AHIP Chief Medical Officers: Roadmap for Protecting Americans' Privacy, Confidentiality, and Cybersecurity of Health Information and Data

February 2022

Everyone should feel safe and secure knowing that their personal health information is private and protected.

The AHIP Chief Medical Officers leadership team joins the AHIP Board of Directors in their shared commitment to core guiding priorities to protect patients' and consumers' privacy, confidentiality, and cybersecurity.

We are fully committed to advocating for standards and policies that improve health data governance, protect patient privacy, and foster trust, and that enhance consumer access to their data and promote interoperability, health equity, and fair practices for the people we serve.

Health insurance providers have been a leader in developing privacy, confidentiality, and cybersecurity practices to protect health information. And we are committed not just to keeping pace with new trends, developments, and solutions – but leading them.

These supportive priorities describe our current policy positions and the ways in which new legislation should evolve in the age of technology and health care innovation.

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act and corresponding regulations should remain the primary legal framework for protecting health information.

Building on these requirements, we support government policies that advance the following positions:

- **HIPAA or similar requirements should be expanded to entities that collect, use, disclose, or store individuals' health information but are not currently subject to the rigorous privacy or security parameters that our industry requires.**
    - Privacy requirements should be designed and applied across all entities maintaining health and health-related information to allow appropriate communication and sharing of information without reducing privacy protections.
    - Consumer notices should be transparent, readily available, and easy to understand.
    - Regulators should consider new strategies to ensure consumers review and agree to terms and conditions governing the use of their health care information.
    - Small businesses should be considered for certain accommodations from interoperability requirements to facilitate access to the industry without exorbitant start-up costs.

- Additional specifications should be publicly vetted before regulatory adoption to ensure they meet baseline requirements and expectations for protecting consumers' privacy and security.

- **Individuals should have access to their health data and be able to easily know how their health information may be shared.**
  - Consumers should be informed in a way that is clear, concise, and easy to understand about how to access their personal health information and how it could be used and disclosed.
  - Health insurance providers should seek new solutions to provide consumers with more options about how their information is shared.
  - Policies should support the ultimate goal of seeking specific authorization from individuals for the use of particularly sensitive data (e.g., DNA) and giving them the ability to delete information to the extent safe and practicable. For example, legislators and regulators should evaluate and modify existing record retention requirements to facilitate data deletion at a consumer's request. However, clinicians and other health care entities should be protected if they must rely on incomplete or unavailable data in these situations.
- **Privacy requirements governing private entities should support digital platforms and telehealth in a way that promotes the privacy and security of information exchanged.**
  - Privacy requirements should be responsive and evolve to better support digital solutions, addressing data collection, security, and storage requirements, as well as the cybersecurity risks of transmitting information real-time.
  - Consumer protection requirements that limit communication channels for health-related communications should be updated.
  - Government policies should support efforts by entities to develop consistent, secure mechanisms to share information with other entities and consumers to accommodate digital solutions but avoid delays or cybersecurity risks.
- **Privacy requirements should evolve to better support public health requirements.**
  - Privacy requirements, coupled with increased communication and coordination between entities, should allow data sharing and automated solutions to support public health authorities.
- **The commercial sale of identifiable health information should be prohibited without the agreement of the individual.**
  - Identifiable data cannot be sold under HIPAA. Digital tools not subject to HIPAA should be subject to similar robust privacy law ensuring a consumer's identifiable data cannot be sold without a consumer's knowledge beyond the initial "click box" terms and conditions.
- **The United States should have a national privacy and security approach for health information.**
  - A federal standard can help overcome and preempt a varied patchwork of state laws for a more cohesive approach. In the interim, state and federal coordination should continue to be a goal.

- States should be consulted for ways to work together with their federal and private sector partners.
- Coordination among states will promote consistent definition of health information and application of privacy requirements.
- We support federal initiatives to promote a national patient identifier where use of a patient identifier is necessary and possible.

- **Laws and regulations and resulting costs should be analyzed with any resulting benefits before new or changing administrative, technical, and physical policies or controls are implemented.**
  - Such an analysis will help ensure that new policies and controls are commensurate with consumers' needs and balance risks and benefits.
- **Government policies should recognize that, as an industry, health insurance providers have continued to invest in and adhere to strong cybersecurity practices and policies.**
  - Information sharing between public and private entities facing threats, attacks, or mitigation strategies should be allowed and encouraged.
  - Dialogue between industry partners should be encouraged to develop and promote best-in-industry protection for information.
  - Government policies should recognize that increased use and evolution of digital solutions, virtual health care, cloud storage, and information systems requires investment in cybersecurity to promote secure environments capable of supporting consumer needs and communication between entities.
- **Consumer data such as race, ethnicity, religion, sexual orientation, gender identity, and disability status should be used to reduce disparities and improve outcomes.**
  - Data should not be used to discriminate or to have adverse impacts on a person or community. Data should be used when needed to create equity.
  - Standard setting organizations should work with public and private entities to determine how best to collect data. Organizations should work to collect as little data as necessary to achieve the intended purpose. Any mandates regarding the collection of data should come only after standards are complete and clearly defined, including ways in which each entity that has access to the data should take steps to protect the privacy of that data.
  - Government entities should allow the use of demographic information to support the health of an individual, public health initiatives, and other purposes consistent with HIPAA - but only in compliance with these principles. Non-health data (e.g., location, buying preferences) should be protected just like identifiable health information when used in conjunction with or connected to identifiable data.

- **The Federal Trade Commission should work on guidance addressing these priorities to the extent they have authority and seek authority from Congress where needed.**

Americans deserve better access to personalized, actionable health care information to empower them to make more informed decisions. They should have the confidence of having that access in a way that protects their privacy, confidentiality, and security.

# # #