

September 28, 2023

Senator Bill Cassidy, M.D.  
Ranking Member  
Committee on Health, Education, Labor, and Pensions  
United States Senate  
455 Dirksen Senate Office Building  
Washington, DC 20510

Dear Ranking Member Cassidy,

On behalf of the 31 member companies of the HIMSS Electronic Health Record (EHR) Association, we appreciate the opportunity to offer feedback on the HELP Committee's request for information on ways to improve the privacy protections to safeguard health data.

As a national trade association of EHR developers, EHR Association member companies serve the vast majority of hospital, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs and other health IT across the United States. Together, we work to improve the quality and efficiency of care through the adoption and use of innovative, interoperable, and secure health information technology.

The EHR Association has long advocated for enhanced protection of sensitive health data held by actors outside of the bounds of HIPAA regulation. Health data is a multifaceted category of information that extends beyond the confines of HIPAA. The governance of health data should evolve to keep pace with the rapid advancements in technology while also respecting individuals' expectations of privacy. A flexible and context-aware regulatory framework can strike the necessary balance between safeguarding health data and fostering innovation in healthcare.

We support the Committee's efforts to modernize HIPAA and are pleased to provide our perspective on this issue. Our specific responses follow.

Sincerely,



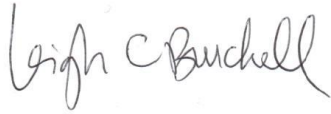
David J. Bucciferro  
Chair, EHR Association  
Foothold Technology



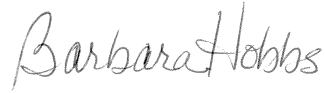
William J. Hayes, M.D., M.B.A.  
Vice Chair, EHR Association  
CPSI

AdvancedMD	eClinicalWorks	Flatiron Health	MEDITECH, Inc.	Oracle Cerner
Allscripts	Elekta	Foothold Technology	Modernizing Medicine	PointClickCare
Altera Digital Health	eMDs – CompuGroup Medical	Greenway Health	Netsmart	Sevocity
Athenahealth	EndoSoft	Harris Healthcare	Nextech	STI Computer Services
BestNotes	Epic	MatrixCare	NextGen Healthcare	TenEleven Group
CPSI	Experity	MEDHOST	Office Practicum	Varian – A Siemens Healthineers Company
CureMD				

## HIMSS EHR Association Executive Committee



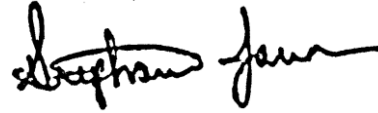
Leigh Burchell  
Altera Digital Health



Barbara Hobbs  
MEDITECH, Inc.



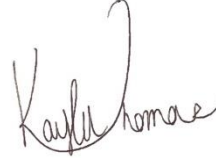
Cherie Holmes-Henry  
NextGen Healthcare



Stephanie Jamison  
Greenway Health



Ida Mantashi  
Modernizing Medicine



Kayla Thomas  
Oracle Cerner

*Established in 2004, the Electronic Health Record (EHR) Association is comprised of 31 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families. The EHR Association is a partner of HIMSS. For more information, visit [www.ehra.org](http://www.ehra.org).*

## Electronic Health Record Association

Feedback on the HELP Committee's request for information on ways to improve the privacy protections to safeguard health data.

---

### General Privacy Questions

1. What is health data? Is health data only data governed by HIPAA, or are there other types of health data not governed by HIPAA? Should different types of health data be treated differently? If so, which? How? If not, why not?

Health data is information that is individually identifiable and pertains to an individual's past, present, or future behavioral or physical health, including their health conditions. This definition can encompass a broad spectrum of data, potentially extending to Social Determinants of Health (SDOH) data when relevant to a patient's health.

It is critical to acknowledge that health data is not confined solely to the realm of data governed by HIPAA. In recent years, the proliferation of smart devices, fitness trackers, and various consumer technologies, such as health-related mobile applications, has led to the generation of substantial volumes of health data that fall outside the jurisdiction of HIPAA.

Crucially, individuals reasonably expect that their health data should be safeguarded and its privacy preserved by the entities that possess it. This expectation is underscored by the fact that individuals frequently misinterpret HIPAA's privacy provisions as applying to entities that do hold their health information but are not subject to HIPAA's regulatory framework.

Furthermore, it is worth emphasizing that the identifiability of health data plays a pivotal role in determining the level of protection it should receive. When health data undergoes a process of de-identification, effectively removing personally identifiable information, it may not require the same degree of rigorous protection as identifiable health data.

2. Which entities outside of HIPAA Covered Entities should be accountable for the handling of health data (not necessarily HIPAA-covered data)? Should different types of entities have different obligations and privileges? Please explain using examples.

To establish a robust framework for accountability, the EHR Association recommends that all commercial entities, regardless of their for-profit or non-profit status, should be subject to a baseline set of privacy and security protections akin to those mandated by HIPAA. This approach aligns with the existing expectations patients have regarding the privacy and security of their health information and serves to elevate the minimum standards for data privacy and security practices.

