April 7, 2025

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
2161 Rayburn House Office Building
Washington, DC 20515

The Honorable John Joyce
Vice Chairman
Committee on Energy and Commerce
U.S. House of Representatives
2102 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Guthrie and Vice Chairman Joyce:

On behalf of the Association of American Medical Colleges[1] (AAMC), I write in response to your request for information (RFI) to explore a data privacy and security framework. Academic medicine plays a critical role in advancing patient care, biomedical research, and medical education, all of which rely on the secure and ethical management of health information. We appreciate your attention to this matter and look forward to working with you as you develop this important framework.

The AAMC and its members share your commitment to the responsible collection, use, and protection of personal data. Academic health systems, teaching hospitals, and faculty physician practices have long been at the forefront of leveraging health information technology (IT) to improve patient access, enhance research, and deliver high-quality care for all patients. Our members have made significant investments in electronic health record systems (EHRs), expanded telehealth capabilities, and implemented innovative technologies to support the delivery of high-quality health care. Academic health systems are committed to ensuring the privacy and security of their information systems and the protected health information (PHI) and other personal data these systems produce. Our members operate and comply with stringent federal and state regulations, while continuing to evolve to meet new challenges.

As the data security working group develops a federal privacy and security framework, we urge you to recognize the unique role of academic medicine and ensure that any new regulation aligns with existing health care privacy laws, supports cutting-edge research, and facilitates the delivery of high-quality patient care. The AAMC looks forward to engaging in this process, and offers the following answers to your RFI:

[1] The AAMC is a nonprofit association dedicated to improving the health of people everywhere through medical education, health care, biomedical research, and community collaborations. Its members are all 160 U.S. medical schools accredited by the Liaison Committee on Medical Education; 12 accredited Canadian medical schools; nearly 500 academic health systems and teaching hospitals, including Department of Veterans Affairs medical centers; and more than 70 academic societies. Through these institutions and organizations, the AAMC leads and serves America's medical schools, academic health systems and teaching hospitals, and the millions of individuals across academic medicine, including more than 210,000 full-time faculty members, 99,000 medical students, 162,000 resident physicians, and 60,000 graduate students and postdoctoral researchers in the biomedical sciences. Through the Alliance of Academic Health Centers International, AAMC membership reaches more than 60 international academic health centers throughout five regional offices across the globe.

**I. Roles and Responsibilities**

*How can a federal comprehensive data privacy and security law account for different roles in the digital economy (e.g., controllers, processors, and third parties) in a way that effectively protects consumers?*

The AAMC believes that a federal comprehensive data privacy and security law can best account for different roles in the digital economy if the law has a risk-stratified, scalable approach to protecting consumers' personal information. Requirements under the data privacy and security law should provide regulated entities with flexibility based on whether a requirement is reasonable and appropriate given the regulated entity's environment and risk profile. This approach would allow a small entity, for example, to determine that a costly mitigation is not warranted by the entity's risk analysis and risk mitigation strategy and thus is not reasonable and appropriate. This flexibility is critical to account for the wide range of regulated entity types that may be subject to the provisions of comprehensive privacy and security law. Roles should be defined with this flexibility in mind, recognizing that controllers may act as independent or joint controllers to each other as well as controllers that have processors act on their behalf. Regulated entities should be able to institute risk-based approaches so that any privacy and security measures are tied to the results of their risk analysis.

*Should a comprehensive data privacy and security law take into consideration an entity's size, and any accompanying protections, exclusions, or obligations?*

Yes, a comprehensive data privacy and security law should recognize the differences in types of entities and defer to the risk analysis of the regulated entities in determining which measures are most appropriate to apply to that particular entity. However, there should be a baseline agreed-upon floor that is a minimum viable standard applicable to all entities for sensitive personal information.

Currently, state consumer privacy laws tend to include an exception for non-profits, which is likely simpler to implement at the federal level. For those states that do not have such an exception, the law only applies if a certain threshold is met; this model is based on personal records of its state residents. If following the threshold level for a federal law, the threshold would need to be scaled to the full population, and as such, we recommend no less than 5 million personal records.

**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."*

"Personal information" should include any information that is linked or reasonably linkable to an identified or identifiable natural person and should not include de-identified data. Not all personal information is sensitive and could relate to identifiable information that is of public nature or would have less severe financial or reputational harm to an individual if exposed and thus should not require as stringent protections as those for sensitive personal information. A privacy law should permit the free flow of de-identified information and ensure the applicable legal definition of "de-identified information" which mirrors the HIPAA definition of de-identified information, as HIPAA's standard has been recognized as a "gold standard."

