



Submitted via email to: PrivacyWorkingGroup@mail.house.gov

April 4, 2025

Chairman Brett Guthrie (KY-02)
Vice Chairman John Joyce, M.D. (PA-13)
U.S. House of Representatives Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 2051

RE: Data Privacy Working Group Request for Information

Dear Chairman Guthrie and Vice Chairman Joyce:

The Healthcare Trust Institute appreciates the opportunity to submit comments on the Data Privacy Working Group Request for Information (RFI) issued on February 12, 2025.¹

The Healthcare Trust Institute (HTI) is an alliance of healthcare organizations committed to promoting and implementing effective privacy and security protections for health information that engender trust in the healthcare system and allow for the advancement of treatments, cures and improved healthcare quality for individuals and populations. HTI members, which include companies and organizations from across the U.S. healthcare economy, agree that a strong national privacy standard for health information is needed to protect sensitive data and spur medical innovation.

We applaud the formation of the Data Privacy Working Group (Working Group) and strongly support its stated goal of passing a comprehensive federal law to protect consumer personal information. This is essential not only to maintain consumer trust in digital technology, but to ensure continued US leadership in digital innovation, including in rapidly developing technological areas such as artificial intelligence (AI), where states are stepping in to regulate in the absence of federal standards, with all the attendant inefficiencies, inconsistencies, duplication, and unnecessary costs that this entails. Enacting a federal privacy law is also

¹ See <https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-issue-request-for-information-to-explore-data-privacy-and-security-framework>.

critical to ensure the unrestricted flow of data between the United States and other countries, an increasing number of which now restrict the flow of personal information to jurisdictions where the data is not assured of appropriate protection.

We discuss these and other issues raised by the RFI “prompts” in greater detail below.

I. Roles and Responsibilities

We support clearly articulated roles for data controllers, processors, and third parties that hold personal health data. Without clearly defined roles, there is no consistent baseline for accountability. It is also important for consumers to understand who is responsible when their personal data is misused/breached. We recommend a harmonized approach across HIPAA and non-HIPAA entities, using the HIPAA concepts of “covered entity” and “business associate” as a basis for the roles and responsibilities of controllers/owners and processors/service providers holding personal health data outside HIPAA.

HIPAA and many state privacy laws require covered entities/controllers contractually to flow down to data processors certain data protection obligations already imposed on data processors under the law. This approach has resulted in business contracts being accompanied by increasingly lengthy regulatory data addenda, which is cumbersome and costly and does little to increase privacy protections, since these are already enshrined in the law. As long as a federal privacy law clearly articulates roles and responsibilities, it should not be necessary to restate these contractually. Contractual flow-down provisions should be necessary only when the data recipient would otherwise not be subject to the law directly (for example, if they operate outside the United States). Under this approach the parties may still choose to contractually agree, as a business matter, on additional data terms and restrictions beyond those imposed by the law.

While it is important that entities of all sizes protect consumer personal data, we also believe it is appropriate to take into account the size of the entity in imposing new, and potentially costly and onerous privacy and security obligations. Smaller entities generally have fewer resources, both financial and human, to meet their regulatory obligations, and it is important that they not be put at a competitive disadvantage as a result of the heavier relative regulatory burden. Therefore, we encourage the Privacy Group to consult with stakeholders to consider ways to ease this burden without compromising data privacy and security. For example, the law might allow smaller entities additional time to come into compliance, and provide ways to streamline their compliance obligations, such as through certain types of safe harbors or certifications.

II. Personal Information, Transparency, and Consumer Rights

A. Categories of Personal Information

While we understand that consumers may regard certain types of personal data as more “sensitive” than others, drawing these types of distinctions in law can be challenging because of the subjective nature of these determinations. In addition, personal information that is not considered as “sensitive” could potentially be used to identify other records that are considered as “sensitive,” suggesting that both sets of data receive the same protections. We are also concerned that by creating distinctions between different types of personal information, the law will become unnecessarily complicated. We urge the Working Group to prioritize harmonization

and burden reduction, either by requiring a high enough level of privacy hygiene that all personal information – even that which could be deemed “highly sensitive” - is satisfactorily protected or by minimizing the different categories of data and the number of different controls that must be implemented for each.

