1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

March 7, 2025

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

RE: RIN 0945-AA22/HHS-OCR-0945-AA22

Dear Acting Director Archeval:

The Consumer Technology Association (CTA®) appreciates the opportunity to comment on the proposed HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information.

As North America's largest technology trade association, CTA is the tech sector. Our members are the world's leading innovators – from startups to global brands helping support more than 18 million American jobs. CTA owns and produces CES® – the most powerful tech event in the world. CTA is the trade association representing more than 1200 companies in the U.S. technology industry. Eighty percent of CTA companies are small businesses and startups; others are among the world's best-known brands. We provide members with policy advocacy, market research, technical education and standards development.

CTA's Health Division drives the adoption of consumer-based, technology-enabled health solutions to improve health outcomes and reduce overall health care costs. Comprised of innovative small and large companies across the healthcare and technology sectors – including telehealth providers, personal health wearable companies, health care payers, health systems, and biopharmaceutical innovators – the Division offers policy advocacy, market research, and standards initiatives to promote the effective use of consumer technologies in health care.

General Comments

CTA appreciates the focus of HHS on protecting consumers' electronic protected health information. We believe federal privacy laws are essential for fostering innovation while ensuring consistent consumer protection. With the rapid advancements in technology and healthcare infrastructure, CTA understands the need to strengthen cybersecurity safeguards in response to the dramatic increase in healthcare cybersecurity risks. Mandating compliance with federal cybersecurity initiatives is crucial, as ransomware and hacking breaches not only compromise patient safety and disrupt medical care but also erode trust in healthcare systems.

We have concerns, however, about the proposed rule's prescriptive nature that will pose undue burdens to companies.

For example, the proposed rule requires regulated entities to establish written procedures for restoring certain relevant electronic information systems and data within 72 hours, perform a criticality analysis to prioritize system restoration, and create documented security incident response plans that outline how

workforce members should report and respond to security incidents. While CTA recognizes the importance of efficient incident response, these requirements are inflexible and unnecessarily burdensome. Indeed, the rule's language is ambiguous about what would qualify as a reportable incident, particularly what would be considered an "attempted" unauthorized interference. If the administration intends for the proposed rule to become final, we recommend refining the definition of a "Security Incident" to exclude unsuccessful attempts, as they typically indicate that security controls are functioning properly, and recording every failed attempt would be unmanageable, particularly for business associates handling large volumes of interactions.

We outline other concerns we have with the rule below.

Safeguards

The proposed rule would require onerous new workstreams for covered entities and an inordinate amount of oversight of business associates, rising to the level of asking covered entities to behave like a cybersecurity firm – auditing and overseeing its own and vendors' technology. For example, the proposed rule would mandate the creation and maintenance of an accurate technology asset inventory and network map. Tracking every piece of technology, including mobile devices and workstations, would be burdensome, especially for larger organizations with constantly changing assets. A more practical approach would be to focus on systems that store or affect ePHI, rather than attempting to catalog every individual device.

Additionally, the proposal's requirement for annual updates to the inventory and network map, along with the new mandate for data flow diagrams, creates unnecessary duplication with existing audit processes, such as AICPA Trust Services Criteria (SOC audits), which already verify similar information. The NPRM's proposed cascading verification requirements across business associates and their subcontractors would impose a bureaucratic compliance framework that diverts attention from actual security efforts. This focus on paperwork, including obtaining written verifications and certifications, could become costly and counterproductive, as it does not necessarily improve the security posture of the entities involved.

Furthermore, the NPRM eliminates the flexibility of a risk-based approach that currently allows for compensating controls when a specific safeguard may not be in place. This reduction in flexibility, coupled with the onerous verification requirements, could result in non-traditional entities exiting the market and thus hinder innovation. A more flexible, scalable approach is needed to ensure that the regulations are both effective and practical without imposing undue burdens.

Operational Feasibility

CTA urges HHS to continue to allow for a flexible and scalable approach to HIPAA regulation, as the proposed rule threatens to impose burdensome requirements that do not account for the varying risks and needs of different entities.

