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

March 10, 2021

Robinsue Frohboese
Acting Director and Principal Deputy, Office for Civil Rights
U.S. Department of Health and Human Services
Attention: RIN 0945-AA00
Humbert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

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

Dear Acting Director Frohboese:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our clinician partners – including more than 270,000 affiliated physicians, 2 million nurses and other caregivers – and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) appreciates the opportunity to comment on the Department of Health and Human Services (HHS) Office for Civil Rights' notice of proposed rulemaking (NPRM) on "Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement."

America's hospitals and health systems are dedicated to safeguarding the privacy of patients' medical information. We support efforts to decrease regulatory burdens for covered entities and remove unnecessary barriers to efficient care coordination and/or case management that simultaneously also respect and preserve the privacy and security of patients' health information under HIPAA (the Health Information Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009).

As a preface to our specific comments on the NPRM proposals, we urge HHS to take a holistic approach in its deliberations related to the NPRM. The HIPAA regulations do not operate in a vacuum. It is imperative that HHS acknowledge in the final regulations the intersection of the regulations under HIPAA, the Office of the National Coordinator for Health Information Technology (ONC) Cures Act

interoperability and information blocking requirements, and the Part 2 regulations under Title 42 of the Code of Federal Regulations (CFR): Confidentiality of Substance Use Disorder Patient Records (Part 2).

The overlapping and sometimes inconsistent requirements of these three regulatory regimes create conflicts for health care providers, and we urge HHS to take further steps to ensure that the Part 2 and Cures Act regulations are fully aligned with HIPAA. The current framework results in a patchwork of health information privacy requirements set forth in three different sets of federal rules, enforced by three different agencies as well as numerous conflicting state privacy laws. This current approach continues to pose a significant barrier to the robust sharing of patient information necessary for clinical treatment and coordinated care, which are critical to providers' efforts to improve the quality of care and advance the health of the patients and communities they serve. In addition, these overlapping requirements pose significant challenges for providers' use of certified electronic health record (EHR) systems, which is a critical part of the infrastructure necessary for effectively coordinating care.

HIPAA, as the most comprehensive of the three federal regulatory regimes, should take preeminence for health privacy protections, and the other rules should defer to and conform with its privacy obligations. In particular, the information blocking rules should align with the obligations created under HIPAA and should not create overlapping requirements. Similarly, full alignment of the Part 2 regulations with HIPAA will eliminate existing barriers to the sharing of patient information that is essential for care coordination, as well as compatible with the effective electronic exchange of information. Patient access is important to both providers and patients, but it is critical to accomplish this in a manner that protects and enhances patient privacy while avoiding overlapping regulatory requirements that divert providers' focus from the patient and community to reconciling differences among siloed federal agencies.

As an intermediate step to harmonizing the three sets of regulatory requirements, the AHA urges HHS not to implement any new HIPAA requirements related to additional rights of access that would be enforced prior to the availability of technologies essential for responding to patient requests. For example, as of now, the Cures Act requirements for developers of certified health information technology (IT) to provide technology upgrades, including enhanced application programming interface (API) capabilities, essential to fulfilling requirements related to the proposed new rights of access will not be enforced until at least Dec. 31, 2022. Accordingly, until new capabilities are fully implemented in certified health IT, the additional rights of access proposed for HIPAA should not be enforced. Indeed, in order to give health care providers sufficient time to implement new procedures for responding to right of access requests, enforcement should take effect no sooner than 180 days after the first enforcement of the Cures Act Conditions of Certification certified health IT, including the requirements for enhanced API capabilities.

More generally, the AHA supports many of the NPRM's proposals designed to enhance patient care and decrease regulatory burdens for HIPAA covered entities. We appreciate OCR's efforts to address barriers to efficient care coordination and case management while continuing to respect and preserve the privacy and security of patient information. Better coordination of care is a goal shared by hospitals – but clarity is essential to ensure the greatest practical impact. Particularly for behavioral health, serious mental illness, and substance use disorders, greater care coordination could save lives if implemented successfully. Detailed comments on OCR's proposals in all of these areas are attached.