Treating all personal information as deserving the same protections is consistent with the approach taken in the HIPAA Privacy Rule.² The wisdom of this approach has been proven over the years, particularly for personal health information, as creating different categories of data with different levels of protection in the health sphere has resulted in data siloing and record fragmentation, ultimately leading to unintended negative consequences for care.³ While these care considerations are specific to personal health data, in many cases the line between health and non-health personal information is not clear. Moreover, the complexities of different levels of protections and rules related to different categories of personal information and the operational challenges of data segmentation extend beyond personal health data.

B. Protections for Personal Information

Consumers should be provided a clear and simple privacy notice that explains the purposes for which a regulated entity collects and discloses their personal health information, as well as the consumer’s rights and choices with respect to that information. These rights should generally include the right to access, amend and, subject to limited exceptions, delete their personal information.

In addition, consumers should be assured that their personal information will be used and disclosed only for purposes consistent with their reasonable expectations in the context in which the personal information was provided. This approach has been used effectively under the HIPAA Privacy Rule for many years, where covered entities provide consumers with a notice of their privacy practices describing the health-related purposes for which PHI may be used and disclosed without the consumer’s explicit authorization. Patients understand and accept that by providing their PHI for health-related purposes they are implicitly consenting to its use and disclosure for these purposes. This includes not only direct services such as treatment or payment for health care services, but also certain supporting or secondary uses, known as health care operations. These encompass business and operational uses to support direct services, such as to train AI models used in the development or provision of various health care functions or services. It also includes certain uses and disclosures for the public good, such as for public health, judicial or administrative proceedings and law enforcement, subject to certain conditions and limitations.

² See 65 Fed. Reg. at 82731 (“We generally do not differentiate among types of protected health information, because all health information is sensitive”). The only exception is with respect to psychotherapy notes, a very narrow category of records that, by definition, is created and kept separate.

³ It was for this reason that Congress revised the statute governing substance use disorder records in 2021 to make it more aligned with HIPAA so that it would no longer be necessary to keep these records separate from the rest of the patient’s records.

Unlike an approach that requires consumers to consent to every use and disclosure of their personal information, this approach ensures that the consent mechanism does not become a mere rubber stamp or mandatory hoop that consumers must jump through in order to obtain the services they seek. It also avoids placing all the responsibility on the individual to sift through the consent language, and so effectively police, the various purposes for which their information is used. From a practical perspective, it is much more practical and less burdensome, since many beneficial uses of personal health data would simply not be possible if patients had to consent to every supporting or secondary use of their data, given the difficulty of obtaining such consents and the potential limitations if only a subset of patients consent. Allowing patients to opt out of the use of certain of their data, or to opt out of the use of their data for certain purposes is equally problematic, since this could jeopardize care. By allowing a set of uses and disclosures implicit in the provision of the personal information without explicit consent, and instead focusing on transparency over rigid consent mechanisms, the legislation would create a more balanced and flexible approach that also promotes responsible innovation.

C. Proportionate Data Use and Deidentification

The federal privacy law should incorporate the concept of limiting the use of personal data to that which is proportionate and necessary to the purpose for which it was collected. Allowing de-identification of personal information or privacy-enhancing technology (where feasible) and excluding it from restrictions applicable to personal information is critical to encourage data minimization and allow for important and beneficial public purposes, such as medical research and public health. To engender consumer and patient trust and public support, recipients of deidentified data should be prohibited from attempting to re-identify the data, and should be required to contractually or publicly commit that they will not attempt to do so. The definition of “deidentified information” under a federal privacy law should be harmonized with the HIPAA definition of the term to avoid unintentionally encompassing HIPAA deidentified data within the definition of personal information.⁴

III. Existing Privacy Frameworks & Protections

A. Preemption

In announcing the RFI, Chairman Guthrie and Vice Chairman Joyce stated their strong belief that “a national data privacy standard is necessary to protect Americans’ rights online and maintain our country’s global leadership in digital technologies, including artificial intelligence.” We echo these sentiments, both regarding the urgent need to establish a federal law to protect consumer personal information, as well as the need for that federal law to set a national standard.

HTI has long advocated for a robust, comprehensive federal law to protect the privacy and security of personal information, including personal health information that is not protected by HIPAA or other existing federal data protection frameworks. The federal law should harmonize

⁴ This could occur if the federal privacy law carves out PHI, as recommended in Section III but not HIPAA deidentified data, since latter is no longer PHI and so would not meet the carve out for PHI.

with HIPAA in its approach, concepts, and definitions. However, unlike the current HIPAA privacy framework, which merely sets a federal floor of privacy protections, the law should set a true national standard.

