May 6, 2021

Dr. Robinsue Frohboese
Acting Director and Principal Deputy, Office for Civil Rights (OCR)
U.S. Department of Health & Human Services
200 Independence Avenue, Humphry Building
Washington, DC 20021

Re: Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement

Submitted electronically at: https://www.Regulations.gov

Acting Director Frohboese:

The American Medical Informatics Association (AMIA) appreciates the opportunity to comment on the Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement.

AMIA is the professional home for more than 5,500 informatics professionals, representing frontline clinicians, researchers and public health experts who bring meaning to data, manage information and generate new knowledge across the health and healthcare enterprise. As the voice of the nation's biomedical and health informatics professionals, AMIA plays a leading role in advancing health and wellness by moving basic research findings from bench to bedside, and evaluating interventions, innovations and public policy across settings and patient populations.

AMIA believes that information empowers individuals, but as we have pointed out before, healthcare has lagged other service sectors in reflecting a customer-centric approach. In 1996, HIPAA gave patients a right to a copy of their health information maintained by hospitals, physician offices, and eventually laboratories. However, 25 years later, patients still struggle to leverage this right guaranteed by law.

AMIA therefore supports the direction of the proposals in this rule. In response to OCR's 2018 RFI[1], we identified three core problems with promoting information sharing for treatment and care coordination: (1) it takes too long for PHI to be shared for permitted purposes, including with patients under the right of individual access; (2) HIPAA has been misused to restrict sharing of PHI; and (3) HIPAA has been a barrier to sharing mental health data. We thus applaud OCR for continuing the progress toward resolving these problems in this proposed rule.

Personal Health Applications and Third Parties

[1] https://www.amia.org/sites/default/files/AMIA-Response-to-OCR-HIPAA-RFI_0.pdf

We are pleased that OCR recognizes that patients increasingly wish to direct their data to HIPAA non-covered entities and non-business associates. Thus, we support OCR's proposal to create a separate set of provisions for the right of an individual to direct copies of PHI to a third party. We note, however, that this right must be balanced with new and robust patient privacy protections. As third parties and Personal Health Applications – as OCR proposes to define it – do not fall under the HIPAA Privacy Rule regulations, **we strongly urge OCR to coordinate with the Federal Trade Commission (FTC) to update its Health Breach Notification policies so that there is sufficient protection for patients who use PHAs and/or other third parties to exercise their right of access.**

Alignment with 21st Century Cures Act Final Rule

Finally, Congress has continued to prioritize improved patient data access as a key lever to improve care, enable research, and empower patients to live healthy lifestyles, most recently through 21st Century Cures Act. There are several proposals in this proposed rule that may contradict rules finalized under the Cures Act and/or cause confusion for stakeholders who are subject to both rules. Should these proposals be finalized, **we recommend that OCR coordinate potentially overlapping policies and compliance timelines with the information blocking rules to ensure that the policies are mutually reinforcing.** Most notably, we believe that it is vital for OCR **to review its definition of the HIPAA designated record set (DRS), in light of how the term has been repurposed by ONC and provide additional clarity as to how it should be understood for covered entities and for actors under information blocking.**

Below we outline additional comments and recommendations in response to select questions and proposals in the rule. Should you have any questions or require additional information, please contact Scott Weinberg at scott@amia.org or 240-479-2134. We thank OCR for the opportunity to comment and look forward to continued dialogue.

Sincerely,

Patricia C. Dykes, PhD, RN, FAAN, FACMI

Chair, AMIA Board of Directors
Program Director Research
Center for Patient Safety, Research, and Practice
Brigham and Women's Hospital

(Enclosed: Detailed AMIA Comments Regarding Proposed Modifications to the HIPAA Privacy Rule

Effective & Compliance Dates

OCR requests comment on whether the 180-day compliance period is sufficient for covered entities and business associates to revise existing policies and practices and complete training and implementation.