We appreciate OCR's consideration of these issues, and we look forward to working with OCR to provide meaningful patient access to health information and better facilitate critical care coordination needs, while supporting patient privacy. If you have any questions concerning our comments, please feel free to contact me at mhatton@aha.org, or Maureen Mudron, deputy general counsel, at mmudron@aha.org.

Sincerely,

/s/

Melinda Reid Hatton
General Counsel

Cc: Micky Tripathi, National Coordinator for Health Information Technology;
Cc: Tom Coderre, Acting Assistant Secretary for Mental Health and Substance Use

DETAILED COMMENTS

PATIENT RIGHT OF ACCESS

The AHA strongly supports patients' right to access their health information. Easy access to their health information empowers patients to play an active role in their own care. The AHA is concerned, however, that some of the proposed changes related to patient access rights will excessively burden hospitals and other health care providers without meaningfully advancing patient access to health information. Other rulemakings, such as those focused on interoperability under the Cures Act, are rapidly pushing for health information technology (IT) platforms to incorporate new technologies and capabilities. Because of the rapid pace of change in this area, the AHA is concerned about the challenges for hospitals seeking to achieve compliance when the technology for information sharing is not fully developed. We have addressed specific access proposals below.

Forms and Formats Deemed Reproducible

The AHA recognizes the importance of providing protected health information (PHI) in a form and format that patients and their providers can understand and use. The AHA is concerned, however, that the proposed changes to deem forms and formats required by other regulatory regimes as readily producible under HIPAA – and imposing HIPAA penalties for failure to meet any other such standards – puts OCR in the position of enforcing those other laws, in addition to any enforcement appropriately handled by such other governmental authority.

Linking a covered entity's ability to comply with other federal and state standards to the potential for HIPAA penalties is beyond the scope of HIPAA and also may necessitate other regulatory regimes taking into account how HIPAA-related enforcement may impact changes to those regimes. **Maintaining separate enforcement for overlapping regulatory regimes will ensure that HHS continues to have appropriate enforcement flexibility without causing conflicts between enforcement regimes or requiring that HIPAA enforcement be modified whenever other regulations are altered.** Finally, such a linkage also undermines the intended effects of enforcement discretion announced for other regulations – such as the interoperability and information blocking rules – which are subject to enforcement discretion in order to give health care providers more time to implement requirements in the face of a global pandemic.

In addition, OCR suggests that entities that have an application programming interface (API) also may be deemed to be able to produce information in the form and format consistent with that API. We caution that technology that is not yet fully mature should not be incorporated wholesale into HIPAA's requirements. API technologies that are not fully mature may take significant effort to implement successfully, potentially creating

risks to patient care, while diverting hospital resources away from other initiatives to better serve patients.

If an API-related requirement is created, no enforcement should occur until Cures Act requirements for APIs are fully implemented and enforced, to ensure consistency between HIPAA's requirements for APIs and the availability of suitable API technology to help support compliance with such requirements. Any HIPAA enforcement before then would place hospitals in the impossible position of being required to implement something that the available health IT does not support.

Photographs and Videos

The AHA asks that OCR reconsider its proposal to permit individuals to take videos and photographs of PHI as part of the right of access. Hospitals have long worked to address the challenges that handheld technology in patient care areas may pose to patient privacy. While there may be situations where allowing a patient to take a photograph or video is appropriate, we are concerned that including this as part of an individual right will put health care providers in a difficult position. A hospital may choose to allow a patient to use her mobile phone, for example, to take a photo of a report about the patient. But there are many times where use of cameras in a hospital setting may place other individuals' privacy at risk by potentially capturing sensitive information about other patients, family members or workforce members. **Covered entities should be permitted to allow this type of access but also should be able to exercise judgment in this particularly challenging format and, where appropriate, provide PHI in other formats, instead.**

