American Health Information Management Association
35 W. Wacker Dr., 16th Floor
Chicago, IL 60601

February 27, 2025

Anthony Archeval
Acting Director
Office for Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, DC 20201

Dear Acting Director Archeval:

On behalf of the American Health Information Management Association (AHIMA), I write in response to the Office for Civil Rights (OCR) HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Health Information Proposed Rule, published in the January 6, 2025 *Federal Register* (RIN 0945-AA22).

AHIMA is a global nonprofit association of health information (HI) professionals, with over 61,000 members and more than 88,500 credentials in the field. 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 clinicians. Leaders within AHIMA work at the intersection of healthcare, technology, and business, occupying data integrity and information privacy job functions worldwide.

AHIMA agrees with OCR that changes must be made in healthcare to improve the privacy, security, and protection of electronic protected health information (ePHI) to ensure patient care can be provided in a trustworthy and safe manner. HI professionals directly manage ePHI and the processes and workflows that handle this sensitive data and they have unique insights into the security protections and vulnerabilities that put ePHI at risk. AHIMA believes work must continue to increase resiliency in the healthcare system, improve protection against cyber threats and attacks, and support healthcare organizations in preparation against, during, and after cyber incidents.

AHIMA provides detailed comments below but in general recommends that OCR:

- **Undertake a risk stratification analysis and prioritize requiring proposals that will lead to meaningful and measurable improvements in security;**
- **Consider the regulatory and financial burden of implementing the proposals included in the rule, how they will impact compliance, and adjust the proposed requirements accordingly;**

- **Consult with healthcare entities, vendors, and business associates to create more comprehensive cost and impact analyses to better understand the feasibility of implementation; and**
- **Support and provide resources to covered entities in educating and monitoring business associates on their responsibilities and obligations to implement HIPAA Security Rule requirements.**

The following are detailed comments and recommendations on selected sections of the proposed rule.

Technology Asset Inventory

OCR proposes to require entities to conduct and maintain a written technology asset inventory and network map of its electronic information systems and all assets that may affect the confidentiality, integrity, or availability of ePHI. This inventory is to be done on an ongoing basis but at least every 12 months, or when there is a change in the entity's environment or operations that may affect ePHI.

Entities' knowledge of where ePHI lives in their information technology (IT) systems and the factors that can affect the protection and movement of ePHI are critical to ensuring safeguards and protections are as comprehensive as possible. While a technology asset inventory is a valuable and supported concept and can provide more informed and enhanced security against threats, this proposal will be burdensome to implement, particularly for small, rural, and otherwise under-resourced healthcare entities. We also note that such an inventory and network map not only includes organizations' infrastructure, but also the information that these systems hold, which can become complex to map.

AHIMA urges OCR to provide more information around the "maintenance" implementation specification of this requirement, particularly the requirement that entities must conduct and update the inventory when there is a change in environment or operations. Technology is evolving along with the relationships between business associates, vendors, and other healthcare organizations that entities interact with. This creates a challenge for covered entities when updating and implementing requirements. Many entities are growing and acquiring other, smaller entities and facilities, adding complexity when they must repeat the inventory process each time there is such a change. When entities grow and/or merge, gathering information on the extent of an acquired entity's security protections is time-consuming. Gathering resources needed to implement basic requirements also requires additional dedicated time and resources, especially given the varied security safeguards of smaller, under-resourced entities. Similar challenges extend to meeting this requirement when dealing with the integration of products from an electronic health record (EHR) vendor. Changes from EHR vendors that update systems can be on a quarterly basis, and updating a technology asset inventory after each system update would require significant time and resources.

AHIMA urges OCR to provide more clarity on the definitions and expectations within this proposal to allow entities to better prioritize resources to implement this requirement. We recommend OCR

provide examples, resources, incentives, and funding for entities to develop well-informed and comprehensive technology asset inventories and network maps with minimal burden. Additionally, OCR should consider this proposed requirement be accompanied by appropriate positive incentives for entities to achieve compliance. If such an approach is adopted, OCR could work with entities to develop and share best practices, guidance, and resources based on industry successes that would help with implementation of future compliance requirements.

Network Segmentation

OCR proposes to require that covered entities and business associates segment their electronic health information systems, defined as a physical or virtual division of a network into multiple segments, creating boundaries between the operational and IT networks to reduce risks. What constitutes reasonable and appropriate network segmentation depends on the regulated entity's risk analysis and how it has implemented its network and relevant information systems.

Segmentation of electronic health information systems is a valuable practice to safeguard against the cascading impacts of cyber threats and attacks. However, this proposal is complex and burdensome to implement, especially for smaller entities. Network segmentation requires entities to develop contracts with new vendors and implement new systems, which will involve data migration, and is a lengthy and intensive process. Additionally, having data and assets on separate networks presents challenges in getting devices on those segments to communicate. The communication obstacles can be costly and dangerous, complicating the use of technology in emergency and urgent situations, while also slowing down patient care across care settings. There is also a lack of clarity about what constitutes reasonable and appropriate network segmentation as written in the rule. Reasonable and appropriate segmentation will vary depending on the entity's size and characteristics, business associate agreements, the entity's level and volume of health and administrative data, the number of patients the entity serves, how complex the risk analysis is, as well as additional factors that impact an entity's ePHI.

AHIMA recommends OCR provide a decision matrix or similar type of resource for entities on how to determine what is reasonable and appropriate based on the aforementioned factors. Smaller entities working with fewer patients and less data may not have to segment as deeply as larger entities. AHIMA urges OCR to provide guidance, use cases, and other additional information to entities to clarify the level of segmentation needed and how segmentation would be impacted by an entity's characteristics.