"Sensitive personal information" should mean personal information that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of sensitive personal information include Social Security numbers,

credit card and banking information, and health information. A privacy law should require stricter requirements on regulated actors to protect sensitive personal information.

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

Consumers should have a right to know about the personal information a regulated entity collects about them, and how it is used and sold or shared. To exercise this right, individuals should be able to request that a regulated entity that collects personal information about the individual disclose to the individual certain details about the personal information collected by the regulated entity, and how the regulated entity uses the information it collects. Individuals should be able to request from a regulated entity disclosures of what personal information is sold or shared and to whom. Additionally, individuals should have the right to direct a regulated entity that sells or shares personal information about the individual to third parties not to sell or share the individual's personal information (an "opt-out" right), subject to reasonable exceptions that are disclosed at the time of collection.

*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?*

It is essential to ensure that the data controller holds responsibility for the use, storage, and collection of personal information it collects, and that the use of personal information should be limited to what a reasonable consumer would expect is reasonably necessary in relation to the purpose for which the data is collected.

The controller should establish and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of the personal data as appropriate to the nature of the data at issue. Only the minimum amount of data needed for a given purpose should be collected. Individuals should have the right to obtain a copy of their personal data provided to the controller and should be able to opt out of the use of their personal data for advertising purposes or the sale of their personal data. Consumers should be provided with a privacy notice that explains how the data will be used and the consumer rights they can exercise regarding the use of their data. When required, consent should be obtained in advance. Reasonable security of the data should be required to protect it from theft, loss, misuse, or unauthorized disclosure.

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

Consumers should have a right to access, correct, delete, and obtain a copy of personal data, and to opt out of use of their personal data for the purposes of targeted advertising. Controllers should not process any sensitive data concerning a consumer without obtaining the consumer's prior consent.

**III. Existing Privacy Frameworks and Protections**

*Given the proliferation of state requirements, what is the appropriate degree of preemption that a federal comprehensive data privacy and security law should adopt?*

Consumers and entities benefit when there is certainty and consistency regarding privacy laws and protections. Navigating a confusing and inconsistent patchwork of state laws is extremely difficult. The myriad state requirements create confusion and inconsistencies that stifle innovation and increase

compliance burdens. Privacy frameworks should be consistent nationally so that providers, researchers, health plans, and others working across state lines may exchange information efficiently and effectively to provide treatment and advance research while limiting administrative burden. We recommend Congress adopt a federal privacy framework that fully preempts state laws related to data privacy and security, particularly those that are contrary to federal privacy laws unless a specific exception applies (for example reporting of abuse, disease, or injury). This is essential for data flow, economic development, and innovation.

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

Certain entities are already regulated by sector-specific federal privacy statutes and regulations, including financial service organizations, health services providers and vendors, education entities, and those that conduct research with human subjects. We recommend harmonizing privacy and security regulations to reduce administrative burden and ensure clarity for covered entities, business associates, and patients. For these entities currently regulated, there should be exemptions from federal data privacy law to ensure harmonization. Specifically, we recommend a carve-out from any comprehensive federal data privacy law for HIPAA-covered entities and their business associates (governed by the privacy, security and breach notification rules) when using PHI, any de-identified information (as defined by HIPAA), identifiable information collected as part of human subjects research (which is already subject to privacy board review and other protections for research participants), and information and documents created for purposes of the federal Health Care Quality Improvement Act, and information used for public health activities and purposes as authorized by HIPAA. Additionally, we recommend a carve-out for personal data from the higher education sector regulated by the federal Family Educational Rights and Privacy Act (FERPA).

There should also be an exemption for data of individuals employed by or who are independent contractors of a controller to the extent that data is collected and used within the context of their role or the extent that data is used to administer benefits or for contact purposes.

**IV. Data Security**

*How can such a law improve data security for consumers? What are appropriate requirements to place on regulated entities?*

Regulated entities are already following a patchwork of industry-accepted federal and state standards related to data security that has made compliance challenging and burdensome. For example, in cybersecurity, the Assistant Secretary for Technology Policy (ASTP)/Office of the National Coordinator for Health Information Technology (ONC) certification criteria for certified electronic health record technology (CEHRT) includes a privacy and security certification framework for health information technology modules. The Department of Health and Human Services has published voluntary health care sector-specific cybersecurity performance goals (CPGs) that are based on industry-accepted best practices and guidelines and are broken down into essential and enhanced goals. The National Institute of Standards and Technology (NIST) has issued a cybersecurity-specific framework with guidance on managing cybersecurity risks as well as guidance on protecting controlled unclassified information in nonfederal systems and organizations. This NIST guidance, NIST Technical Series Publication 800-171 (NIST SP 800-171), has been used by health care organizations, including providers, to develop procedures for protecting ePHI. Federal agencies have begun to adopt these standards in their own cybersecurity regulations, including the Department of Defense (DoD) and the National Institutes of Health (NIH). DoD has incorporated the requirements of Pub. 800-171 into its Cybersecurity Maturity