Timeliness for Responding to Access Requests

The AHA urges keeping the privacy rule's existing timeliness requirements for responding to access requests as-is. The proposed changes to shorten timeframes for responding to access requests fail to take into account the range of requests that are received and what practically is required for a response. While health IT may appear to facilitate the rapid provision of PHI, physically stored PHI will not be as immediately available, and even electronic PHI (ePHI) may not be immediately accessible depending on its form and format. Because hospitals may not always be able to meet the proposed new accelerated timelines for all information maintained in a designated record set, the gathering of information for certain types of access requests will continue to be a manual process.

Covered entities' current practice is to respond promptly to requests, and typically providers are able to do so well within the current timeline for access requests. In addition, state and other federal requirements, including requirements related to EHR certification, already have eclipsed the specific HIPAA requirements, eliminating the need to revise the HIPAA rules to establish different timeliness standards. The different timeliness standards currently applicable through state and other federal laws are themselves complicated and burdensome to administer. Further accelerating HIPAA's

timelines while technologies and other requirements grow ever more complex would force covered entities to invest disproportionate amounts of resources to provide marginal improvement to a small fraction of requests.

Additionally, the prioritization of requests would not provide an easy fix for these issues. Requiring covered entities to adopt policies for identifying and prioritizing urgent or other high-priority access requests is not as simple as implied. This would require multiple work streams, as well as an additional process for covered entities to evaluate whether a request is truly urgent or high priority, or is merely marked as such incorrectly. In short, requiring covered entities to attempt to prioritize between requests would only increase the burdens of the requirements, potentially slowing down the process rather than improving it.

Should OCR decide to adopt this proposal, the AHA urges OCR to coordinate the implementation of any shortened timeframe with the implementation of interoperability requirements. To the extent that a shorter timeframe is imposed, it will be important that hospitals are able to take advantage of additional technology that facilitates faster response times. Where technology is not yet mature enough to adequately enable covered entities to respond quickly or not available for all types of information, HIPAA should provide flexibility to accommodate the actual state of play within the health care ecosystem.

Disclosures to Third Parties

The AHA is concerned that the proposed changes to expand the right of a patient's access to include requiring disclosures to third parties would result in hospitals being required to provide large amounts of information that may not be easily made available, particularly if the timeframe for responses is shortened. It would create an entirely new set of requirements for access, and hospitals will be burdened to respond to such requests when the technical support needed is not fully mature. Hospitals are focused on providing care, not on serving as a primary method to exchange health information with third parties, including third parties who do not provide health care but wish to receive health information for other purposes. If adopted, this provision should clarify that health care providers bear no responsibility for the use of PHI disclosed to third parties at an individual's request.

Requests on behalf of patients. Hospitals also would be required to submit requests on behalf of patients to other providers, rather than having patients directly submit such requests on their own, potentially leading to unnecessary confusion and delays in request submissions. This requirement would insert hospitals into patient relationships with other providers. Currently, health information exchanges and health information networks already facilitate provider-to-provider exchanges, and Cures Act provides additional opportunities for exchanges that will be less burdensome and more administrable. Rather than creating another layer of requirements that diverts hospital resources unnecessarily and makes the system for health information exchange even

more complex, **OCR should permit ONC to continue leading in this area and allow Cures Act to play its intended role of building technical capabilities and removing barriers to information sharing for patients and health care providers.**

Oral requests. The proposal creates further challenges for hospitals by requiring that they respond to requests that may not be clear. Although requests are required to be "clear, conspicuous, and specific," it appears OCR intends that requests may be oral or submitted through a personal health application, creating a greater likelihood for misunderstandings. **The proposed requirement would be welcome if included as an option for flexibility for hospitals, but as a requirement it is unworkable in real-world applications.** Requiring responses to requests in many formats could require hospitals to deal with unclear requests coming in through a vast array of sources, undermining the developed requests processes and leading to errors or misunderstandings on the part of hospitals or patients. The ability for hospitals to appropriately limit the methods through which requests can be received will prevent unnecessary complexity and risk, and ultimately lead to more timely responses to all requests.