While the NPRM aligns the HIPAA framework with best security practices, it introduces overly prescriptive measures that eliminate the flexibility necessary for effective risk management. The rigid demands for data flow diagrams and asset management would create significant challenges for providers, potentially hindering their ability to address cybersecurity risks effectively. Additionally, the one-size-fits-all approach fails to recognize the differing levels of risk based on an entity's engagement with ePHI, such as entities that conduct forensics versus those that continuously manage ePHI. Maintaining flexibility, as previously emphasized by OCR, would allow entities to implement safeguards in a way that is reasonable and appropriate for their specific environments, consistent with the objectives of reducing administrative costs and ensuring effective security measures without unnecessary burdens. A risk-based approach would better support the diverse needs of the healthcare sector while still upholding the overarching goals of HIPAA.

As we noted earlier, CTA supports ensuring security safeguards are implemented when reasonable and appropriate as applied to a specific regulated entity's environment under a risk-based approach. Instead, the NPRM proposes safeguards that are universally reasonable and necessary instead of safeguards based on a regulated entity's informed security professionals based on their unique environment. This leads to an extraordinary, inherently unnecessary cost burden that will lead to increased costs of health care services. Instead, HHS should recognize that business associates, as agents of covered entities, will be responsible as a matter of contract to implement safeguards under an informed, risk-based approach. Overall, the NPRM's proposed addition of specific timeframes for required activities is problematic and may be cost-prohibitive for regulated entities, particularly in areas like data segmentation, where the cost to come into compliance is high.

Transition Provisions

The proposed transition period for revising business associate agreements (BAAs) or other written arrangements under §164.318 is inadequate and imposes significant administrative burdens on regulated entities. The proposed rule anticipates covered entities completing this process within a year. This time period is not feasible given the quantity of vendors and it also ignores the regular contracting process. We recommend extending the transition period to provide more flexibility, allowing entities to update their BAAs as part of their regular business cycles, rather than mandating amendments within a rigid one-year timeframe. Additionally, since all BAAs already include "compliance with laws" provisions, these agreements should be allowed to remain in effect for a reasonable period, with updates made during contract renewals or through standard business cycles. Requiring such amendments within one year is both unrealistic and unnecessary, as the "compliance with laws" provision already ensures adherence to evolving legal requirements**.**

Workforce Requirements

CTA encourages HHS to reconsider the 24-hour notification requirement for changes or terminations of workforce members' access to ePHI or electronic information systems. While we understand the intent to enhance security, the 24-hour timeframe presents challenges from an operational perspective, particularly given the variability in termination processes across organizations. The reliance on timely HR system updates to trigger automation, along with the use of system reports in some entities, makes it difficult to consistently meet this strict timeline. Furthermore, the requirement could result in frequent notifications for minor changes, such as new hires or role reassignments, without providing significant security benefits. We suggest HHS engage with industry groups to develop clearer guidelines and best practices, such as notifying security teams of terminations, to ensure a practical and effective approach to ePHI access management. Additionally, considering that SOC2 audits already include workforce termination requirements, there may be opportunities to align these regulations with existing industry standards.

Further, the proposed requirements under § 164.308(a)(5)(i) to apply sanctions against workforce members who fail to comply with security requirements would require entities to rely on asset inventories and network diagrams to identify where ePHI is stored, processed, and transmitted. Given the scope of these requirements, meeting them annually would necessitate significant program redesign and resource allocation across the organization. While the Department has highlighted failures in implementing a risk-based approach, the conclusion that safeguards must always be implemented—regardless of whether they are reasonable and appropriate in a specific environment—could impose an undue financial burden on market participants, contradicting the intent of Congress and the flexibility intended by the Security Rule.

CTA urges HHS to work with industry and accredited standards development organizations to develop best practices for appropriate, feasible standards for workplace/employer compliance with HIPAA regulations.

Conclusion

CTA appreciates the opportunity to comment on the proposed HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information. We look forward to continuing to work with HHS to achieve our shared goal of protecting patient health information.

Sincerely,

Michael Petricone
Senior Vice President, Government Affairs
Consumer Technology Association

René Quashie
Vice President, Digital Health
Consumer Technology Association