March 7, 2025

Robert F. Kennedy, Jr., JD
Secretary
U.S. Department of Health and Human Services
Hubert H. Humphrey Building
200 Independence Avenue, S.W.
Washington, D.C. 20201

RE: RIN 0945-AA22 — HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information

Dear Secretary Kennedy,

The American Academy of Nursing (Academy) is pleased to offer the following comments in response to the January 6, 2025, proposed rule to modify the Security Standards for the Protection of Electronic Protected Health Information (Security Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). With more than 3,200 Fellows, the Academy—an honorific society and policy organization—represents nursing's most accomplished leaders in policy, research, administration, practice, and academia. Collectively with our Fellows and partners, the Academy aims to create solutions that matter, inspire change that propels transformation, and envision a healthier future. Through intentional actions the Academy advances its vision of *Healthy Lives for All People*.

The Academy applauds the Department of Health & Human Services' (HHS) actions to strengthen cybersecurity and ensure protections for the confidentiality, integrity, and availability of electronic protected health information (ePHI). The Academy supports the proposed updates to the Security Rule and we believe they will support these key objectives. However, as HHS updates security guidelines to align with new and emerging technologies, we encourage HHS to maintain an overarching focus on supporting productive and sustainable patient care workflows. Cybersecurity is a critical priority for health systems. However, the overall delivery of care is influenced by many complex factors with which security measures must be balanced to avoid unintentionally impeding achievable, effective, efficient, and fair workflows. As HHS considers preparing a final rule, the Academy offers the following comments on areas to consider and clarify in the section *New and Emerging Technologies*, in alignment with the questions HHS has outlined.

Whether the Department's understanding of how the Security Rule applies to new technologies involving ePHI is not comprehensive and if so, what issues should also be considered.

Overall, the Academy believes that the proposed changes to the Security Rule would strengthen its application to new technologies for increased cybersecurity while remaining technology neutral. We

support the additional requirements for risk assessments to be comprehensive and in writing; requiring entities to keep a written inventory of their technology assets; and requiring entities to monitor authoritative sources for known vulnerabilities in their technology to remediate them. However, we encourage HHS to consider entities' ability to implement these requirements as technologies, particularly artificial intelligence (AI) technologies, evolve rapidly. For an inventory of assets, for example, entities may not be aware of the full extent of the technologies they possess or where the data is processed and stored, as some technologies may inform only the back end of an AI functionality that would be listed. Addressing this aspect with technology vendors by establishing or strengthening base criteria for software and other technologies used in the health care setting may be a key step in facilitating compliance with this aspect of the rule.

Whether there are technologies that currently or in the future may harm the security and privacy of ePHI in ways that the Security Rule could not mitigate without modification, and if so, what modifications would be required.

The Academy highlights that care delivery is rapidly advancing in an increasingly technological world. Given this, it will be important for HHS to consider adding language that encompasses areas where care is provided beyond traditional settings. For example, as technology evolves to encompass care delivery models such as the hospital-at-home model, language could be added that would define the home as a site of care. If a home was considered a site of care, this oversight and guidance would be crucial because technological infrastructure and security measures may be more difficult to manage in a home care setting.

Additional areas to explore in the rule include the impact of ambient intelligence technologies and wearable devices on security. Ambient intelligence technologies used in care delivery include sensors and processors that capture data on individuals beyond just the patient. With wearable devices, the data transmitted and uploaded from the patient may not necessarily be encrypted when it is sent to their provider. Both of these are areas to be considered. In the space of virtual reality (VR) and augmented reality (AR), we appreciate HHS's consideration of applying the Security Rule and agree that the proposed modifications are necessary to promote security as these technologies grow within health care.

Whether there are additional policy or technical tools that the Department may use to address the security of ePHI in new technologies.

As noted above, the Academy encourages HHS to consider implementing or strengthening baseline criteria for vendors of AI technologies to help entities more effectively account for the technologies in their inventory, promoting compliance with the rule. Furthermore, we recognize that HHS has carefully considered the impact of the proposed changes on small and rural health care entities and has declined to propose exceptions or alternate actions such entities could take. While we support the rationale and agree that gaps in security protections should be minimized, we recommend HHS consider additional

measures to support small and rural health care entities' ability to comply with the rule. This could include financial support or additional information to serve as resources. Additionally, we note that the risk of reidentification of patient data presents a significant challenge for entities. Greater understanding of how to protect against the risk of data reidentification would help entities address the security of ePHI in new technologies.

Finally, we underscore that continuing education on cybersecurity for clinicians and caregivers is key to the success of the Security Rule. While the existing rule speaks to the implementation of authorization, supervision, and sanction procedures for staff who work with ePHI, we encourage HHS to more broadly consider the need for proper education and protection for clinicians and caregivers working or interacting with ePHI. As an overarching recommendation, we suggest that HHS consider implementing a formal HIPAA advisory committee to guide efforts on cybersecurity. Nurses, with key expertise on patient safety, data, and technology, could play a critical role on this advisory committee.

The Academy appreciates the opportunity to provide comments in response to the *HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information* proposed rule. The Academy stands ready to work with you to provide expertise and shape policy solutions that champion health and well-being. If you have any questions or need additional information, please feel free to contact the Academy's Chief Policy Officer, Christine Murphy, at cmurphy@aannet.org.

Sincerely,

Linda D. Scott, PhD, RN, NEA-BC, FADLN, FNAP, FAAN
President, American Academy of Nursing