time associated with retrieving records, which in many cases, may be spread across multiple record systems and may include physical records in different locations. Recognizing the importance of patient's access to their PHI, health care providers have absorbed these extra costs associated with record retrieval.

In the rule, HHS proposes to eliminate the distinction under HIPAA that has been in place between costs that may be reimbursed for individual access to PHI (the patient rate) and costs for third party access. HHS proposes that covered entities be required to provide PHI without cost to any third parties (such as insurance companies or law firms) accessing PHI through a patient's PHA and would limit charges to third parties seeking PHI held in an EHR to only the labor costs for copying the PHI (similar to the patient rate). HHS assumes that internet-based access would not involve an entity's workforce members and therefore labor costs for these requests would be unlikely.

While the AAMC supports limiting the fees charged to individuals for access to their PHI to the reasonable cost-based fee currently in effect, we oppose applying the same individual patient fee limitation to third parties seeking health care records for non-health care purposes. If this proposal is finalized, health care providers would incur significant labor costs for record retrieval and compilation to respond to requests from third parties. Most academic medical centers have multiple hospitals and



physician offices that may have different systems with data that are not fully integrated. To respond to a request for PHI, it is common for academic medical centers to access multiple systems, even when all the records are held in an EHR. In some cases, records are stored in physical locations outside of the EHR. Responding to the high volume of requests for PHI is resource-intensive, complex, and requires knowledge of state and federal laws. Therefore, many AMCs enter into arrangements with outside vendors that have the expertise to handle these requests on behalf of the AMC.

Requiring hospitals, physicians, and other providers to subsidize the record retrieval activities associated with third party requests for non-health care purposes would divert resources away from other important activities that are beneficial to patients. Making this change now would be especially problematic as hospitals, physicians, and other health care providers need to devote their resources toward addressing the COVID-19 public health emergency.

**Therefore, the AAMC recommends that CEs be allowed to charge third parties that are requesting the PHI for non-health care purposes a reasonable fee that accounts for the labor, including retrieval and compilation and other costs, involved in responding to these requests.**

#### **AMENDING THE DEFINITION OF HEALTH CARE OPERATIONS TO CLARIFY THE SCOPE OF CARE COORDINATION AND CASE MANAGERMENTS (45 CFR 160.103)**

HHS proposes to clarify that the definition of “health care operations” includes the disclosure of PHI for purposes of individual-level care coordination and case management. Historically, “health care operations” has been considered to only include population-based care coordination and management, thereby limiting information sharing that is essential to providing access to quality health care to individuals. **The AAMC supports the clarification that health care operations includes individual-level care coordination and management as this will improve coordinated care for patients.**

#### **CREATING AN EXCEPTION TO THE MINIMUM NECESSARY STANDARD FOR DISCLOSURES FOR INDIVIDUAL-LEVEL CARE COORDINATION AND CASE MANAGERMENTS (45 CFR 164.502(b))**

HHS proposes to create an exception to the “minimum necessary” standard regarding the amount of PHI shared for individual-level care coordination and case management uses and disclosures. The minimum necessary standard is a critical protection of PHI but in some circumstances, it may act as an obstacle to information sharing between health care providers. **We support the proposal to except from the “minimum necessary standard” disclosures for individual-level care coordinating and case management activities to better allow providers to coordinate care and improve outcomes.**

#### **CLARIFYING THE SCOPE OF DISCLOSURE OF PHI TO CERTAIN THIRD PARTIES FOR INDIVIDUAL-LEVEL CARE COORDINATION AND CASE MANAGEMENT (45 CFR 164.506)**

HHS seeks to clarify when PHI may be shared with social services agencies, community-based organizations and home and community-based (HCBS) providers. These organizations provide important and beneficial services to individuals. Covered entities and business associates should not fear that they may inadvertently violate HIPAA when sharing PHI with such organizations for individual-level care

coordination and case management. However, the AAMC is concerned that the proposal to expressly permit the sharing of PHI with such organizations is too broad, particularly the references to “similar third party” and “health or human services.” This language could encompass a broad range of entities well beyond those whose primary functions involve performing the types of social service activities contemplated by HHS and described in the preamble. Disclosures to such entities, who are unlikely to be covered by HIPAA, could erode patient confidence and trust in providers. Therefore, **we recommend that HHS provide greater specificity and restrict disclosure to those qualifying organizations whose primary purpose is the provision of specified social services.** This will ensure this express permission does not become a loophole that puts vulnerable patients’ sensitive health information at risk.

