American Health Information Management Association®

233 N. Michigan Ave., 21st Fl., Chicago, IL USA 60601-5809 | www.ahima.org | 312.233.1100

June 12, 2023

Director Melanie Fontes Rainer
Office for Civil Rights
US Department of Health and Human Services
200 Independence Avenue, SW
Room 509-F, HHH Building
Washington, DC 20201

Dear Director Fontes Rainer:

On behalf of the American Health Information Management Association (AHIMA), I am responding to the Office for Civil Rights (OCR) *HIPAA Privacy Rule To Support Reproductive Health Care Privacy* proposed rule, as published in the April 27, 2023 *Federal Register*.

AHIMA is a global nonprofit association of health information (HI) professionals who work with health data for more than one billion patient visits each year. The AHIMA mission of empowering people to impact health drives our members and credentialed HI professionals to ensure that health information is accurate, complete, and available to patients and providers. Our leaders work at the intersection of healthcare, technology, and business, and are found in data integrity and information privacy job functions worldwide.

The following are our responses to selected provisions.

1. Executive Summary

A. Overview

It is noted in the proposed rule that OCR is prevented by statute from updating the HIPAA Privacy Rule multiple times in a 12-month period. While this may be true and OCR does not intend to update the HIPAA Privacy Rule multiple times, this current proposed rule reflects the third proposed modification of the HIPAA Privacy Rule to be released since 2020. With the other two rules[1][2] yet to be finalized, there is increasing anxiety among those that must comply with the HIPAA Privacy Rule about the work needed to prioritize and operationalize the updated regulatory requirements to ensure compliance. As a result, AHIMA urges OCR to provide a roadmap and timeline for when they anticipate finalizing the previously proposed HIPAA Privacy Rule modifications.

[1] https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/hipaa-care-coordination/index.html.
[2] https://www.federalregister.gov/documents/2022/12/02/2022-25784/confidentiality-of-substance-use-disorder-sud-patient-records.

Providing a roadmap and timeline will help covered entities better plan financially and organizationally for when they may need to undertake key activities. For instance, all three proposed rules require an update to the Notice of Privacy Practices (NPP). Updating the NPP is a significant undertaking for covered entities but is more disruptive to small and under-resourced covered entities who do not have access to the same legal services compared to more well-resourced covered entities. Updates to the NPP take legal experts significant amounts of time to review existing policies, understand new requirements, and finalize the updated NPP.

Without an understanding of when a covered entity's NPP may need to be updated, it is difficult for regulated entities to plan if they require legal representation to complete the update when planning budgets for the following year. Providing a roadmap is crucial for ensuring updates to the NPP proposed in this, and other, proposed rules do not disrupt a covered entity's day-to-day activities. This roadmap would also ensure a smoother and quicker compliance timeline as well, since covered entities would have ample notice of when they need to comply. If OCR were unable to provide such a roadmap AHIMA encourages the agency to assist providers in understanding how best to sequence preparation activities to ease the future compliance burden.

IV. Section-by-Section Description of Proposed Amendments to the HIPAA Privacy Rule

AHIMA urges, once this rule is finalized, that OCR provide extensive education to the provider community prior to the compliance deadline outlined in the proposed rule. As noted within the proposed rule, states across the nation have a patchwork of laws related to both patient privacy and the disclosure of reproductive health data as defined in the proposed rule. This patchwork makes it difficult for organizations, such as AHIMA, to provide state-level guidance and increases the risk of confusion among covered entities on how to comply with the proposed rule.

Given the nuances and intricacies presented in the proposed rule and the state privacy and reproductive health legal landscape, providers may be left in the troubling position of potentially violating a patient's privacy due to confusion versus willful intent. Similarly, given the HIPAA breach implications that could be at play, if a provider inappropriately disclosed the described reproductive healthcare information, there is the potential for under-resourced regulated entities to be at a higher risk for negative financial consequences than better-resourced regulated entities. Under-resourced regulated entities across the nation often lack the staff knowledge and abilities that larger regulated entities have to understand and implement complex regulations, such as those proposed. Often, under-resourced providers rely on education and guidance provided by the regulating entities, such as OCR, to help them understand their regulatory obligations.

