



Health Information Privacy Modernization: New Technologies

Modernizing privacy protections matters because patients increasingly rely on digital tools to manage their care. Their data often moves across multiple systems, and without clear policies patients may face barriers accessing their information or understanding how it is used.

The American Medical Informatics Association (AMIA) supports efforts to expand privacy protections beyond traditional healthcare entities. To ensure these protections work in practice, policymakers should align with interoperability policies and ensure requirements are implementable through certified health information technology.

The Health Information Privacy Reform Act (HIPRA) – S. 3097 – is an important step toward modernizing U.S. health privacy protections. The Health Insurance Portability and Accountability Act (HIPAA) established essential safeguards nearly 30 years ago, but today’s digital health environment includes electronic records, health apps, wearable devices, and other commercial platforms that aim to manage sensitive health information. ¹ **In advancing legislation on this important issue, AMIA recommends:**

1 Make Patient Access Rights Operational Through Health IT

- Establish a standardized, computable “health data set” that includes clinical, biomedical, and claims data.
- Ensure data is electronically accessible through certified health IT² using API-enabled view, download, and transmit functions.
- Maintain structured, machine-readable formats.³

Why it Matters?

Ensures patients can reliably access and share their health information across systems.

Potential Improvements?

Modernize HIPAA’s Designated Record Set definition to clarify accessible information and require electronic, computable access through certified health IT.

1. [AMIA](#) | 2018
2. [ONC](#) | 2026
3. [AMIA](#) | 2024

2

Ensure Consistent Access Rights Across All Data Holders

In extending privacy protections to consumer health apps and other commercial entities, policymakers should:

- Apply consistent timelines and formats for access requests.
- Enable secure electronic access across entity types, including APIs.

Why it Matters?

Patients should receive the same privacy access rights regardless of whether their data is held by a hospital, insurer, or digital health company. ⁴

3

Promote Transparency While Protecting Privacy

To align with transparency policies such as the 21st Century Cures Act, policymakers can:

- Encourage real-time clinical data sharing with the patient or user.
- Use program incentives to encourage timely electronic patient access.

Why it Matters?

Patients would gain clearer insight into their care while privacy protections remain strong.

4

Clarify Guardrails for Third-Party Data Access

Congress should:

- Require legal process for third-party disclosures without patient direction.
- Establish clear authorization standards for patient-directed disclosures.
- Set clear boundaries on data access so only the health information covered under HIPRA is shared, preventing unnecessary or excessive disclosure.

Why it Matters?

Protects patients from inappropriate, coercive requests while allowing responsible data sharing.

By aligning privacy modernization with interoperable technology standards, policymakers can strengthen patient trust, improve access to health information, and support a more transparent digital health system. **Work with the Health, Education, Labor, and Pensions (HELP) Committee to ensure people have control over their health and wellness data.**

4. [AMIA](#) | 2024

5. [AMIA](#) | 2024