The healthcare sector – including the members of HTI – have invested heavily in privacy and cybersecurity protections designed to comply with HIPAA. HIPAA has benefited the sector by increasing patient trust and elevating security and data protection standards across HIPAA regulated entities. HTI strongly urges the Working Group to have conversations with healthcare stakeholders so as to be able to build upon lessons learned from the healthcare sector’s experience under HIPAA in any new legislation. A comprehensive privacy law should incorporate the tenants of the HIPAA framework that have proven effective, creating a harmonized privacy framework that adequately encompasses the modern data ecosystem.

This cannot be achieved without broad preemption of all state laws addressing the privacy and security of personal information, regardless of whether they are more or less stringent than the federal standard, or whether they conflict or overlap with it. Broad preemption is essential not only to ensure a consistent privacy and security standard across the country, but also to increase efficiency, promote innovation, and avoid the cost, burden and compliance challenges involved in implementing a patchwork of inconsistent, potentially even conflicting, state standards, requirements, and consumer privacy rights.

The need for broad federal preemption has become more urgent as more states have stepped in to pass comprehensive data protection laws in the absence of progress at the federal level,⁵ creating a thicket of different data protection laws. This is both confusing and difficult to navigate for patients and consumers as well as burdensome and costly for businesses, with no counterbalancing privacy benefits. It also inhibits technological improvements and innovation, particularly in the area of AI, as different rules for the use of data needed to develop and deploy AI solutions apply in different states, imposing operational and compliance barriers.

B. Existing Data Protection Frameworks

It is important that a federal data protection law not disrupt or interfere with existing federal data protection frameworks, such as HIPAA. HIPAA has been in place for a quarter of a century, and has become the gold standard for the protection of patient health information in the health care sector. It is well-understood and trusted by patients and health care organizations alike, and should remain the framework for the regulation of patient health information in the health care industry and, ideally, should become the single national standard for the protection of PHI, preempting state laws addressing the privacy and security of PHI.

While HIPAA is the best known federal data protection framework, we believe the same considerations apply to other sector-specific federal data protections laws, such as Gramm-Leach Bliley and federal regulations protecting personal information used in research, and

⁵ To date, 20 states have adopted generally applicable privacy laws, and this number is expected to grow as long as Congress does not pass a national privacy law that applies to personal data, including personal health data not already subject to HIPAA. See <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>.

entities and data subject to these frameworks should be exempt from the comprehensive federal data protection law.⁶

IV. Data Security

We agree that robust security for consumer personal information should be a foundational requirement of any federal comprehensive data protection law, particularly as the number, scale and sophistication of cyber-attacks has escalated in recent years.

The federal law should adopt a risk-based approach to security that is consistent with nationally-recognized frameworks, such as the National Institute for Science and Technology (NIST) Cybersecurity Framework and the NIST Special Publication 800-53. While all regulated entities should be required to implement administrative, technical, and physical safeguards to protect personal information, the law should be flexible and technology neutral, allowing regulated entities to adapt to evolving cyber threats and to tailor their safeguards to their security needs, taking into account the nature of their operations, the data they hold, their operating environment, size, and organizational structure, among other relevant factors. Stronger, uniform standards along with streamlined reporting to a single entity, are both protective and cost-effective for healthcare organizations, with long term benefits far outweighing any short-term costs.

We also believe the federal government has a critical role to play in bolstering cybersecurity, particularly for regulated entities in critical infrastructure sectors, such as health care. Key areas that would benefit from federal involvement, and where the federal government is uniquely qualified to help, include establishing a national cybersecurity insurance fund, providing incentives to increase the workforce of cybersecurity professionals, increased bi-directional cybersecurity intelligence sharing between the government and the private sector, and funding to support the cybersecurity needs of smaller entities. We encourage the Working Group to engage with stakeholders to determine how best to incorporate these concepts into a comprehensive federal data protection law.

V. Artificial Intelligence

Given the centrality of data to AI solutions, the passage of a comprehensive federal data protection law should be a prerequisite for adoption of any national standards for the development and use of AI. Without robust national protections for personal information any incident involving personal data used in AI solutions is more likely to trigger consumer skepticism and distrust in AI, which could in turn dampen and inhibit the development of new AI solutions, acting as a headwind to US AI innovation and leadership.