Permitted fees. The AHA supports limitations on fees charged to patients accessing their PHI and agrees that fees should not be charged to patients for accessing their information through a patient portal or other internet-based method. The AHA is concerned, however, that OCR's proposal would prohibit health care providers from charging reasonable fees for internet-based access by business and commercial third parties. OCR's rationale for the prohibition on fees (that the information is electronically available) fails to account for the frequency with which the required information resides on multiple systems and compiling the information must be done manually. **OCR's fee structure should recognize, as ONC's does, a difference when manual efforts are required.**

Disclosures to Personal Health Applications

Disclosures to personal health applications should be viewed as disclosures to third parties (namely, the companies running those applications) rather than to individuals. These disclosures force hospitals to facilitate data exchanges between individuals and third parties who are not covered entities and with which the hospitals have no relationship. Proposing to facilitate widespread disclosures to non-covered entities may place patient privacy and safety at risk, because application developers are not subject to HIPAA and may not have the same level of protections.

If this proposal is adopted, the AHA renews its call for OCR to work with other entities to provide model language that could be provided to patients to inform them of the risks involved and emphasize that the covered entity can no longer protect their data once it is disclosed in this manner. Although providers should not be required to step into the role of educating patients about their privacy and security choices related to third-party applications, some hospitals may wish to do so in order to help their patients. Without readily available patient education resources, covered

entities will lack guidance on how to help patients make informed decisions about who receives copies of PHI. Moreover, model resources will help to educate patients about potential risks from applications that may expose patient information through poor privacy protections or inadequate security. Patients also may be unaware if an application is capable of correctly displaying information received from an EHR as compared to information obtained from a consumer fitness device or patient-input values. Improper display of health care information transposed from an EHR could confuse or misinform patients and lead to health decisions based on incorrect or inaccurate information displays.

In order to protect patients and prevent unreasonable demands on providers, it is essential that the definition of "personal health application" be limited, especially if the proposed change is adopted. **Personal health applications should be limited to applications that do not permit third-party access to the information, include appropriate privacy protections and adequate security, and are developed to correctly present health information that is received from EHRs.**

Definition of Electronic Health Record
EHRs are critical tools used by health care providers to improve the quality, safety and efficiency of patient care. OCR proposes to formalize a definition of EHR based, in part, on the HITECH Act definition. While the proposed definition aligns with the HITECH Act in that it references records of a health care provider that has a direct treatment relationship with patients, it significantly broadens the HITECH Act definition beyond clinical information to include non-clinical records, such as billing records.

The AHA does not support the inclusion of non-clinical records in the definition of EHR. Billing records generally are contained in systems separate and apart from the EHR, which would require additional effort on the part of health care providers to compile into a single record set. In addition, billing records do not provide information relevant to the delivery of patient care or care coordination. Patients are able to access billing records through existing mechanisms and share with third parties via a HIPAA authorization. Treating clinical and non-clinical records the same does not appropriately recognize the separate nature of these records in terms of technology or relevance to the delivery of patient care. **We urge OCR to further align its definition of EHRs with the HITECH Act by limiting the scope of an electronic record to clinical information of a health care provider that has a direct treatment relationship with patients.**

We also note that, as defined under the HITECH Act and as proposed by OCR, the scope of clinical information contained within an EHR may encompass not only PHI but also other health-related information that is not PHI. Thus, for example, health care providers that are not HIPAA covered entities may have EHRs, and covered entities may have both PHI and non-PHI within an EHR. We appreciate that OCR has recognized this distinction when proposing to implement requirements related to PHI

that resides in an EHR, implicitly acknowledging that not all individually identifiable health information within an EHR is subject to HIPAA.

