April 7, 2025

The Honorable Brett Guthrie
U.S. House of Representatives
Washington, D.C. 20515

The Honorable John Joyce
U.S. House of Representatives
Washington, D.C. 20515

RE: Response to Privacy Working Group's Request for Information

Dear Chairman Guthrie, Vice Chairman Joyce, and Members of the Data Privacy Working Group:

The Healthcare Leadership Council (HLC) and the Confidentiality Coalition appreciate the opportunity to respond to your Request for Information (RFI) to inform the Privacy Working Groups efforts to explore the parameters of a federal comprehensive data privacy and security framework. Our collective members prioritize efforts to provide clear digital protections for Americans while navigating the complex state and federal data privacy and security laws which often create conflicting legal requirements in the health sector. We are eager to collaborate with the Privacy Working Group to develop a path forward and bring consumer protections into the digital age while ensuring that the United States continues to lead in a globally competitive environment.

HLC is an association of CEOs and C-suite executives from all sectors of healthcare working to shape the future of the U.S. healthcare system. HLC is the exclusive forum for the nation's healthcare industry leaders to lead on major, sector-wide issues, generate innovative solutions to unleash private sector ingenuity, and advocate for policies to improve our nation's healthcare delivery system. Members of HLC – hospitals, academic health centers, health plans, pharmaceutical companies, medical device manufacturers, laboratories, biotech firms, health product distributors/ wholesalers, post-acute care providers, homecare providers, group purchasing organizations, and information technology companies – advocate for measures to increase the quality and efficiency of healthcare through a patient-centered approach.

The Confidentiality Coalition is a diverse alliance dedicated to balancing the protection of confidential health information with the need for efficient, interoperable systems that enhance healthcare delivery and clinical research. The Coalition's aim is to safeguard the privacy of healthcare consumers while improving the essential flow of information

necessary to deliver high-quality, timely, and effective care and facilitating the development of innovative medical interventions.

The HLC and the Confidentiality Coalition have long advocated for privacy frameworks that are consistent nationally and across sectors so that providers, health plans, and researchers working across state lines and with entities governed by other privacy frameworks may exchange information efficiently and effectively in order to provide treatment, extend coverage, and advance medical knowledge, whether through a national health information network, clinical research network, or another means of health information exchange. The timely and accurate flow of de-identified data is crucial to achieving the quality-improving benefits of national health information exchange while protecting individuals' privacy. Before responding to the RFI's specific questions, we offer general health sector background considerations including: context as to the existing privacy matrix; principles given the existing primary framework for data privacy and security in healthcare, and recommendations for harmonizing a federal comprehensive data privacy and security framework.

GENERAL HEALTH SECTOR BACKGROUND CONSIDERATIONS

Existing Privacy Matrix

Including the Health Insurance Portability and Accountability Act (HIPAA) statute and regulations. data privacy laws and standards are largely derived from fundamental principles originally published by the Organization for Economic Co-operation and Development (OECD). The OECD privacy principles, developed in the 1970's, are similar to the United States' Fair Information Practice Principles (FIPPs), which inform U.S. privacy statutes and regulations. The following chart lists OECD, FIPPs principles, and corresponding component(s) of HIPAA privacy and security rules.

OECD	FIPPs	HIPAA
Collection Limitation	Minimization	Minimization
Data Quality	Quality and Integrity	Data Quality/Integrity (Security Rule)
Purpose Specification	Purpose Specification	Permitted uses and Disclosures
Use Limitation	Use Limitation (with purpose specification)	Permitted uses and Disclosures
Security Safeguards	Security	Data Safeguards
Openness	Transparency	Notice of Privacy Practices
Individual Participation	Individual Participation	Right to Access and Amend

OECD	FIPPs	HIPAA
Accountability by Data Controller	Accountability by Data Controller	Accountability by Covered Entities and Business Associates
	Authority	Permitted to collect and use information for Treatment, Payment, and Operations
	Access and Amendment	Right to access and amend

The implementation of these principles is widely termed “privacy by design,” which has been the basis of FTC’s framework for evaluating privacy practices. Privacy by Design calls for proactive consideration of privacy policies, processes, and practices in data collection, use, and workflows. This is generally the approach adopted by U.S. entities that are required to meet privacy standards, including financial service organizations, health services providers and vendors, education entities, and medical research organizations.

For the entities currently regulated by sector-specific U.S. federal privacy statutes and regulations, ensuring harmonization by following FIPPs and the sector-specific approaches is essential as data flows, purposes, and uses may cross sectoral boundaries.

