The Honorable Brett Guthrie
Chairman
Energy & Commerce Committee
US House of Representatives
2161 Rayburn House Office Building
Washington, DC 20515

Vice Chairman John Joyce, MD
Vice Chairman
Energy & Commerce Committee
US House of Representatives
2102 Rayburn House Office Building
Washington, DC 20515

April 7, 2025

RE: Response to Privacy Working Group Request for Information

Submitted via email to PrivacyWorkingGroup@mail.house.gov

Dear Chairman Guthrie and Vice Chairman Joyce,

Thank you for the opportunity to provide feedback on data privacy and security. The increase in ways to share data, specifically health data, both within and beyond traditional healthcare settings, and the expansion of wearable devices, smart devices, and health and wellness apps have made protecting the privacy and integrity of data more complex and more important than ever.

AHIMA is a global nonprofit association of health information (HI) professionals. AHIMA represents professionals who work with health data for more than one billion patient visits each year. 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. Our leaders work at the intersection of healthcare, technology, and business, and are found in data integrity and information privacy job functions worldwide.

We appreciate the commitment to addressing challenges associated with building a framework to address the current state of data privacy and security. AHIMA is pleased to provide perspectives and expertise on health data and is supportive of the current framework in place to protect information covered by the Health Insurance Portability and Accountability Act (HIPAA). Regulatory changes are needed however to address health data held by entities that are currently not covered by HIPAA. Federal privacy and security baseline standards should be developed for the protection of health information held by data holders[1] outside of the scope of HIPAA. AHIMA offers the following feedback in response to the Request for Information.

II. Personal Information, Transparency, and Consumer Rights

Please describe the appropriate scope of such a law, including definitions of "personal information" and "sensitive personal information."

[1] The National Committee for Vital and Health Statistics (NCVHS) defines a "data holder" as "an inclusive term referring to entities that design and maintain proprietary databases and algorithms, sell data products, or design and build apps and devices that capture, transmit or use health data."

AHIMA suggests that for purposes of protecting consumer health data, the term "health information" should be construed as "electronic health information" as defined at 45 CFR 171.102.[2] "Electronic health information" as defined is broadly understood by the healthcare community as know what types of health data it encompasses while at the same time flexible enough to include future types of health data yet to be contemplated by stakeholders.

What disclosures should consumers be provided with regard to the collection, processing, and transfer of their personal information and sensitive personal information?

Any federal policy and security framework should enhance communication and transparency around health information. Policies must ensure data holders communicate to consumers what information will be collected and maintained and generally how the data may be processed and disclosed, including whether data will be sold or commercialized. This information should be provided to individuals in language consistent with an eighth grade reading level to ensure appropriate comprehension of the disclosures by individuals.

Please identify consumer protections that should be included in a comprehensive data privacy and security law. What considerations are relevant to how consumers enforce these protections and how businesses comply with related requirements?

What heightened protections should attach to the collection, processing, and transfer of sensitive personal information?

The sensitivity of consumer health information should be subject to the highest protections within a federal privacy and security framework. AHIMA believes that a federal framework must:

- **Guarantee individuals' access to their health information**. Policy must guarantee that individuals have access to their health information regardless of where it travels.
- **Improve accountability**. Policy must ensure that data holders develop, document, communicate, assign, and are held accountable for their privacy policies and procedures.
- **Limit the collection, use, and disclosure of health information**. Policy must ensure data holders limit the amount of health information collected, used, and disclosed to the minimum necessary.
- **Ensure the accuracy and integrity of health information**. Policy approaches must encourage the completeness, accuracy, and integrity of health information.
- **Prioritize the protection of health information against various privacy and security risks**, including breaches and unauthorized disclosures.
- **Address health information retention concerns**. Policy should safeguard that health information is retained no longer than necessary by data holders.
- **Facilitate disposition and destruction of health information**. Policy should facilitate the proper disposition and destruction of health information.
- **Assign appropriate oversight and enforcement responsibilities**. Policy must designate and adequately fund oversight and enforcement responsibilities.