A lack of clarity on these requirements also puts patients at risk as their data may be inadvertently disclosed. Additionally, given that under-resourced regulated entities will have the hardest time achieving compliance with the requirements outlined by OCR in this proposed rule, it means those patients are placed at greater risk of having their reproductive data inappropriately disclosed. This could become a health equity concern for patients that receive care at under-resourced covered entities versus more resourced facilities. Patients deserve the same right to privacy no matter where they receive care, nor should their sensitive health information be at risk of being inappropriately disclosed because a provider lacked the resources to understand and comply with the complex intersection of state and federal privacy laws. Additionally, given this risk to patients and the complexity of the legal landscape, where possible, OCR should also extend this education to the patient community.

Due to the above reasons, AHIMA recommends OCR engage in an extensive education campaign to inform covered entities, especially providers, on how to achieve compliance if the provisions in this proposed rule are finalized. The education should take the form of, but not be limited to, educational webinars, information graphics, FAQ sheets, guidance, office hours, and other education formats. OCR is well-positioned to provide this education and would

help ensure more consistent compliance nationwide. While providing this education, OCR should also consider providing enforcement discretion until a time when a majority of the health system has access to the educational tools.

A. Section 160.103-Defintions

OCR proposes specific details on what types of medical conditions and procedures are included under the definitions proposed in the rule. This specificity is aimed at providing clarity to ensure the proposed definitions are free from misinterpretation by a third party. This specificity is not present in other regulatory texts discussing similar information privacy issues. As a result, such specificity could make it difficult for health information (HI) professionals to operationalize the proposed rule as the specific examples, as outlined, are included in all parts of a patient's health record. The reality of a patient's health record is that such information is documented as structured and unstructured data. As a result, it will be difficult to find and separate each individual piece of information that is identified in the proposed detailed definitions. The proposals on what data should be protected and which data is safe to release should rely on a covered entity's expertise and judgment. Allowing a covered entity to further define inclusion without the specificity OCR provided ensures covered entities can operationalize these requirements in a way that best aligns with their organizational structure.

Additionally, the proposed rule appears to leave certain definitions open-ended such as the definition for reproductive healthcare that includes numerous specific treatments, but also concludes with the statement, "and other types of care, services, or supplies used for the diagnosis and treatment of conditions related to the reproductive system." This open-ended nature of the definition has already caused confusion, with organizations using different interpretations of what is included in care related to the reproductive system. For instance, depending on the organization, care for transgender individuals may be included in the definition while others may think transgender care is outside the scope of the definition. Given the specifics offered in the proposed rule and the potential for reinterpretation, this rule could be burdensome on HI professionals to operationalize. Given the proliferation of reproductive data throughout a patient's record, including in clinical notes, the proposed definition could cause entire patient records to be covered by this proposed rule. These parameters, if finalized, could fail to achieve OCR's specific goal of protecting certain parts of a patient's record while creating enormous burden on those tasked with managing the record.

We urge OCR to work with relevant stakeholders to revise the proposed definitions to make them actionable and more understandable. Given the sensitive nature of this information, it is critical that OCR ensures the burden to implement any finalized proposals is minimal. By working with the healthcare community, OCR can ensure its policy goals are achieved with limited impact on the burden experienced by covered entities.

4. Request for Comment

OCR proposed multiple updated or new definitions for key terms throughout the proposed rule. To maintain definitional alignment across federal agencies and to facilitate compliance, we urge OCR to review the proposed definitions and compare them to the data elements mandated for inclusion in Certified Electronic Health Record Technology (CEHRT) products by the Office of the National Coordinator for Health IT (ONC) and in the electronic clinical quality measures (eCQMs) that providers are required to report to the US Centers for Medicare and Medicaid Services (CMS). While we are encouraged by OCR's desire to provide clarity to key terms, if the definitions fail to align with the data standards that are implemented to maintain such information, there could be a bifurcation of data capture and exchange. This increases the inaccuracy of patient health records and increases the risk of different EHRs maintaining different data dictionaries. Therefore, we urge OCR to review its proposed

definitions and adjust as needed to ensure data definition alignment is maintained across the standards environment.