AMIA Comments: OCR should coordinate the compliance period with those of the information blocking rules that are currently in effect, though have no published enforcement mechanisms at this time. We stand by our previous recommendation to the HHS OIG that it establish an effective date 60 days following publication of a civil monetary penalties (CMP) final rule in the *Federal Register*, followed by a period of enforcement discretion between three and six months.[2] Though this regulation would not apply to providers, we believe that understanding the particulars of information blocking claims and exceptions will be important for all stakeholders so that clarifying guidance and educational information can be broadly disseminated. Once this, and a similar period of learning for providers is completed, then we would support a 180-day compliance period for OCR's proposed modifications.

Adding Definitions for Electronic Health Record or EHR and Personal Health Application

OCR proposes a new definition of Electronic Health Record (EHR) and Personal Health Application.

AMIA Comments: We request clarification on OCR's reason for differentiating between individuals with a direct treatment relationship and those with an indirect treatment relationship in its proposed definition of EHR. The definition assumes that any information from an indirect treatment provider would necessarily be documented in the EHR by the direct treatment provider; however, this assumption may not always be true. For example, if a laboratory report is sent back to the EHR, the ordering clinician may review the information, but would not necessarily replicate every single lab value in their documentation. The distinctions between direct and indirect treatment relationships are thus prone to misinterpretation and confusion. We believe it would be preferable for HIPAA-related protections to apply to individuals who are generating information related to health care, regardless of whether their relationship to an identified patient is direct or indirect.

We further suggest the definition to be slightly amended to: "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, staff, **and researchers.**" Researchers – with or without clinical duties – should be recognized in the definition of EHR. For many years, AMIA has sought to facilitate the use of EHRs to improve care through a number of important avenues. Following the widespread implementation of EHRs, the potential to use in a secure manner the data now stored in siloes throughout the healthcare system to improve care through data analytics has never been greater. Indeed, recouping substantial value from this national investment in EHRs can only be expected if greater access to this information is forthcoming. This will help move us toward the goal of a Learning Health System.[3]

---

[2] https://www.amia.org/sites/default/files/AMIA-Response-to-OIG-Information-Blocking-NPRM.pdf
[3] https://www.ahrq.gov/learning-health-systems/index.html

As for the definition of Personal Health Applications (PHAs), we note that OCR writes that the "proposed definition of personal health application is meant to be consistent with the HITECH Act definition of personal health record (PHR), but specifically addresses certain health applications, which may or may not be PHRs." We understand that both PHAs and PHRs specifically do not fall under HIPAA regulations. However, PHRs are regulated by the FTC under its Health Breach Notification Rule. We request additional clarification on how PHAs will be regulated with respect to privacy and security, especially as OCR grants that some PHAs may also be PHRs. In comments to the FTC last year,[4] AMIA recommended that the FTC take near-term action and develop guidance that 1) Explicitly includes usernames / passwords maintained by an NCE as being considered PHR identifiable health information, thus subject to the HBN Rule if breached; and 2) Expand on the concept of "unauthorized access" under the definition of "Breach of security," to be presumed when a PHR or PHR related entity fails to adequately disclose to individuals how user data is accessed, processed, used, reused, and disclosed. If PHAs will fall under the purview of FTC, we similarly believe that these near-term actions should apply to them, as well.

Thus, we strongly urge OCR to coordinate FTC and other relevant policymakers within HHS and Congress to develop policies to bolster privacy and security for PHAs. As OCR seeks to expand the rights of patient to use PHAs and third parties to direct and access their data, we reiterate our recommendations to: 1) Expand the purview of the HBN Rule to include technology beyond PHRs, including technology described by ONC in its 2016 report on NCEs, such as mHealth and health social media; 2) Ensure uniformity in applying the HBN Rule so that all NCEs that generate health data are subject to the Rule's provisions, not just PHRs; 3) Expand and promote reporting pathways to affected individuals, not simply firms who notice a breach; 4) Ensure the HBN Rule acts as a deterrent to poor data management and security practices through enforcement that is sufficiently stringent and appropriate to compel secure/responsible management of health data; and 5) Ensure alignment with the European General Data Protection Rule, the California Consumer Protection Act, and other relevant consumer data privacy policy.