Primary Framework for Data Privacy and Security in Healthcare

The framework established by the HIPAA Privacy Rule should be maintained and any privacy framework for personally identifiable information (PII) should harmonize with HIPAA to ensure efficient data flow. HIPAA established a uniform framework for acceptable uses and disclosures of individually identifiable health information within healthcare delivery and payment systems for the privacy and security of health information to enable the provision of health care services to patients. Existing sectoral laws like HIPAA provide robust, well-tested protections that should be preserved under any federal privacy law. Displacing such frameworks could undermine effective data governance in critical sectors like healthcare. HIPAA follows the widely accepted FIPPS.

The HIPAA Privacy Rule, through “implied consent,” permits the sharing of medical information for specified identified healthcare priorities which include treatment, payment, and healthcare operations (as expected by patients seeking medical care). This model has served patients well by ensuring quick and appropriate access to medical care whenever the patient seeks that care, especially in emergency situations where the patient may be unable to give written consent.

The HIPAA Privacy Rule requires that healthcare providers and health plans limit disclosure of protected health information (PHI) to the minimum necessary to pay for healthcare claims and other essential healthcare operations. This practice provides privacy protection while allowing for continued operations. Minimum necessary is relatively easy and simple to administer and practice for healthcare treatment, payment and operations. Ultimately, personal health information must be secured and protected from misuses and inappropriate disclosures under applicable laws and regulations.

A Federal Comprehensive Data Privacy and Security Framework Must Harmonize with HIPAA

HIPAA-covered entities and their business associates, all of which must comply with HIPAA and interoperability requirements, note that in healthcare data flows between HIPAA-covered entities and business associates. For those not regulated by HIPAA, it is vital that privacy governing PII harmonizes with HIPAA to make for efficient and protected data flow.

There are several components of a baseline federal data privacy law that would be essential to harmonization for the healthcare sector. In this vein, we urge policymakers to:

- Carve out entities regulated by sector-specific federal data privacy standards (e.g., health sector with HIPAA and HITECH, health and medical research conducted under federal regulation, finance sector with Gramm-Leach-Bliley Act (GLBA), and higher education sector with The Family Educational Rights and Privacy Act of 1974 (FERPA), so they continue to need only meet that standard to be compliant.
    - By exempting these covered entities from the new federal framework and avoiding duplication with any new regulation, their proven standards can be maintained, and unnecessary regulatory overlap will be avoided.
    - These existing federal laws already provide specialized protections in areas such as healthcare, research, and financial services.
    - This approach respects established sector-specific rules while ensuring that the new federal law fills gaps and addresses privacy in areas not covered by existing legislation.

- Pre-empt all state data privacy laws and create a federal data privacy law standard. This is essential for data flow, economic development, and innovation.
    - Ensure HIPAA-like protections for non-HIPAA protected personal information.
        - The data controller holds responsibility for the use, storage, and collection of information consistent with the purposes for which the data was collected.

        - HIPAA permits a provider whose patient has generally agreed to the office's Notice of Privacy Practices (NPP) access to an individual patients' personal health data without needing to expressly receive patient consent each time the given patient shows up to obtain medical care for the purposes of treatment, payment, and operations.
    - The use of the information is limited to a "minimum necessary" standard.
        - Collect only the data necessary to perform the core functions of the tool. For instance, if tracking sleep patterns does not require capturing GPS location, that data should not be collected.

- Ensure the applicable legal definition of "de-identified information" aligns to the HIPAA definition of de- identified information, which is globally recognized as the 'gold standard.' For healthcare in particular, a federal data privacy framework should not create 'subcategories' of data (issue-specific) given the operational and compliance burdens borne to covered entities/business associates to manage.
- Enforcement and federal pre-emption of state law are imperative and must be done wisely.
    - Allowing local courts to interpret the rules could turn each one into a separate regulator, leading to inconsistent consumer protections and varying interpretations of the law.
    - A right to cure in a timely manner before enforcement takes place provides incentives to protect data and cure issues as they occur.

RESPONSES TO THE RFI'S SPECIFIC QUESTIONS

I. Roles and Responsibilities

A. How can a federal comprehensive data privacy and security law account for different roles in the digital economy in a way that effectively protects consumers?

- A federal comprehensive data privacy and security law should maintain the existing roles of controllers, processors, and third parties, as used in most current privacy laws. This structure is effective because it clearly defines who is responsible for deciding why and how personal data is processed, which is essential for protecting consumers.
- Introducing additional roles, like the "contractor" role in the California privacy bill, creates unnecessary confusion due to overlapping responsibilities and increased compliance complexity.

- By sticking to the clear and established framework, it ensures responsibilities are well-understood and consumer data is more reliably protected.