Multi-Factor Authentication

OCR proposes to require the use of multi-factor authentication (MFA), defined as information known by the user, an item possessed by the user, and a personal characteristic of the user. A user would be required to provide at least two separate factors from two separate categories to authenticate identity.

AHIMA supports the concept of requiring users within healthcare entities to verify their identity in a rigorous way beyond a simple username and password login. However, MFA is just one method of accomplishing reliable identity verification and may not be the best solution for all care settings. MFA mechanisms often send alerts to another device to complete verification, such as a personal cell phone or email. These devices and services are not always accessible in healthcare environments where there is no cellular service, or devices are not permitted due to potential interference with other devices used for patient care.

For that reason, AHIMA urges OCR to consider recognizing tap-and-go technology as an acceptable method of identity verification. Tap-and-go technology is used when the user has a key card that is tapped to a sensor on the computer that logs a user in without having to type any information, remember unique PINs and keys, or use external devices to authenticate. AHIMA members report tap-and-go technology is used heavily across different care environments, known to be very secure and reputable, and considered an industry best practice.

Requiring MFA as the only solution may inhibit the HIPAA Security Rule from remaining flexible in the evolving digital landscape as it does not leave room for advancements in identity verification technology that may provide better security with a lower risk of interrupting patient care. AHIMA supports the ability of entities to continue using tap-and-go technology and recommends OCR include this technology as a valid method of identity verification along with MFA in this requirement. If OCR moves forward with requiring MFA, we recommend introducing the requirement only in administrative operations first, before requiring it for use in patient care interactions, while still preserving the use of tap-and-go technology. If this requirement is finalized, OCR should clarify and refine where MFA or any identity verification is needed in the healthcare entity. Requiring MFA in all technology assets and at each point of care can delay patient care, especially in emergency or urgent care situations. AHIMA encourages OCR to consider and compare the benefit of requiring MFA against the risk of users inadvertently creating vulnerabilities in data security when trying to find ways to bypass these requirements in order to provide timely patient care.

Increased Regulatory Burden and Regulatory Impact Analysis

Regulatory Compliance Burden

Throughout the proposed rule, OCR hypothesizes many HIPAA-covered entities do not follow the requirements within the HIPAA Security Rule because they choose not to or do not understand the rule. In reality, those unable to attain compliance often fail to do so due to a lack of resources available or work to achieve compliance to the best of their knowledge but may require additional clarity on the current requirements.

The HIPAA Security Rule requirements are critical to ensuring the security of an entity and its ePHI, however, these requirements are not funded and the lack of flexibility in the number of compliance

pathways poses barriers to compliance. Without resources and assistance, entities often have no choice but to prioritize the requirements they are financially able to implement. **AHIMA recommends OCR provide funding, resources, guidance, and education for entities on how to best implement the proposed HIPAA Security Rule requirements to reduce the compliance burden.** We also recommend, as OCR works to provide this assistance, that additional flexibilities to support for small, rural, and otherwise under-resourced entities are considered by OCR.

To assist covered entities in compliance activities, AHIMA urges OCR to provide and incentivize the use of industry standards. Utilizing consensus industry standards creates a predictable environment covered entities can operate in to lower the burden for compliance. To further the adoption of industry standards, AHIMA urges OCR to preserve and enforce the requirements in Public Law 116-321, signed by President Trump in 2021. Public Law 116-321 directs OCR to consider the adopted use of industry standard cybersecurity practices utilized by HIPAA-covered entities and business associates while making a determination during an enforcement action. By implementing this law, OCR can provide a predictable compliance pathway that reduces burden on covered entities while incentivizing adoption with little burden placed on OCR.

Finally, a notable cost incurred by providers during compliance is ensuring HIPAA Security Rule requirements are implemented by their business associates and adjusting business associate agreements as needed to ensure compliance activities cascade from the provider to the business associate. Revising business associate agreements is a complex and time-consuming process. Since business associates are required to self-report breaches to covered entities, such as what happened during the Change Healthcare breach, providers are required to ensure they regularly monitor business associates for compliance. This is an ongoing process, with additional time burden incurred if a provider must play an active role in the investigation of a business associate's potential breach to determine which entity needs to notify both patients and OCR. To reduce this burden, AHIMA recommends OCR consider the time and expense burden placed on providers as part of these investigations and provide education to all covered entities to ensure business associates are complying with the Security Rule, thus lessening the review burden on providers.

Proposed Regulatory Impact Analysis

The regulatory impact analysis and associated cost estimates in the proposed rule do not fully capture the burden placed on providers to achieve compliance. The existing analysis in the proposed rule does not consider such factors as educating employees and staff on the impact of these proposals, the cost of compliance, and the cost of conducting initial and ongoing penetration testing and assessments. AHIMA therefore encourages OCR to prioritize the proposals that will lead to meaningful and measurable improvements in security by looking at which proposals will address high risk issues and adjust the requirements and compliance timelines accordingly. Providing flexibility for requirements that address low risk areas will encourage entities to prioritize time and resources on more meaningful requirements.

A revised regulatory impact analysis by OCR that captures the true burden for compliance is necessary for organizations to plan for implementation if this rule is finalized.

Thank you for the opportunity to provide comments on this proposed rule. AHIMA remains a committed partner to OCR in improving the cybersecurity of ePHI in all areas of healthcare. If you have any questions or if AHIMA can provide any further information on this letter and its recommendations, please contact Tara O'Donnell, Manager of Regulatory Affairs, at tara.odonnell@ahima.org.

Sincerely,

Lauren Riplinger, JD
Chief Public Policy & Impact Officer