Whether the Department should instead define EHRs to align with the scope of paragraphs (1)(i) and (2) of the definition of designated record set.

AMIA Comments: In the information blocking provisions of the Cures Act Final Rule, ONC repurposed the definition of designated record set (DRS) outside of the context of a covered entity and HIPAA. Indeed, we note that the definition of DRS has historically been used in relation to patient or an authorized representative access to their records. When ONC added the DRS concept and definition to the definition of electronic health information (EHI) for information blocking, ONC moved DRS considerations from only a patient access issue, to a need for all actors under information blocking compliance requirements to have a better understanding of what the DRS is. Thus, there is an urgent need for a clear and objective understanding of the scope of the DRS.

The current definition of DRS enables subjective understanding, which can lead to contention and confusion across the industry when different covered entities have different definitions. In addition, there are aspects of the definition, such as in 45 CFR 164.501(iii), which would include any information used to make decisions about individuals. This could include a wide variety of

[4] https://www.amia.org/sites/default/files/AMIA-Response-to-FTC-Health-Breach-Notification-Rule.pdf

information, potentially including unverified external records that may be used in clinical decision support algorithms.

We ask that OCR review the definition of DRS, considering its new use cases. OCR should work with ONC to provide additional clarity and guidance as to how it should be understood for covered entities and for actors under information blocking.

Whether the proposed definition of EHR includes PHI outside of an electronic designated record set, whether it should, and examples of such PHI.

AMIA Comments: We believe that the proposed definition of EHR should be broad enough to include PHI outside the designated record set. The patient should have the right to see and control anything that is patient information.

Should "health care clinicians and staff" be interpreted to mean all workforce members of a covered health care provider?

AMIA Comments: There may be instances when non-clinician staff of a health care provider may need to access files on a need-to-know basis. We do not believe that third parties, such as insurers, should fall under this interpretation.

Strengthening the Access Right to Inspect and Obtain Copies of PHI

OCR proposes to add a new right at 45 CFR 164.524(a)(1)(ii) that generally would enable an individual to take notes, videos, and photographs, and use other personal resources to view and capture PHI in a designated record set as part of the right to inspect PHI in person. OCR is also proposing to extend the right to inspect to situations where mutually convenient times and places include points of care where PHI in a designated record set is readily available for inspection by the patient.

AMIA Comments: AMIA generally supports patients having complete access to their data. However, this must be balanced with privacy protections for other patients. While we recognize that patients will use their personal devices to inspect their own protected health information, we are concerned about health care settings where patients might – intentionally or unintentionally – capture another patient's information via audio or video. Covered entities should be granted more flexibility in deciding which care settings this should be permitted. In particular, if a patient wishes to make a visit recording, a CE or its representative must be permitted enough time to ensure the data of other patients is not being captured as well.

The benefits of the latter proposal are unclear, as the requirement that "a covered health care provider is not permitted to delay the right to inspect" is potentially disruptive and problematic. This is especially true if providers are already granting patients access to their records via a patient portal. At the point-of-care, the information is only available in the EHR through a login of one of the clinicians or staff. To allow a patient to sit at a computer using another's login to browse through the chart, albeit their own, is prone to potential issues with record integrity (e.g. what if they clicked the wrong button?) and could take considerable unreimbursed staff time. We continue to support other efforts to share clinical notes with patients during visits, including the successful OpenNotes initiative, and recommend that OCR work within HHS at-large to encourage more providers to

share notes with patients through federal policies, such as Medicare and Medicaid payment programs.

Allowing CEs to provide copies in lieu of in person inspection of PHI

OCR is seeking comments on whether covered entities should be permitted to provide copies of PHI in lieu of in-person inspection of PHI when necessary to protect the health or safety of the individual or others, such as during a pandemic.