In addition, as with data protection standards, we believe that it is imperative that standards for AI be set at the national level. Within the last year alone, hundreds of state bills have been introduced seeking to regulate almost every aspect of the development and use of AI, and the pace of new state bills on AI is only increasing, with more and more being enacted each year. Compliance with this proliferation of state laws will be extremely challenging and onerous for the vast majority of organizations that do not operate exclusively within one state. For these

⁶ The Virginia Consumer Data Protection Act, which has been used as a model by many other states, provides a clear and comprehensive list of appropriate exceptions. See Va Code § 59.1-576.

reasons we support explicit federal preemption of state laws regulating AI. This is especially important for key areas where inconsistent and conflicting requirements would become impracticable or overly burdensome.

A federal AI framework should focus on high-risk AI, rather than any automated decision-making, and should be established in coordination with industry, rather than being solely government-driven. It should be based on widely-used and well-respected frameworks that rely on a risk-based approach, such as the AI Risk Management Framework (RMF) issued by NIST. This framework was developed with cross-industry and business perspectives in mind, ensuring that its approach responsibly addresses the risks of AI without being overly prescriptive so as to stifle innovation or competition. Quantitative measures, data specifications, and reporting requirements should be based on nationally adopted voluntary consensus-based standards.

Establishing a national framework for AI is essential also because the development and use of AI-solutions is generally sector-specific, with different use cases, risks and regulatory environment and context in each sector. As a result, the only way to provide workable standards for the use of AI (i.e., that do not upend or conflict with existing frameworks or regulations) is to set a national framework, and then delegate the responsibility for any more specific regulation to existing sector-specific federal agencies with the necessary regulatory background, and subject matter knowledge and expertise. For example, the regulation of AI in the health sector should be delegated to the Department of Health and Human Services (HHS), which should work in partnership with healthcare organizations to develop a consensus on what constitutes high-risk AI warranting regulation in healthcare.

A federal AI framework will also bring greater regulatory certainty, which will create a more fertile environment for the development of AI solutions, as major investment in AI depends on a clear understanding of the “rules of the road.” Thus, regulation based on adoption of national standards can promote American competitiveness and promote innovation through investments in AI. Both AI developers and those deploying AI need the assurance that the regulatory environment will not be hostile to the application of AI, whether through overly prescriptive requirements or undue burdens, such as onerous and frequent evaluations and assessments of all AI tools rather than targeted risk-based evaluations and assessments as needed.

VI. Accountability & Enforcement

We strongly support a robust enforcement mechanism for a federal data protection law that effectively punishes wrongdoers and deters against violations while providing for consistent and predictable enforcement. When enforcement changes with each administration, it creates an environment of uncertainty detrimental to long-term privacy and security investments.

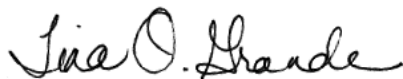
We recommend an enforcement framework with tiered penalties based on level of culpability that is clear, well-defined, and leaves little room for interpretation beyond statutory language. This could be enforced by any of the existing agencies, but we urge lawmakers and, in their turn, government agencies, to retain control over the targeting and type of penalties imposed to better achieve the policy goals of the legislation.

It is also critical that whatever government agency is responsible for enforcement be invested with the authority and resources necessary to do so, including funding to develop the necessary expertise to effectively enforce the law. We also believe there would be significant value in form of greater consistency, shared expertise, and efficiency for the same government agency to be responsible for enforcing all privacy and security laws pertaining to personal health information.

We also believe that safe harbors and similar concepts, such as allowing regulated entities an opportunity to cure before the imposition of penalties, can play a constructive role in promoting compliance while reducing costs and inefficiencies.⁷ For example, regulated entities that comply with well-established national cybersecurity frameworks, such as the NIST cybersecurity framework, could be deemed to be in compliance with the federal law's security requirements. We recommend that the Workgroup convene stakeholder meetings to consider innovative and effective safe harbor mechanisms that encourage compliance while alleviating unnecessary burden.

Thank you for your consideration of our comments. We appreciate the efforts of the Working Group and look forward to working with you as you proceed with the important work of developing the necessary foundation for passage of a federal data protection law. Please do not hesitate to contact me at tina@hctrustinst.com or 202-750-1989 if you have any questions

Sincerely,

A handwritten signature in cursive script that reads "Tina O. Grande".

Tina O. Grande
President, Healthcare Trust Institute

⁷ See, for example, the Virginia Consumer Data Protection Act, which provides for a 30-day cure period before the imposition of any penalties. VA Code § 59.1-584.