March 7, 2025

Anthony Archeval, Acting Director
Office for Civil Rights
Office of the Secretary
Department of Health and Human Services
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue SW
Washington, DC 20201

Re: Comment on Notice of Proposed Rulemaking: "HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information", RIN Number: 0945–AA22; Docket No. HHS–OCR–0945–AA22

Acting Director Archeval,

Thank you for the opportunity to address changes in the NPRM*, HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information*. These proposals represent the first significant revision of the HIPAA Security Rule in over a decade, addressing the increased risks posed by advancements in technology and the rise in cyberattacks targeting healthcare data. While the American Medical Informatics Association (AMIA) acknowledges the critical need to safeguard electronic protected health information (ePHI), we want to emphasize the necessity of addressing key challenges to ensure the proposed regulations are both effective and feasible for implementation.

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.

Under AMIA's Public Policy Principle on Health Information Technology (HIT) Safety[1], we emphasize that ensuring the safe and effective use of HIT is a shared responsibility. Oversight bodies (both governmental and nongovernmental) along with developers, implementers, healthcare organizations, health systems, clinical practices, users, and patients all play a critical role in maintaining HIT safety. As a leading organization in health informatics, AMIA recognizes that HIT and the practice of clinical informatics are essential for advancing medical interventions, reducing errors, improving patient safety, and supporting learning healthcare systems. However, we also acknowledge that HIT can introduce new risks, unintended consequences, and operational burdens that must be addressed to uphold patient safety.

To maximize the benefits of HIT while minimizing risks, it is imperative to identify and mitigate safety concerns in a coordinated, collaborative, and non-punitive manner at both the local/organizational and national/systems levels. A highly functional HIT ecosystem depends on a structured approach to recognizing and addressing potential hazards. Additionally, fostering an environment where information about HIT-related harm—whether caused by technology, human factors, or operational processes—is openly shared is crucial for continuous system improvement. Safe and supervised spaces must be established to facilitate discussions on HIT-related harm, allowing stakeholders to learn from past experiences and enhance patient and clinician safety. Through collaboration, transparency, and proactive risk management, AMIA remains committed to ensuring that HIT fulfills its potential as a transformative force in healthcare.

Key Proposals and Recommendations

Enhanced Encryption and Access Controls

The proposed regulations require enhanced encryption and access controls, including mandatory data encryption and multifactor authentication (MFA) to protect electronic ePHI from unauthorized access. Additionally, organizations must maintain detailed logs and reports on encryption measures, MFA implementation, and access control enforcement for review. However, legacy HIT and medical device systems, which remain prevalent—reported by 73% of healthcare cybersecurity professionals in a 2021 survey[2]—may not

[1] AMIA PUBLIC POLICY PRINCIPLES AND POLICY POSITIONS 2024-2029 Priorities, Pg. 9, https://brand.amia.org/m/11e36a0494d4bc9a/original/AMIA-Public-Policy-Principles-2024-Final.pdf

[2] "2021 HIMSS Healthcare Cybersecurity Survey," Healthcare Information and Management Systems Society, p. 18 (Jan. 28, 2022), *https://www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf*.

support modern encryption, leading to costly upgrades or replacements. Furthermore, encryption can introduce interoperability challenges with third-party partners, such as billing and laboratory services, potentially disrupting critical healthcare operations. To mitigate these challenges, it is recommended that encryption standards be tailored to specific use cases, guidance be provided for legacy systems, and exceptions or compensating controls be made available for the more complex workflows.

Staffing

The proposed regulations would necessitate increased staffing to meet compliance requirements, posing significant challenges for healthcare organizations. Implementing new technical solutions and processes, such as maintaining asset inventories, conducting risk assessments, and obtaining certifications, will require additional personnel. The healthcare industry faces a well-documented shortage of cybersecurity professionals, making recruitment difficult. Additionally, existing staff may require extensive training to understand and implement the new requirements, further straining resources. The increased workload and compliance pressures could also contribute to staff burnout and higher turnover rates. To address these challenges, it is recommended that funding or incentives be provided to support workforce development and retention in health care cybersecurity.

Compliance Timeline

The proposed 180-day compliance timeline presents significant challenges due to various operational and logistical constraints. Organizations may experience procurement delays as they navigate lengthy purchasing processes or vendor backlogs, hindering their ability to acquire necessary tools and solutions. Additionally, many vendors may not be fully prepared to meet the new compliance requirements within the designated timeframe, leading to further setbacks. Healthcare providers also face numerous competing priorities, balancing regulatory and operational demands that make simultaneous compliance particularly difficult. Moreover, recruiting and onboarding qualified personnel to implement and maintain new cybersecurity measures is a time-intensive process, further complicating timely compliance. To address these challenges, a tiered compliance timeline should be implemented based on an organization's size and complexity, with extensions granted for procurement or vendor-related delays. Additionally, organizations

should be allowed to prioritize initiatives based on risk assessments, enabling them to develop a realistic and achievable compliance roadmap.

Cost Estimates

While the proposed modifications to the HIPAA Security Rule are presented as maintaining most of the existing obligations for regulated entities, the Office for Civil Rights (OCR) simultaneously estimates that compliance with the new rule will result in first-year costs of approximately $9 billion, with ongoing annual costs of $6.8 billion years two through five.

These changes will demand a significant investment of time, resources, and effort from most HIPAA-regulated entities. OCR's cost and effort projections are based on the assumption that the majority of regulated entities are already compliant with the current Security Rule. However, this assumption does not reflect the actual state of compliance. The proposed rule itself acknowledges that, during an audit of regulated entities against the current Security Rule, OCR found that 94% failed to implement appropriate risk management activities sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. This finding indicates that most entities still have considerable work to do to meet existing Security Rule requirements. AMIA supports the critical need to address the proposals but concerned about the additional burden of achieving compliance with the proposed updates for regulated entities.

Impact on Documentation Burden

The proposed HIPAA Security Rule update introduces additional documentation requirements, significantly increasing the administrative burden on healthcare entities. Organizations must maintain a technology asset inventory and network mapping, ensuring detailed, written records of all technology assets affecting ePHI while keeping an up-to-date network map that requires continuous tracking and updates. Regular security audits and testing add to the workload, as entities must document annual audits, security measure reviews, biannual vulnerability scans, and annual penetration tests to demonstrate compliance. Additionally, incident response and risk management plans must be documented, regularly updated, and retained, further increasing reporting requirements. Compliance with encryption and access control measures demands that organizations maintain detailed logs and reports on encryption implementation, MFA, and access control enforcement, all of which must be readily available for review.

These requirements have a significant impact on health informatics, leading to an increased administrative workload for IT and compliance teams as they track, update, and report security measures. Many organizations may need to invest in automation solutions to streamline compliance reporting and reduce manual documentation tasks. Additionally, training and resource allocation will be necessary to ensure health informatics professionals can effectively manage these expanded compliance obligations. While these measures enhance cybersecurity, they also introduce greater documentation responsibilities, requiring organizations to adopt improved record-keeping strategies and compliance automation tools to meet the new regulatory demands efficiently.

Overarching Recommendation

We respectfully urge the Agency to consider establishing a framework that prioritizes and aligns with the highest-risk areas, ensuring a more targeted and effective regulatory strategy to meet the approach outlined in the Proposed Rule.

Thank you for your time and consideration of these comments. If you have questions or require additional information, please contact Tayler Williams, AMIA's Senior Manager of Public Policy, at twilliams@amia.org.

Sincerely,

Eileen Koski

Eileen Koski Chair of the Public Policy Committee