HEALTH INNOVATION ALLIANCE

April 7, 2025

The Honorable Brett Guthrie
Chairman
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable John Joyce, M.D.
Vice Chairman
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Re: Privacy Working Group Request for Information

Submitted electronically

Dear Chairman Guthrie and Vice Chairman Joyce,

The Health Innovation Alliance (HIA) appreciates the opportunity to comment on your request for information on exploring the parameters of a federal comprehensive data privacy and security framework. HIA is a diverse coalition of patient advocates, healthcare providers, consumer organizations, employers, technology companies, and payers who support the commonsense use of data and technology to improve health outcomes and lower costs. We are actively engaged in the policy discussion on ensuring the privacy and security of health information, particularly as health information becomes more liquid. We urge you to ensure any privacy policies considered by Congress:

- Avoid duplicative regulation for entities engaged in health care; and
- Ensure that health information continues to flow to those who need it.

HIA has worked with Congress for over 15 years to advance the interoperability of health information. The 21st Century Cures Act, passed in 2016, is still being implemented by the Trump administration to advance the access, exchange, and use of health information. Our nation has made great advancements in health care interoperability, but we have a long way to go. In 2022, we released our Interoperability Workgroup Report recommending key actions Congress and the administration should take to help us achieve true interoperability.[1] Health care interoperability is a bipartisan issue, and HIA will continue to push for a functioning system of accessible, exchangeable, and usable information across the industry.

We have also recognized that health information interoperability requires privacy and security. In 2020, we released principles to guide Congress in the creation of a new health data and privacy framework.[2] We urge you to examine our principles and use them as guidance as you consider privacy reform. Any health data framework should have the following attributes:

1. Patient-Centric
2. Strong Privacy Protections

[1] *Available at* https://health-innovation.org/2022-5-11-healthcare-interoperability-report/
[2] *Available at* https://health-innovation.org/2020-3-9-health-innovation-alliance-calls-on-congress-to-adopt-new-health-data-and-privacy-framework/

3. Trusted and Secure
4. Transparent, Flexible, Consistent, and Sustainable
5. Interoperable
6. Consistent Protections Apply to the Data Regardless of Who Holds the Data
7. Enforcement Incents Better Privacy and Data Stewardship
8. Nationwide and Uniform

Existing Privacy Frameworks and Protections

Use of de-identified data is incredibly important to a functioning health care system. Consistency in de-identification standards is instrumental for compliance. When California was first considering the California Consumer Privacy Act, the law set its own definitions for de-identification that were inconsistent with those in HIPAA. This inconsistency could have resulted in a stoppage of medical research while compliance officers determined how to, or if they even could, comply with both requirements simultaneously. We urge you to use the existing de-identification standards in HIPAA (for HIPAA-covered health data) that are well understood and work to protect privacy. Creating duplicative regulation will result in burdensome and costly compliance and confusion – not just for vendors, but for consumers and patients as well. One potential solution could be creating an entity-level safe harbor when an organization is acting as a covered entity or business associate under HIPAA. Several states have experimented with this type of arrangement in order to avoid overlapping regulatory authority. The safe harbor could apply to the entire law – rather than just portions – to effectively mitigate scenarios where organizations would be required to comply with multiple laws covering the same general area.

Artificial Intelligence

As the Working Group's RFI notes, states have increasingly adopted AI-specific legislation with the goal of protecting patients, consumers, and their data. At the outset, we must note that whether or not a health IT solution incorporates AI, it is still subject to the privacy requirements and protections under existing federal laws like HIPAA and 42 C.F.R. Part 2. Any new legislation or regulation must balance robust consumer data protections while avoiding disrupting innovative solutions that can make the health care system more efficient. In addition, any new oversight should not be duplicative of the existing frameworks which HIPAA-covered entities are currently subject to and comply with to date.