[2] "Electronic health information" means electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in the designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity. EHI does not include psychotherapy notes (as defined in 45 CFR 164.501) or information compiled in reasonable anticipation of, or for use in a civil, criminal or administrative action or proceeding.

III. Existing Privacy Frameworks and Protections

Please provide any insights learned from existing comprehensive data privacy and security laws that may be relevant to the working group's efforts, including these frameworks' efficacy at protecting consumers and impacts on both data-driven innovation and small businesses.

How should a federal comprehensive privacy law account for existing federal and state sectoral laws (e.g., HIPAA, FCRA, GLBA, COPPA)?

AHIMA believes a "floor" should be established at the federal level for privacy and security requirements for health data, whether it is held by HIPAA-covered or HIPAA-non covered entities. This will reduce confusion and uncertainty and improve compliance with privacy standards. Congress should also take into consideration the fact that varying federal statutes have different requirements around privacy which adds to complexity and compliance burden. For example, the current 42 CFR Part 2 and HIPAA often create additional administrative burden and confusions for entities trying to comply with both of these laws. AHIMA supports the existing HIPAA framework to protect the privacy of patients and consumers when health information is held by HIPAA-covered entities and business associates. Regarding the security of health information, the HIPAA Security Rule requirements are critical to ensuring the security of a covered entity and business associates, and its electronic protected health information (ePHI). However, these requirements are not adequately funded and the lack of flexibility in the number of compliance pathways poses barriers to compliance for smaller organizations. Without resources and assistance, covered entities may have no choice but to prioritize the requirements they are financially able to implement. AHIMA recommends Congress direct the US Department of Health and Human Services' (HHS) Office of Civil Rights (OCR) to provide funding, resources, guidance, and education for covered entities and business associates on how to best implement current and future HIPAA Security Rule requirements to reduce compliance burden. We also recommend OCR offer additional flexibilities to support for small, rural, and otherwise under-resourced entities.

V. Artificial Intelligence

The use of non-clinical artificial intelligence (AI) and machine learning (ML) in the management of health information has a direct impact on patient safety and privacy, including the accuracy and quality of data found in medical records. HI professionals have long used non-clinical tools to support clinical documentation. In a 2023 survey[3], AHIMA asked HI professionals about their use of the following non-clinical AI or ML technologies:

- autonomous coding
- computer assisted coding
- algorithms for patient matching
- AI risk adjustment
- healthcare utilization management
- administrative workflow assistance
- chatbots (such as ChatGPT)

Survey results found that highly automated tools such as autonomous coding had higher error rates than tools that required greater human intervention, such as computer assisted coding. With the long-term

[3] Available at: https://7932134.fs1.hubspotusercontent-na1.net/hubfs/7932134/Whitepapers/Workforce-AI%20Study%20Final.pdf.

impacts of AI/ ML tools unclear, continued investigation into the impacts and development of guidance and best practices is needed to ensure effective use and appropriate of funding. Additional research by government and external stakeholders is needed to further understand real-world experiences with AI/ ML tools, as well as downstream implications including: implementation challenges; barriers to adoption, impact on data quality, patient privacy, and patient safety; workflow impacts; governance; and impacts on HI workforce staffing needs.

VI. Accountability and Enforcement

Please identify the benefits and costs of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law.

Any federal privacy and security framework should involve the appropriate, fully-resourced federal agencies with the necessary expertise to investigate and enforce requirements related to both HIPAA covered entities and business associates, and non-HIPAA covered entities. AHIMA recommends ensuring there are adequate resource, funding, and staff within the Federal Trade Commission (FTC) and HHS OCR to ensure oversight of a federal privacy and security law to protect consumer health information. Further reduction in each agencies' funding levels could further erode the ability for either agency to implement a privacy and security framework.

AHIMA thanks Chairman Guthrie and Vice Chairman Joyce for their leadership around data privacy and security and the opportunity to provide feedback. We look forward to working with you to ensure a system that protects individuals' health information. Should you or your staff have any additional questions or comments, please contact Kate McFadyen, Senior Director, Government Affairs, at kate.mcfadyen@ahima.org or (202) 480-6058.

Sincerely,

Lauren Riplinger, JD
Chief Public Policy & Impact Officer
AHIMA