**ENCOURAGING DISCLOSURES OF PHI WHEN NEEDED TO HELP INDIVIDUALS EXPERIENCING SUBSTANCE USE DISORDER, SERIOUS MENTAL ILLNESS, AND IN EMERGENCY CIRCUMSTANCES (45 CFR 164.502 AND 164.510-514)**

***Adopting the “Good Faith Belief” Standard Will Facilitate Necessary Disclosures in the Best of Interests of Patients in Emergencies***

The HIPAA Privacy Rule currently allows CEs to disclose PHI of patients experiencing serious mental illness (SMI), substance use disorder (SUD), and in emergency circumstances without individual authorization under the “exercise of professional judgment” standard. HHS proposes to amend this standard for five specific areas<sup>11</sup> and replace it with a standard permitting certain disclosures based on a “good faith belief” about a patient’s best interests.

**The AAMC supports this new standard and believes it will facilitate sharing of PHI with family and caregivers in crisis and emergency situations by permitting health care providers to disclose PHI in the best interests of their patients.** AAMC members place patient outcomes at the center of their mission, and the proposed change to the HIPAA Privacy Rule will advance this central goal. For example, if an individual suffering from SMI were to experience a moment of heightened mental health episode, it would be critical for providers to be able to share PHI with members of their close social support network in a timely manner.

***Assessing Threats Under a “Serious and Reasonably Foreseeable” Standard is More Appropriate to Facilitate Disclosures to Avert Potential Harm***

HHS also proposes to replace the “serious and imminent threat” standard with a “serious and reasonably foreseeable threat” standard to help prevent situations in which providers decline to appropriately use and disclose PHI due to concerns about their ability to determine whether a threat of harm is indeed imminent. AAMC member teaching hospitals and health systems and teaching physicians take seriously their duty to advance the best interests of their patients and to ensure optimal patient outcomes while protecting the privacy of their health information. The current “serious and imminent” standard may prove to be impracticable in some cases related to SUD, SMI, and other emergency circumstances. In particular, the “imminent” element of disclosure can be difficult to determine, even if a fact-specific analysis is conducted. Considering the time-sensitive nature of medical emergencies, particularly those for patients

---

<sup>11</sup> The five areas are: (1) Parent of guardian who is not the individual’s personal representative (45 CFR 164.502(g)(3)(ii)(C)), (2) Facility Directories (45 CFR 164 (510)(a)(3)(i)(B)), (3) Emergency contacts (45 CFR 164.510(b)(2)(iii)), (4) Emergencies and incapacity (45 CFR 164.510(b)(3)), and (5) Verifying requestor’s identity (45 CFR 164.514(h)(2)). 86 *Fed. Reg.* 6446, 6481-6482.

experiencing SUD or SMI, the time spent making an “imminent determination” may be a barrier to making permissive disclosures that would improve the safety of the public and the individual patient. The “serious and reasonably foreseeable” standard would empower providers making critical determinations about whether to disclose information and better protect the best interests of the patient and of the community in critical care situations.