C. Section 164.509 - Uses and Disclosures for Which an Attestation

2. Proposal

AHIMA acknowledges and understands the reason for OCR's proposal to require regulated entities to obtain a signed attestation that the disclosed health information will not be used to investigate or punish someone for seeking, obtaining, or providing legal healthcare services. While we do not intend to comment on the merits of this specific proposal, we do want to share our operational concerns related to the method for the collection and storage of the attestation given the unique role HI professionals play in privacy and compliance.

The proposal as described by OCR, places significant burden on HI professionals and release of information (ROI) specialists within a covered entity. It will be ROI specialists who will be tasked with understanding whether an attestation is needed and ensuring the required entities sign them. Unfortunately, these decisions and evaluations may be outside their area of knowledge at times and may require additional legal support from within the covered entity to understand whether the attestation is in fact needed. This complexity leaves room for potential error and could fail to accomplish the goal of protecting reproductive health data.

Additionally, while the proposed rule offers protection for providers from a potential breach if a requestor misrepresents the intended use of the data on an attestation form, there are no ramifications or penalties for the requestor. It creates a scenario where attestations will need to be signed by a requestor but carry little to no ability to protect patient data. As a result, even if the provider ceases to send data to a requestor that misrepresented themselves, the patient's information has already inadvertently been shared with the requestor and the privacy of their sensitive health information is put at risk. Given the significant burden needed for compliance with minimal guarantee of protection, AHIMA recommends OCR reevaluate the attestation requirement to ensure its intended goals are accomplished by implementing this requirement.

Should OCR finalize this requirement, AHIMA suggests the inclusion of a safe harbor from penalty and guidance on how a covered entity will be judged in determining whether an attestation is credible. While the proposed rule states it is not a covered entity's responsibility to ensure data is being used as described in an attestation, a covered entity that becomes aware of data misuse must revoke the attestation. The proposed rule lacks specifics on how a covered entity should evaluate whether data misuse has occurred and what criteria should be used to determine whether a request is untrustworthy. Without such guidance, covered entities could deny reasonable and justifiable requests for data out of fear the data could be misused at a later date. As a result, AHIMA recommends OCR provide additional guidance regarding the attestation implementation process in addition to a safe harbor protecting those covered entities acting in good faith from penalty if OCR were to finalize these proposals.

Additionally, if finalized, it is crucial for OCR to provide clarity to covered entities about the length of time in which an entity must retain a copy of the signed attestation form. While we applaud OCR for allowing covered entities to collect the attestation and signature in a digital format, storing the forms is still a difficult process even in a digital format. As a result, we encourage OCR to indicate the length of time in which such an attestation must be retained by the covered entity prior to disposition and destruction, even if that length of time is consistent with other document retention rules in HIPAA.

Additional education is also needed on how the attestation forms can be provided to the requestor for signature and whether the requirements are consistent with the requirements surrounding a patient attestation when they

receive an NPP. In the past, OCR has provided examples of how the patient attestation form for the NPP should be presented and signature should be captured. Similar guidance would be appreciated to assist regulated entities in their compliance activities. A detailed education campaign in either pictorial or video format could also provide additional clarity.

Furthermore, AHIMA recommends OCR convene various stakeholders to understand the true implications of requiring attestations, such as the ones outlined in the proposed rule. Improving data flows and data sharing has been a top priority for the US Department of Health and Human Services for over a decade. AHIMA is concerned the attestation requirement could discourage such sharing as some regulated entities may misunderstand the attestation requirements. Engagement with the stakeholder community, especially those that will be responsible for operationalizing the proposed rule, could provide OCR with important insights related to the implications associated with the implementation and execution of the attestation requirements.