B. What are appropriate obligations for different regulated entities, and what are the practical and legal limitations associated with each type of entity?

- Controllers should not be held vicariously liable for actions of processors if certain conditions are met. If controllers conduct thorough due diligence when selecting processors or lack the authority to choose the processor, they should be afforded a safe harbor. This concept ensures that controllers are responsible for their choices and oversight but are not unfairly penalized for actions beyond their control.

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

- Any requirements or obligations should be scaled based on the size of an entity so that the law can ensure fair and practical compliance. This approach will promote wider compliance by providing clear guidelines that accommodate the operational realities of smaller entities, like independent rural providers.

II. Personal Information, Transparency, and Consumer Rights

A. Please describe the appropriate scope of such a law, including definitions of "personal information" and "sensitive personal information."

- In defining "sensitive personal information" (SPI) for a comprehensive data privacy and security law, it is crucial to have a consistent and clear definition across all jurisdictions to ensure cohesive regulation. Key considerations include:
  1. SPI should exclude PHI when it is covered by HIPAA and Nonpublic Personal Information (NPI) when covered by the GLBA. This exclusion avoids regulatory overlap and ensures clarity in legal obligations.
  2. Establishing a uniform, national definition of SPI is essential to facilitate compliance and simplify interstate operations. Currently, much of the SPI is defined by circumstances not directly related to privacy laws, making it difficult for data holders to discern. Any future law should also consider contextual variability, as some data, like purchase of bandages,

can span both sensitive and non-sensitive contexts. Addressing these nuances will prevent overgeneralizations and enhance data protection.

- Requirements related to consumer data opt-outs within an AI context should be carefully evaluated to ensure feasibility and avoid unintended consequences.

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

- To ensure appropriate consumer disclosures regarding the collection, processing, and transfer of personal and sensitive information, especially health and financial data leaving HIPAA- and GLBA-regulated entities, the following should be implemented: Non-HIPAA entities, such as third-party app operators, must clearly state why they collect, use, and disclose identifiable health information. Requiring public posting of a NPP for these entities can enhance transparency.

C. Please identify consumer protections to include 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?

- Consumers should have the right to access their personal information held by businesses. This empowers individuals to understand what data is collected, how it is used, and with whom it is shared.
- Like HIPAA, consent or authorization to use or process non-HIPAA-covered identifiable health information should be assumed when a consumer seeks a service or purchase the consumer initiated. Privacy policy for each entity should be straightforward and accessible, ensuring consumer privacy and security policies integrated within digital health tools.
- Entities not subject to existing privacy laws should provide consumers the ability to consent before their sensitive personally identifiable information is collected, processed, or transferred beyond the initial terms of agreement. This ensures individuals are fully aware of and agree to how their information is handled.

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

- Businesses not subject to the privacy law should follow heightened protections such as:

1. HIPAA-Like Protections: Implement protections parallel to those under HIPAA, including limitations on data use and adherence to the “minimum necessary” standard. This minimizes the risk of unnecessary exposure of sensitive personal information.
2. Privacy Framework Adherence: Businesses should align their practices with the established frameworks such as the National Institute of Standards and Technology (NIST) privacy framework. This provides a structured approach to managing privacy risks and reinforces security and compliance.

III. Existing Privacy Frameworks & Protections

A. Please provide any insights learned from existing comprehensive data privacy and security laws that may be relevant to the working group’s efforts, including these frameworks’ efficacy at protecting consumers and impacts on both data-driven innovation and small businesses.

- From existing data privacy and security laws, one key insight is the importance of clarity in how different entities are defined and treated. For example, in California, the distinction between "service providers" and "contractors" has proven to be both confusing and unnecessary.

B. Please describe the degree to which U.S. privacy protections are fragmented at the state-level and the costs associated with fragmentation, including uneven rights for consumers and costs to businesses and innovators.

- No input at this time.

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

- The federal comprehensive data privacy and security law should adopt total preemption to establish a universal standard. This would ensure consistent protection for all consumers and simplify compliance for businesses operating nationwide, eliminating confusion from the current patchwork of state laws.

D. How should a federal comprehensive privacy law account for existing federal and state sectoral laws?

- A federal comprehensive privacy law should incorporate exemptions for existing sectoral laws such as HIPAA, HITECH, and GLBA. These laws already provide specialized protections in areas such as healthcare and financial services. By exempting them from the new federal framework, we can maintain their proven standards and avoid

unnecessary regulatory overlap. Exemptions should apply to the law in its entirety, not specific sections. This approach respects established sector-specific rules while ensuring that the new federal law fills gaps and addresses privacy in areas not covered by existing legislation.

