INFORMATICS PROFESSIONALS. LEADING THE WAY.

The Honorable Brett Guthrie
Chair
House Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable John Joyce, M.D.
Vice Chair
House Committee on Energy and Commerce
U.S. House of Representatives
2102 Rayburn House Office Building
Washington, D.C. 20515

Re: Request for Information to Explore Data Privacy and Security Framework

Dear Chairman Guthrie and Vice Chairman Joyce,

Thank you for the opportunity to share our insight and suggestions through the Request for Information to explore data privacy and security framework.

The American Medical Informatics Association (AMIA) is the professional home for more than 5,500 informatics professionals, representing frontline clinicians, researchers, and public health experts who bring meaning to data, manage information, and generate new knowledge across the health and healthcare enterprise. As the voice of the nation's biomedical and health informatics professionals, AMIA plays a leading role in advancing health and wellness by moving basic research findings from bench to bedside, and evaluating interventions, innovations and public policy across settings and patient populations.

In this letter, we will explore several key areas essential for developing a comprehensive data privacy and security framework. We will begin by discussing the scope of the law and definitions, including what constitutes personal and sensitive personal information. Next, we will explore the necessary disclosures to consumers, ensuring transparency in data collection, processing, and transfer. We will then outline various consumer protections, such as the rights to access, correct, delete, and object to data processing. Additionally, we will address heightened protections for sensitive personal information, emphasizing the need for explicit consent and enhanced security measures. Lastly, AMIA adds considerations for artificial intelligence (AI) and its impact on data privacy.

All the information and AMIA's considerations are based on the *AMIA Public Policy Principles and Policy Positions*[1] and AMIA's policy brief, *AI in Healthcare: Touchstones for Responsible Use*[2].

II. Personal Information, Transparency, and Consumer Rights

A. Scope of the Law and Definitions The appropriate scope of a comprehensive data privacy and security law should include clear definitions of "personal information" and "sensitive personal information." Personal information generally refers to any data that can identify an individual, such as name, address, email, phone number, and social security number. Sensitive personal information includes data that requires higher protection due to its nature, such as health information, financial data, biometric data, and information about racial or ethnic origin, political opinions, religious beliefs, or sexual orientation.

B. Disclosures to Consumers

Consumers should be provided with clear and comprehensive disclosures regarding the collection, processing, and transfer of their personal information and sensitive personal information. These disclosures should include:

- The types of personal and sensitive information being collected.
- The purposes for which the information is being collected and processed.
- The third parties to whom the information may be transferred.
- The rights of consumers regarding their data, including access, correction, deletion, and objection to processing.

C. Consumer Protections A comprehensive data privacy and security law should include several consumer protections, such as:

- The right to be informed about data collection and processing activities.
- The right to access personal data held by organizations.
- The right to correct inaccurate or incomplete data.
- The right to delete personal data under certain conditions.
- The right to restrict or object to data processing.

[1] AMIA PUBLIC POLICY PRINCIPLES AND POLICY POSITIONS 2024-2029 PRIORITIES
[2] AI in Healthcare: Touchstones for Responsible Use

- The right to data portability, allowing consumers to transfer their data to another service provider.
- The right to not be subject to automated decision-making, including profiling.

Considerations for enforcement and compliance include:

- Establishing clear guidelines and standards for data protection.
- Providing resources and support for businesses to comply with the law.
- Implementing regular audits and assessments to ensure compliance.
- Enforcing penalties for non-compliance to deter violations.

D. Heightened Protections for Sensitive Personal Information Sensitive personal information should be subject to heightened protections due to its nature. These protections may include:

- Explicit consent requirements for the collection and processing of sensitive data.
- Enhanced security measures to protect sensitive data from unauthorized access and breaches.
- Restrictions on the transfer of sensitive data to third parties without explicit consent.
- Regular reviews and updates to security protocols to address emerging threats.

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? A federal comprehensive data privacy and security law should account for state-level AI frameworks by harmonizing requirements related to automated decision-making and ensuring consistency across jurisdictions. This approach would help maintain U.S. leadership in AI while protecting consumer privacy and promoting ethical AI practices.

1. **Establish Baseline Standards**: Create minimum requirements for AI transparency, accountability, and ethical practices that states can build upon.
2. **Promote Interoperability**: Ensure that AI systems and regulations are compatible across states to facilitate innovation and compliance.

3. **Encourage Collaboration**: Foster partnerships between federal and state agencies, industry stakeholders, and academic institutions to develop and implement AI policies.

4. **Support Continuous Improvement**: Implement mechanisms for regular review and updates to AI regulations based on emerging technologies and best practices.

5. **Transparency and Accountability**: The federal law should mandate transparency in the planning, designing, developing, validating, deploying, monitoring, and maintaining AI tools. This is crucial to avoid unintended consequences and ensure that AI tools are used responsibly.

   It should also require structured accountability, where AI harm and unintended consequences are reported, assessed, monitored, measured, and mitigated as needed. This includes guaranteeing responses to complaints and redress.

6. **Privacy Protections**: The law must secure individual and population data by consistently maintaining privacy protections and respecting privacy preferences across clinical, research, community services, and commercial use of health data.

7. **Ethical Principles and FAIR Sources**: AI tools should be developed with ethical principles in mind, using data of the highest quality that adheres to Findable, Accessible, Interoperable, and Reusable (FAIR) principles.

8. **Protecting Vulnerable Populations**: Increased scrutiny and appropriate community involvement are necessary when applying AI to vulnerable populations to avoid worsening inequity in healthcare.

9. **Collaboration with Experts**: The federal law should encourage collaboration with clinical informaticians and leverage the expertise of organizations like AMIA, which have decades of real-world AI experience.

By integrating these elements, a federal comprehensive data privacy and security law can effectively address the challenges posed by AI while supporting U.S. leadership in the field.

***

Thank you for your time and consideration. We look forward to your feedback and are ready to assist further. If you have questions or require additional information, please contact Tayler Williams, AMIA's Senior Manager of Public Policy, twilliams@amia.org.