ASHA 1925–2025
Legacy. Impact. Possibilities.

March 7, 2025

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HIPAA Security Rule NPRM
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue SW
Washington, DC 20201

To Whom It May Concern:

On behalf of the American Speech-Language-Hearing Association (ASHA), I write to comment on the notice of proposed rulemaking modifying 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).

ASHA is the national professional, scientific, and credentialing association for 241,000 members, certificate holders, and affiliates who are audiologists; speech-language pathologists (SLPs); speech, language, and hearing scientists; audiology and speech-language pathology assistants; and students.

Audiologists and SLPs are communication specialists who work with individuals across the lifespan to maximize functional independence, safety, and the ability to fully participate in their lives. They are dedicated health care professionals working in a variety of settings including hospitals, rehabilitation facilities, private practices, and outpatient clinics. Audiologists specialize in preventing and assessing hearing and balance disorders as well as providing audiology treatment, including hearing aids. SLPs identify, assess, and treat speech, language, cognitive, and swallowing disorders.

Most ASHA members qualify as HIPAA covered entities and are very familiar with HIPAA and HITECH act requirements. In the course of treating their patients, audiologists and SLPs are entrusted with electronic protected health information (e-PHI) on a daily basis. Strengthening protections for this data is incredibly important, and our members know that intimately as they work to improve communication for all the patients they serve.

Though this rule is proposed with good intentions, in practice it will be extremely burdensome for many health care settings, especially small or solo practices, to implement. This is a challenge that even the Office of Civil Rights at the Health and Human Services Department (HHS OCR) acknowledges in the proposed rule itself. Many practices and work settings cannot afford employees solely dedicated to information technology (IT) or patient privacy alone. Because of the high administrative burden that these proposed changes would create, it would be near impossible for them to comply without a dedicated staff member to focus solely on implementing and monitoring the new standards this proposed rule would create.

Some of the most burdensome elements that ASHA identified in this proposed rule include:

- Requiring the development and maintenance of a written inventory and network map of the regulated IT's assets that process PHI, tracking how that ePHI travels through the practice, and keeping such resources updated annually;
- Requiring an enhanced Security Risk Analysis that must be done annually, including anticipating threats, assessment and documentation of security measures, assessment of risk level and determination of threat, and potential impact of each threat in relation to the vulnerabilities;
- Requiring new business associate agreements completed at least every 12 months with assurances including an analysis of how the business associate has or has not complied with the agreement and approval by someone with authority at the business associate; and
- Conducting vulnerability scans at least every six months, monitoring known vulnerabilities, and performing penetration tests at least once every 12 months.

We are concerned that—even in the standards which seem less burdensome—there is a lack of understanding about the very limited resources that most smaller health care practices and work settings have available to implement these new standards.

Therefore, ASHA respectfully requests that HHS OCR consider exemptions for small setting providers and only implement these proposed changes in larger settings (e.g., large hospital systems) that have the capacity to absorb the cost of implementing these standards. Larger settings also process a much larger volume of ePHI than small setting providers. In addition, please consider maintaining the addressable provisions for smaller settings with specific guidance that considers the different elements small practices face, which are unlike those of large hospital systems. If exemptions to the rule are not allowed, at a minimum, we ask that smaller covered entities to be afforded additional time to come into compliance.

We appreciate the opportunity to comment and urge you to consider that while all covered entities wish to protect e-PHI, not all entities can do that in the same way. Please reach out to Caroline Bergner, ASHA's director of health care policy for Medicaid, at cbergner@asha.org with any questions or concerns.

Sincerely,

A. B. Mayfield-Clarke, PhD, CCC-SLP
2025 ASHA President