While these state efforts are well-intentioned, they are resulting in a complicated patchwork of regulations that are difficult for AI developers and end users to navigate, and in some cases are harming innovation. A prime example is Colorado's Artificial Intelligence Act, which was enacted on May 17, 2024. Though the bill does not take effect until 2026, Colorado's Governor convened an Artificial Intelligence Impact Task Force to consider modifications to the framework to avoid adverse effects to health care innovators.[3] The Task Force delivered its final report in February 2025 which highlighted the numerous unintended consequences of the legislation.[4]

[3] https://leg.colorado.gov/committees/artificial-intelligence-impact-task-force/2024-regular-session
[4] https://leg.colorado.gov/sites/default/files/images/report_and_recommendations_0.pdf

HIA has worked extensively over the past year to develop resources around the use of artificial intelligence in health care, which included taking privacy protections into account. In July 2024, we released our Principles for the Use of Artificial Intelligence in Health Care and Life Sciences, which includes details on how AI must be compliant with existing regulatory requirements, including regulations around privacy.[5] In March 2025, we released our Use Cases for AI Tools to Improve Health Care, which outlines the need for a risk-based approach to AI regulation.[6] AI risks and benefits vary depending on a variety of factors, and a one-size-fits-all approach risks mitigating any benefits associated with deploying AI. We believe these resources will be useful as the Working Group considers what role federal data privacy legislation should play in an increasingly complicated landscape.

Our Work on Health Privacy

Due to the complexity of existing health care data privacy requirements, we have advocated for the creation of a commission that could make recommendations to Congress on this important issue. In the 117th Congress, we worked with Senator Cassidy's (R-LA) office on the Health Data Use and Privacy Commission Act to do just that.[7] More recently we have worked with Congress to ensure that legislation intended to increase the privacy of consumer data does not unintentionally stop the use of health data in areas like care delivery, licensing, and medical research.[8]

We worked directly with Energy & Commerce Committee in the 118th Congress on the American Privacy Rights Act (APRA).[9] The base text of that bill did not initially provide carve-outs for existing, protected uses of data in the health care sphere broadly. Had the bill become law, this would have resulted in critical processes that already have robust, proven patient data protections being ground to a halt as stakeholders attempted to comply with the requirements of the new framework. That is why we collaborated with Energy & Commerce staff to include carve-outs for clinical trials, patient safety, public health, and other areas in the bill, edits which were included in a modified version of the bill before its consideration at the scheduled full Committee markup on June 27, 2024.[10] As the Privacy Working Group considers a new comprehensive, federal data privacy framework, we urge you to avoid disrupting existing processes in the health care ecosystem where robust data protections are already standard and well-proven.

The National Conference of Insurance Legislators (NCOIL) adopted a resolution HIA drafted to ensure that state consumer privacy legislation include exemptions for health privacy laws that cover medical research,

---

[5] *Available at* https://health-innovation.org/wp-content/uploads/2024/07/Principles-for-the-Use-of-Artificial-Intelligence-in-Health-Care-and-Life-Sciences.pdf
[6] *Available at* https://health-innovation.org/wp-content/uploads/2025/03/HIA-AI-Use-Cases-Report-2025.pdf
[7] *Available at* https://www.congress.gov/bill/117th-congress/senate-bill/3620
[8] *See* https://health-innovation.org/2022-6-14-draft-privacy-bill-misses-the-mark-national-framework-is-needed-to-work-for-patients-not-enrich-trial-lawyers/ *and* https://health-innovation.org/2023-2-28-privacy-legislation-should-not-impede-advances-in-healthcare/
[9] *Available at* https://www.congress.gov/bill/118th-congress/house-bill/8818
[10] https://energycommerce.house.gov/posts/chair-rodgers-announces-full-committee-markup-of-11-bills

patient care delivery, and other aspects of health care that are already well regulated. Please examine this model resolution to ensure policies you consider do not impede the active use of health information to produce new treatments and cures, protect patients from harm, and ensure caregivers have accurate information to treat their patients.[11] We urge Congress to balance the advances made in health care interoperability, medical research, and care delivery with any proposals you consider to modernize privacy protections.

We appreciate the opportunity to comment on this RFI and look forward to working with the Working Group to ensure the privacy and security of health information is consistent, trusted, and reliable for patients and consumers.

Sincerely,

Brett Meeks
Executive Director

[11] *Available at* https://ncoil.org/wp-content/uploads/2023/07/NCOIL-Draft-Data-Privacy-Resolution-6-20-23.pdf