AMIA Comments: We believe that this should be an acceptable option, regardless of whether public health crises are occurring. The rights should be the same as those for receiving electronic health data – time frame, ease of access, low cost, etc. There should, however, be additional restriction on access for health/safety of others. It would be problematic, in the behavioral health context for example, if extremely delusional or agitated individuals could demand access to their records at any point.

Modifying the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access: Requests for Access

OCR proposes that a covered entity may require an individual to make a request for access in writing (in electronic or paper form), provided that it informs the individual of such a requirement and does not impose unreasonable measures that impede the individual from obtaining access when a measure that is less burdensome for the individual is practicable for the entity.

AMIA Comments: AMIA generally supports this proposal. However, we recommend further defining "unreasonable measures," which should include, at the least, coming in person, using a fax machine, and using mail, barring a major concern about identity that would need to be approved by someone high ranking to justify the burden on the patient.

Modifying the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access: Addressing the Form of Access

OCR seeks guidance on whether a covered health care provider should be required to inform an individual who requests that PHI be transmitted to the individual's personal health application of the privacy and security risks of transmitting PHI to an entity that is not covered by the HIPAA Rules.

AMIA Comments: We note that individuals generally do not have sufficient understanding of the risks of security breaches with various apps or software products. Virtually no one reads or could understand the fine print of security/privacy agreements with apps, and even if they did, an individual whose information was released via a breach of such an app would have almost no ability to take legal action, even if they could afford to do so financially. The large number of existing breaches in other realms has been considerable and should be a warning to the wholesale push for individuals to share PHI with a host of potentially unscrupulous actors.

Further, breaches are not the only concern that patients should consider. Patients should also be aware of how a third party will use their data. If a third party has a policy of selling patient data to whomever will pay, patients should know that possibility exists and ideally would have a way to learn if that was the case.

With these concerns in mind, however, we do not believe that notifying the patient of privacy and security risks should be incumbent upon the provider. Rather, OCR should partner with ONC to provide model language about privacy risks based on ONC's various educational resources that all providers could easily share at the time of a data request (e.g. during an OAuth session).[5,6] This would ensure consistent messaging to patients. We further recommend that OCR and ONC heed the Privacy and Security recommendations in the Health Information Technology Advisory Committee's (HITAC) 2019 Annual Report.[7] Finally, we urge OCR to work with ONC to develop a data sharing labeling requirement for third party apps that would allow patients to easily see how their data are being used and/or shared.

Proposed: Add two new sections to section 164.524(c)(2)(iii) of the current Privacy Rule

OCR proposes to add sections that when a summary is offered by CE in lieu of access the CE must tell individual that they still have a right to contain a copy of the PHI or direct an electronic copy in an EHR to a third party if they do not agree to receive the summary.

AMIA Comments: AMIA notes that 164.524(c)(2)(iv)(B) may be problematic for situations where someone, such as a family member, provides information in confidence to the health provider, but asks that it not be disclosed to the patient. This is a common occurrence in psychiatry, for example, when family are fearful that the patient may behave violently towards them. This information still needs to be able to be recorded in the chart for medicolegal reasons.

Modifying the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access: Addressing the Individual Access Right to Direct Copies of PHI to Third Parties

OCR is proposing to create a separate set of provisions for the right of an individual to direct copies of PHI to a third party.

AMIA Comments: AMIA supports these provisions, but it should be followed up with formal guidance on how this would apply in different situations. For example, patients may want to direct their health data to businesses outside of medicine, such as with an architect who is going to modify a home to make it less prone to induce falls, or to a personal trainer who will help a child with cerebral palsy practice her walking. If increased sharing is the desired outcome, there is also a need for better visibility into who accessed and acquired patient data through such pathways. As we have stated previously, better audit trails and accounting of disclosures are necessary to ensure accountability and oversight.

We additionally support the proposal to limit the requested PHI to electronic copies in the EHR, excluding psychotherapy notes, from disclosure requirements.