Finally, OCR indicates it is not the covered entity's responsibility to investigate if an entity requesting data has falsified information on their attestation. However, it is not indicated in the proposed rule whether the covered entity is required to report that a requestor has misused data obtained through an attestation. Additional clarity from OCR would be helpful in understanding a covered entitie's obligations as part of the attestation process.

3. Request for Comment

The proposed rule indicated that providers should limit the amount of patient data sent in response to a request to "minimum necessary." AHIMA supports limiting data exchange to information that is needed to satisfy a particular purpose or function to limit unnecessary or inappropriate disclosure of protected health information (PHI) and believes this is a bedrock principle of maintaining the privacy and confidentiality of a patient's record. However, it is important to note that at this time, there are significant limitations within CEHRT to segment sensitive health information, like reproductive health, from the rest of a patient's record. While some EHR systems do have limited capabilities to segment this data, many more function in an "all or nothing" or document-level segmentation exchange and access environment.

Private sector stakeholders have been working to identify solutions to improve data segmentation within EHRs. The ONC recently released their HTI-1[3] proposed rule that proposes to rectify some of these limitations. Within ONC's proposed rule, developers of CEHRT would be required to implement the ability for patients to flag data that should not be disclosed or redisclosed due to patient privacy preferences. AHIMA urges OCR to review the HTI-1 proposed rule and provide comment on whether the provisions on flagging individual data elements for privacy would fulfill the goals outlined in this proposed rule. Similarly, we urge OCR to engage in stakeholder feedback and listening sessions with relevant stakeholders to discuss the feasibility and ongoing ability to segment health data and how to advance data segmentation at the data element level, including a roadmap to the future. Until then, we recommend OCR refrain from the proposed data segmentation requirements given the difficulty providers would face to implement them.

The health IT community will continue efforts to advance data segmentation, but additional work is needed to make widespread data segmentation capabilities a reality. It is important for OCR to play an active part in these conversations, and we hope they will assist in outlining and implementing data segmentation capabilities.

E. Section 164.520-Notice of Privacy Practices for Protected Health Information

[3] https://www.healthit.gov/topic/laws-regulation-and-policy/health-data-technology-and-interoperability-certification-program

3. Request for Comment

AHIMA has highlighted the need for clarity regarding the timeline for updates to the NPP in this letter. However, we also urge OCR to explore consolidating all NPP updates into one proposed rule in which the public can provide feedback on prior to finalization. Combining all proposed NPP requirements into a single proposed rule allows a covered entity to undertake one revision to their NPP and could alleviate the cost and burden associated with multiple revisions. For example, in addition to updating the NPP, covered entities would need to update the corresponding business associate agreements (BAAs) that rely on the contents of the NPP. This additional contract modification could increase the burden and cost of updating an NPP multiple times in successive years. AHIMA members reviewed the burden of cost table included with the proposed rule and disagree with the analysis of cost burden per organization, believing it is significantly higher. The true cost burden for responding to an NPP update is difficult to estimate as different organizations of size and magnitude will experience different levels of burden. Condensing the NPP updates requirements into a single rule could help alleviate some of this administrative burden, ensuring that covered entities could focus their time and efforts on understanding what is required to update the NPP and how best they can ensure they are compliant while also improving the clarity of the NPP for an improved patient experience.

AHIMA thanks OCR for the opportunity to provide input on this important proposed rule. We remain steadfast in our commitment to protect patient data and assisting covered entities in their compliance activities. Moving into the rest of 2023 and 2024, we look forward to continuing our partnership with OCR and hope we can continue to be a resource for the agency. If you have any questions or would like to discuss our comments further, please do not hesitate to contact AHIMA's Director of Regulatory Affairs Andrew Tomlinson at Andrew.tomlinson@ahima.org.

Sincerely,

Lauren Riplinger, JD
Chief Public Policy and Impact Officer