**The AAMC supports these changes to benefit the delivery and coordination of care and treatment for individuals across patient populations.** We reiterate our request that HHS assure HIPAA will control health privacy protections, and the other rules should defer to and conform with its privacy obligations. In particular, the “preventing harm exception” in the information blocking rule is destined to create even greater confusion than currently exists for providers who must make decisions on a day-to-day basis to protect the interests and safety of patients and the safety of others. **There should be no doubt that the HIPAA standards prevail and that, when acting consistent with the HIPAA rules, providers are excepted from the information blocking requirements.**

***HHS OCR Should Implement Regulations Harmonizing SUD Disclosure Standards Under HIPAA and 42 CFR Part 2***

Greater harmonization is needed with HIPAA and the regulations implementing 42 CFR Part 2 in order to achieve the goals to encourage critically needed PHI disclosures under HIPAA rules to support patients with SUDs. Part 2 providers may find themselves unable to use their discretion with the proposed changes to disclosure standards, as Part 2 generally requires patient consent to disclose except in cases of *bona fide* medical emergencies. Even CEs that are not Part 2 providers may find it challenging to take advantage of the proposed SUD disclosure changes because they may encounter data segmentation challenges with patient records including data from Part 2 providers. The 2020 Coronavirus Aid, Relief, and Economic Security (CARES) Act requires HHS to issue new Part 2 regulations, and HHS should use this opportunity to bring additional clarity to the relationship between 42 CFR Part 2 and the HIPAA Privacy Rule. **We encourage HHS to focus on harmonization with HIPAA and information blocking rules when crafting new Part 2 regulations.**

**NOTICE OF PRIVACY PRACTICES REQUIREMENTS (45 CFR 164.520)**

HHS proposes to eliminate requirements for covered health care providers with a direct treatment relationship to an individual to obtain a written acknowledgement of receipt of the provider’s notice of privacy practices (NPP). The AAMC agrees with HHS OCR that the current requirement has not contributed to a greater understanding of privacy practices, and in some cases has even created confusion and misunderstanding. **We commend HHS for its proposal to eliminate the written acknowledgement requirement, which recognizes the lack of patient benefit and the significant paperwork burden on covered entities of the NPP acknowledgement requirement.**

HHS also proposes changes to the required content of the NPP, requiring significant resources to develop and update the NPP in all of the physical and electronic locations it resides. For example, HHS proposes a requirement to provide particular examples of how an individual’s PHI could be used or disclosed in health care operations, which would result in a more complex document and is inconsistent with the directive that the NPP be shortened. **The AAMC asks HHS OCR to create a standard federal notice**

**based on the model NPP created in collaboration with the ONC<sup>12</sup> that would provide assurance to providers that their NPP complies with HIPAA and ensure adequate time for providers to implement these changes to the NPP and come into compliance.**

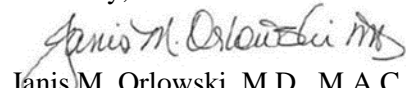
#### ACCOUNTING FOR DISCLOSURES

**The AAMC appreciates that this NPRM does not include a proposal to establish an individual right to an access report.** We strongly supported the withdrawal of the Accounting for Disclosure NPRM. As we wrote in our 2011 comment letter, our members receive very few requests for such an accounting, and the proposed access report requirement would create undue burden without providing meaningful information to individuals. In most cases, when a request is made it is because of a fear that someone has “snooped” into the record, something that can be handled through an investigation. Most AAMC members routinely monitor medical records for inappropriate access and have in place policies and procedures for dealing with inappropriate access. Furthermore, any access in violation of the Privacy Rule is subject to the breach notification provisions thereby ensuring that patients are informed of the accesses most of interest to them, without the need for a request of an accounting. There also are substantial concerns about the ensuring the safety and privacy of staff when their names are released to a patient.

#### CONCLUSION

Thank you for this opportunity to provide comments on the proposed changes to the HIPAA Privacy Rule. We remain committed to work with HHS on any of the issues discussed above or related topics that impact the teaching hospital and academic health center community. If you have questions regarding our comments, please feel free to contact me or Phoebe Ramsey, [pramsey@aamc.org](mailto:pramsey@aamc.org).

Sincerely,



Janis M. Orlowski, M.D., M.A.C.P.  
Chief Health Care Officer

cc: Phoebe Ramsey, J.D., AAMC  
Gayle Lee, J.D., AAMC

---

<sup>12</sup> See HHS OCR [Model Notices of Privacy Practices](#) (last accessed April 18, 2021).