---

[5] https://www.healthit.gov/topic/patient-access-information-individuals-get-it-check-it-use-it
[6] https://www.healthit.gov/topic/patient-education-and-engagement
[7] https://www.healthit.gov/sites/default/files/page/202003/HITAC%20Annual%20Report%20for%20FY19_508.pdf

AMIA also strongly recommends that DNA sequence data additionally be *excluded* from such requests, unless the patient specifically requests that it be disclosed. In many situations in the research field, DNA sequence data is considered de-identified, which allows the use and sharing of genetic data in a much more permissive manner compared to other data elements that are considered PHI and sensitive. However, the advancement of sequencing science has made the identification of individuals based solely on DNA sequences more and more commonplace. In fact, the National Human Genome Research Institute recognizes that "each person's DNA sequence is unique and ultimately, and there is enough information in any individual's DNA sequence to absolutely identify her/him."[8] As early as 2004, researchers have shown that a person can be uniquely identified with access to just 75 single-nucleotide polymorphisms (SNPs) from that individual.[9] The scientific community is becoming more aware of the increasing amount of available genetic data. This in turn is increasing the potential for privacy violations due to either intentional, open sharing of genetic data, or through unintentional data breaches. Given these, and other factors, we recommend that genetic data at the genome scale should be considered PHI.

In addition to genetic data, AMIA believes that all health data must always be collected, managed, and shared in ways that minimize the risk of reidentification of individuals, both now and in the future. We note that it is far too easy to reidentify individuals today when CEs share PHI in a HIPAA-permissible manner, with the full knowledge that sharing this information with third parties can allow identification of the individuals whose data was shared – often without the express permission of those patients and without an option for them to object. OCR should work with ONC to require entities engaging in sharing of deidentified data to (a) notify patients prior to sharing the data, and (b) give each patient the right to opt out of their data being shared.

OCR seeks comments on approaches it may take to clarify that the Privacy Rule permits covered entities to use HIEs to make "broadcast" queries on behalf of an individual to determine which covered entities have PHI about the individual and request copies of that PHI.

AMIA Comments: This permission should be viewed as one about patient access. We thus recommend that OCR clarify this permission further by adding that "covered entities may use HIEs to make 'broadcast' queries on behalf of an individual **with their notification and consent,** to determine …"

OCR requests comment on how to interpret the phrase "clear, conspicuous, and specific," including when the request is verbal.

AMIA Comments: Verbal request are potentially problematic in terms of health information management at large organizations. We caution OCR that tracking and accountability would likely be impacted if individual providers are sending info based on verbal requests.

Adjusting Permitted Fees for Access to PHI and ePHI

[8] "Use of Human Subjects in DNA Sequencing." n.d. National Human Genome Research Institute (NHGRI). https://www.genome.gov/10000921/

[9] Lin, Zhen, Art B. Owen, and Russ B. Altman. 2004. "Genetics. Genomic Research and Human Subject Privacy." Science 305 (5681): 183.

OCR proposes to modify the access fee provisions for the individual right to inspect PHI and to obtain copies of PHI about the individual.

AMIA Comments: AMIA believes that there should be as few barriers as possible for patients to obtain their health data. Thus, we are generally supportive of a requirement to eliminate fees for digital items. However, we also recognize that there is a Fee Exception under the information blocking rules. OCR must coordinate with ONC on guidance to help affected actors comply with both rules without running afoul of one or the other.

Technical Change to General Rules for Required Business Associate Disclosures of PHI

OCR proposes to insert clarifying language to specify that a business associate is required to disclose PHI to the covered entity so the covered entity can meet its access obligations. However, if the business associate agreement provides that the business associate will provide access to PHI in an EHR directly to the individual or the individual's designee, the business associate must then provide such direct access.

AMIA Comments: AMIA appreciates this proposed clarification. Increasingly, PHI is organized, managed, and/or stored by third parties, such as cloud based EHRs and image repositories. This potentially complicates patients' access to their non-provider-hosted PHI. We thus support the inclusion of the proposed clarifying language.