Model Certification Program, which governs the protection of sensitive information shared by DoD with its contractors and subcontractors. NIH updated its Genomic Data Sharing Policy to require that users of its genomic data ensure their IT systems comply with the NIST SP 800-171. Given the adoption of NIST SP 800-171 by other federal agencies and the adherence to these standards by private sector entities, there should be alignment by incorporating these standards into any new cybersecurity requirements, instead of developing new requirements that could conflict with these standards. Adopting these vetted standards would ensure consistency in cybersecurity practices by stakeholders across these critical infrastructure sectors.

**V. Artificial Intelligence**
*How should a federal comprehensive data privacy and security law account for state-level AI frameworks, including requirements related to automated decision-making?*

The AAMC believes that any federal comprehensive data privacy and security law must thoughtfully account for the evolving landscape of state-level AI frameworks, particularly those governing automated decision-making. AAMC members recognize that, while automated decision-making is often categorized as a privacy concern, the broader issue with AI lies in the unconsented and non-transparent use of individuals' data to train AI models. This concern is particularly acute in health care, where patient data requires the highest levels of protection.

The AAMC urges Congress to continue its efforts to develop legislation to establish clear parameters around AI-driven decision-making, including requirements for transparency, consent, and accountability. The rise of agentic AI, or AI systems that operate without direct human oversight, raises significant concerns about data security, potential re-identification of individuals, and unintended data leakage. AAMC members have expressed apprehension that once AI is implemented in health care settings, patients may unknowingly provide protected health information (PHI) to AI-driven systems, potentially leading to privacy breaches and regulatory challenges.

To mitigate these risks, the AAMC believes that federal legislation should include robust controls, such as requiring AI developers and vendors to implement strict guardrails around data usage. While we acknowledge that sufficient controls can mitigate risks associated with AI-driven decision-making, we must caution that our members' experience has shown the potential for unforeseen consequences, such as the emergence of web-tracking technologies, that were not initially well-regulated. Thus, the legislation must incorporate proactive safeguards that anticipate the evolving capabilities of AI.

One critical aspect of AI regulation is consent and transparency. The AAMC believes that patients should be clearly informed when they are interacting with AI rather than a human. Federal policy should require that AI systems disclose their nature and purpose, ensuring that patients and consumers can make informed choices. While we do not necessarily believe that consent alone is sufficient due to the complexity of AI systems and the challenges associated with conveying meaningful, comprehensive disclosures to patients, we believe that consent is a critical starting point for these conversations.

The AAMC and our members maintain rigorous data governance standards, and we believe that accountability is integral to any framework, and that it supports the overall goal of improving the health of patients as they interact with the health system. We continue to hear concerns from our members, however, that large technology companies operating in the AI space may not adhere to the same level of diligence. We urge you to ensure that any future legislative efforts do not sacrifice patient protections in AI development in the name of carve-outs for large technology companies' accountability. The AAMC believes that any federal privacy framework must ensure that health care-related AI applications are not exploited by technology vendors without appropriate oversight and governance.

To address these concerns, the AAMC urges Congress to establish clear enforcement mechanisms that hold AI vendors accountable for data privacy and security violations. Our members have raised concerns that contractual agreements with vendors often include provisions prohibiting the use of sensitive data for AI training, yet there is uncertainty about how compliance with these agreements is monitored and enforced. Therefore, the AAMC recommends that federal law include provisions that empower institutions to audit AI systems, implement ongoing monitoring mechanisms, and hold vendors accountable for compliance failures.

Finally, the AAMC supports a federal approach that harmonizes AI-related privacy regulations across states to prevent a fragmented regulatory landscape. While recognizing the need for flexibility to accommodate evolving AI technologies, the AAMC requests that a federal framework should provide consistent, enforceable standards that ensure patient privacy, enhance transparency, and safeguard the responsible use of AI in health care.

On behalf of America's medical schools, academic health systems and hospitals, and physician faculty, we thank you for your interest in exploring a comprehensive data security and privacy framework. If you have any questions, please contact me (dturnipseed@aamc.org) and Ally Perleoni, director of government relations (aperleoni@aamc.org).

Sincerely,

Danielle Turnipseed, JD, MHSA, MPP
Chief Public Policy Officer
Association of American Medical Colleges

CC: David Skorton, MD
President and CEO
Association of American Medical Colleges