CARE COORDINATION AND CASE MANAGEMENT

Care coordination is essential to providing the best patient experience possible, and the AHA appreciates OCR's efforts to modify various provisions to better support covered entities in critical care coordination and case management activities.

Definition of Health Care Operations

The AHA supports OCR's proposal to modify the definition of "health care operations" to make clearer that it includes individual-level care coordination and case management. Historically, certain covered entities have interpreted the definition of health care operations to include only population-based care coordination and management, hindering information sharing due to perceived restrictions on uses and disclosures. Additional clarity regarding the definition of health care operations will remove barriers to health care providers receiving information from health plans to aid in better coordinated care for individuals.

Minimum Necessary Exception

The AHA also supports the proposal to create an exception to the ''minimum necessary'' standard for individual-level care coordination and case management uses and disclosures. Streamlined information sharing will improve care coordination and promote more effective value-based care. While we acknowledge that the minimum necessary standard serves as an important protection in many circumstances, it also can act as an obstacle to crucial information sharing between health care providers and others providing care. Trying to balance the minimum necessary standard prior to disclosing health information often delays or inhibits the effective provision of care to individuals. We believe that OCR's proposal to except disclosures for individual-level care coordination and case management activities will provide practical support for hospitals to coordinate care and improve outcomes.

In response to OCR's specific questions for comment on this proposal, we do not believe that an unintended consequence would be that covered entities will request and receive more information than needed for care coordination and case management, nor that covered entities would then use that PHI for unrelated purposes. Covered entities are accustomed to requesting the information they need, and we expect this will continue to be the case. This proposed exception would simply remove any hesitancy covered entities may have in sharing information based on a potential violation of the minimum necessary standard. Moreover, covered entities are subject to extensive rules regarding how PHI may be used, and this exception will not somehow open the door to potentially abusive practices. Rather, this proposal will help to further facilitate care coordination and case management activities for individual patients and is consistent with the HHS' efforts to encourage such activities, while preserving privacy protections.

Community- and Home-based Services. Additionally, **the AHA supports expressly permitting covered entities to disclose PHI to social services agencies, community-based organizations, home- and community-based service providers, and similar third parties that provide health-related services to specific individuals for individual-level care coordination and case management**. Permitting these disclosures, without a need to distinguish them as health care operations or treatment, will promote better exchanges of needed information for care coordination and enable better care for patients by making it less burdensome to coordinate with service providers working to help patients.

CHANGE IN STANDARDS FOR DISCLOSURES IN INDIVIDUAL'S INTEREST OR IN CONNECTION WITH SERIOUS THREATS

Encouraging Disclosures for Individuals with Substance Use Disorder (SUD) and Serious Mental Illness (SMI)

The AHA appreciates the special attention afforded the SUD and SMI patient population in these proposals, as these vulnerable individuals have unique needs where disclosure of PHI frequently falls into a "gray area." We have long advocated for clear guidelines on appropriate information sharing among clinicians and caregivers, as a lack of clarity can have a chilling effect on practitioners taking on complex cases or sharing information when it is appropriate in fear of violating arcane regulations.

This advocacy has most recently involved encouraging HHS to align the Privacy Rule and 42 CFR Part 2, which requires certain federally funded SUD treatment programs and downstream recipients of PHI to maintain the confidentiality of records related to the diagnosis and treatment of SUD. While HHS notes in this NPRM that Part 2 modifications are "outside of the scope of this rulemaking," it is impossible to discuss PHI disclosures for SUD patients without considering the intersection with that portion of the CFR. The Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020 included several provisions that would alter the statute upon which the Part 2 regulations are based, but requires rulemaking to implement these provisions. We are taking this opportunity to urge HHS to promulgate these rules as soon as possible.