IV. Data Security

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

- To enhance consumer data security, a comprehensive federal privacy law should:
    1. Align with current laws and applicable frameworks to leverage established protections and streamlining integration.
    2. Create a flexible framework that enables customization of cybersecurity measures based on the unique operational contexts of different entities, moving away from a one-size-fits-all model.
    3. Ensure that all definitions are clear and appropriately scoped to minimize confusion and aid compliance.
    4. Design requirements that encourage essential documentation and processes while minimizing excessive administrative burdens.
    5. Set implementation and compliance timelines that respect the diverse needs of industries like healthcare and align with existing audits and certification processes to ease transition.
    6. Include safe harbor provisions to protect entities adopting established frameworks, like NIST, from liabilities. This incentivizes adherence to recognized security standards and promotes robust data security practices.

V. Artificial Intelligence (AI)

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

- It is important to simultaneously consider AI frameworks and impact on AI and innovation. Recommendations include:
    1. Alignment with Existing Standards: Policymakers should prioritize deferring to and aligning with existing laws, regulations, and guidance whenever applicable. This ensures consistency and leverages established frameworks.
    2. Adopt Expert-Developed Standards: Support alignment with expert- and consensus-developed standards, ensuring

consistent definitions and a risk-based approach to regulation. This provides clarity and precision in addressing AI and automated decision-making.

3. Preempt State AI Regulations: To maintain a unified national framework and encourage innovation, federal law should preempt state regulations on AI. This prevents a fragmented regulatory landscape and supports consistent policy implementation across all states.
4. Avoid Conflicts with AI Regulations: Ensure that privacy laws do not conflict with AI regulations, creating a coherent legal environment that allows both privacy and technological advancement to coexist harmoniously.
5. Consider Third-Party Regulations: Evaluate the need for regulations concerning third-party AI providers to ensure accountability and maintain data protection standards.

- Policies regarding AI use in health care should be led by the Assistant Secretary for Technology Policy (ASTP) to effectively account for industry-specific needs and differences.

VI. Accountability & Enforcement

A. Please identify the benefits and costs of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law.

- Entities subject to the new privacy law should be regulated by a single expert agency, like the Federal Trade Commission. As such, any health care-aligned entities should be regulated by the Department of Health and Human Services. This centralized approach ensures that enforcement is consistent, predictable, and driven by specialized expertise.
- Avoid Complexity of Locally Determined Private Right of Action (PRA): Allowing local courts to interpret the rules could turn each one into a separate regulator, leading to inconsistent consumer protections and varying interpretations of the law.

B. What expertise, legal authorities, and resources are available—or should be made available—to the FTC and state Attorneys General for enforcing such a law?

- Drawing from California's example, a portion of the fines collected from enforcement actions could be allocated back to the enforcing agencies. This funding can support operating expenses, enhancing their capacity to enforce the law effectively.

C. How could a safe harbor be beneficial or harmful in promoting compliance with obligations related to data privacy and security?

- Including a safe harbor provision that offers an affirmative defense for entities complying with established security measures, like HIPAA or NIST frameworks, can be highly beneficial:
  1. Incentivizes organizations to adopt robust security measures, motivating adherence to high standards.
  2. Aligning with established frameworks provides clear guidelines and predictability, enhancing data protection.
  3. Allows businesses to focus .on effective security practices rather than potential litigation, promoting a preventive culture.

VII. Additional Information

In addition to the topics detailed above, we are extraordinarily concerned about the impact that changes in privacy policy could have on clinical research, and consequently drug development. We encourage the Privacy Work Group to incorporate these specific guidelines into draft legislation, to ensure that these critical research programs can continue.

- Clinical Research Exemptions:
  Legislation should appropriately balance the rights of individuals to their personal information with researchers' need to be able to collect, use, and share information for scientific advancement, through the inclusion of exemptions for clinical research activities.

- Appropriate Definition of Health Data:
  Legislation should appropriately define "health information" or "health data" to protect information that actually reveals an individual's medical history, condition, or treatment, but that is not so broad it impedes pharmaceutical and medical device companies' ability to provide beneficial information to patients.

- Workable Consents Frameworks:
  Legislation should promote transparency, so consumers are aware of what and how their personal information is used and promotes consumer choice regarding their sensitive information, while creating workable notice and consent frameworks that are operationally feasible and do not subject consumers to notice and consent fatigue.

Conclusion

HLC and the Confidentiality Coalition appreciate the opportunity to partner on the development of the federal comprehensive data privacy and security framework. Thank you for considering our comments. If you have any questions, please do not hesitate to contact me at kmahoney@hlc.org.

Sincerely,

Katie Mahoney
Executive Vice President and Chief Policy Officer