Good Faith Belief

We believe a standard for disclosing based on "good faith belief" would reduce hesitation for appropriate non-physician health care personnel to disclose PHI when in a SUD or SMI patient's best interest, and as such improve outcomes and access to care. If finalized, we suggest HHS also issue sub-regulatory guidance to help operationalize these changes and further take the guesswork out of appropriate information sharing; such guidance should include clear examples of permitted and prohibited activities specific to practitioners who treat SUD and SMI patients, e.g., **clear guidance on the definition of "good faith belief" beyond the absence of bad faith. In addition, as non-clinical care support personnel such as peer counselors become more**

commonplace in treatment of SUD and SMI, we urge explicit direction on who becomes a HIPAA-covered entity and thus subject to these regulations. We are ready to assist HHS in gathering and assessing such examples with the input of our hospital and health system members.

Reasonably Foreseeable Threat
We agree with HHS' rationale behind replacing "serious and imminent threat" with "serious and reasonably foreseeable threat" regarding use or disclosure of PHI. The "reasonable person" standard is generally easier to apply than imminence of threat is to calculate, and would allow clinicians to make *appropriate* disclosures to prevent harm.

The AHA particularly appreciates HHS' acknowledgment that it is unfounded to assume a person is a threat to themselves or others merely by virtue of a diagnosis of SUD or SMI, and that in the context of behavioral health professionals the reasonably foreseeable standard includes the exercise of the specialized training, expertise, or experience of the provider. While we believe that this change is positive and has the potential to prevent incidence of violence, we also must acknowledge that softening the regulatory language could open providers to additional liability if they were not to disclose information in a situation later determined to have foreseeably led to harm. However, this risk is far outweighed by the benefits of the provision.

The AHA also welcomes the benefits these changes will have for the care, treatment and care coordination of individuals across other patient populations. Finally, **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 protected from information blocking enforcement.**

OTHER PROPOSALS

Notices of Privacy Practices
The AHA supports the elimination of the requirement for covered health care providers to make a good faith effort to obtain individuals' written acknowledgment of receipt of a Notice of Privacy Practices (NPP). The AHA agrees with OCR's assessment that the signature and recordkeeping requirements associated with distribution of the NPPs impose unnecessary administrative burdens on covered health care providers. The requirements also do not provide increased privacy protection, nor do they serve the individual well; creating confusion for individuals who

often do not understand the purpose of the acknowledgement and may, for example, erroneously believe the NPP is instead an authorization or other waiver.

OCR further proposes a number of changes to the required content of the NPP. While we support finding ways to promote better understanding and awareness of patients' rights under HIPAA, the proposed changes would require significant resources on the part of hospitals to develop and update the NPP in all of the physical and electronic locations it resides. **Should this proposal be finalized, we urge OCR to create a standard federal notice based on the model NPP created in collaboration with ONC that would provide assurance to health care providers that their NPP complies with HIPAA and ensure adequate time for health care providers to come into compliance.**

Accounting of Disclosures

The AHA appreciates that the NPRM does not include a proposal to establish an individual right to an access report. OCR's previous proposal, which was subsequently withdrawn, did not appropriately balance the relevant privacy interests of individuals with the substantial burdens on covered entities. It also was based on a fundamental misunderstanding of the value to individuals of receiving the particular information that the access report would cover.

There are already a number of ways in which patients are informed about how their information is used and disclosed by a covered entity, including the NPPs. Further, the experience of hospitals continues to suggest that patients are more interested in knowing whether a specific violation relating to their electronic health information has occurred and getting detailed information in response to a specific inquiry and investigation by the hospital's privacy and compliance staff. Patients value these investigations because they provide information about specific violations and what appropriate disciplinary and other measures were taken to ensure that violations do not reoccur. These processes and procedures already are in place and are aimed at ensuring patients receive the information they feel they need and value most. The AHA believes that an additional mandate to provide an access report would not add value to patients and would place unnecessary administrative burden on hospitals in light of existing sources of information and mechanisms for addressing any inappropriate uses and disclosures of their electronic health information.