Standardizing privacy and security protections will foster trust among stakeholders involved in health data stewardship, including third-party applications and healthcare systems. Patients and individuals will have greater confidence that their health information is safeguarded, irrespective of the entity holding it.

A uniform set of standards encourages greater interoperability and innovation in the healthcare ecosystem. When patients, health systems, and other health data custodians are assured that their data will be protected to a level similar to HIPAA standards, they are more likely to engage in data sharing and collaboration. This eases the development of novel healthcare solutions, as well as the seamless exchange of health information between entities.

## Health Information Under HIPAA

### 1. How well is the HIPAA framework working? What could be improved?

The HIPAA framework has, by and large, worked reasonably well in regulating the entities for which it was initially designed. However, in the ever-evolving landscape of healthcare data stewardship, there is concern regarding the disparity in expectations between HIPAA-regulated entities and other custodians of health data. There is a need for greater transparency and control for individuals over the usage of their health data, regardless of whether the data holder is a HIPAA-regulated entity.

Opportunities for improvement include refining the scope and definition of health data under HIPAA. Specifically, we recommend eliminating variations that exist in data sensitivity, including distinctions between physical and behavioral health, as well as other health data categories. In our experience, there is an unreconcilable lack of consensus on what is considered “extra-sensitive” health information, because it varies by individual and can vary over time as societal norms evolve. This often results in stringent restrictions being applied to certain types of healthcare (e.g., behavioral health, substance use disorder, reproductive health) in a manner that hampers efficient patient care—only for the rules to be altered when the negative impacts of such stringent rules are realized after the fact. For example, the industry is now recognizing the strains that 42 CFR Part 2 privacy rules have placed on treating individuals with substance use disorder, despite the original positive intent.

We therefore caution against overly restrictive requirements for ill-defined “extra-sensitive” health information, since it can add significant burdens to patients, their caregivers, and clinicians. Instead, a robust but consistent set of privacy expectations (including clear guidelines on the ability for law enforcement to request and access patient records/the use of health records in legal proceedings) across all health data will better balance treatment and privacy.

Furthermore, there is potential for standardizing expectations for scenarios involving the privacy of adolescents and older adults. States have implemented a patchwork of laws describing when adolescents and others can enforce restrictions on parent/caregiver access to their records. Standardizing those expectations would improve consistency and make it easier to support health IT tools on which clinicians, individuals, and parents rely.

### 2. Should Congress update HIPAA?

Yes, Congress should consider updating HIPAA to better align with the evolving healthcare landscape. The primary focus of these updates should be expanding the scope of HIPAA to encompass a wider array of entities that have stewardship of health data, including those

companies that develop apps and fitness wearables. This expansion is necessary to establish a consistent baseline of expectations regarding the privacy and security of health information in today's interconnected healthcare environment. By broadening the scope, we can ensure that individuals' health data remains protected, regardless of the entity holding it, fostering greater trust and transparency in the healthcare ecosystem.

3. Should Congress expand the scope of HIPAA? What specific information should be included in the HIPAA framework?

The existing HIPAA framework provides comprehensive guidelines on how to protect health data effectively. Therefore, updates should primarily concentrate on extending these robust data protection measures to all entities that have stewardship health data but that do not fit into the role of a HIPAA Covered Entity or Business Associate today.

Congress should consider expanding the scope of HIPAA to broaden the definition of Covered Entities to include any business that sells or provides consumers with health-related goods or services or receives other valuable consideration for such services. For instance, consumer applications and various service providers, such as worker's compensation providers, handle health data and should be subject to the same privacy and security standards as traditional Covered Entities.

However, as the definition of Covered Entities expands, it will be important to also establish clear criteria for differentiating between Covered Entities and Business Associates. This clarification will help maintain the integrity of the HIPAA framework and ensure that entities act within the appropriate scope of their relationship to individuals and healthcare providers when implementing protections.

4. What challenges would legislative reforms to HIPAA create?

While legislative reforms to HIPAA hold the potential to enhance data privacy and security, they must be carefully implemented to avoid potential challenges.

A potentially significant challenge in change management would arise if reforms included altering the expectations for how already-regulated entities protect health data. Any substantial shift in existing requirements could disrupt established practices and systems and negatively impact patient treatment, data sharing, cross-functional collaboration, research, and innovation. However, if the focus of reform is primarily on extending existing expectations to other types of entities handling health data, it can minimize disruptions for those entities already regulated by HIPAA.

Another challenge stems from the need to coordinate federal HIPAA regulations with various state and local privacy laws. Currently, a significant amount of resources are dedicated to analyzing the interaction between HIPAA and other laws at different jurisdictional levels. Legislative reforms should aim to clarify how and when HIPAA pre-empts state laws, reducing regulatory complexity and ensuring a more consistent approach to data privacy and security across the nation.

Finally, expanding the coverage of HIPAA protections will naturally increase the enforcement complexity and burden on the government agencies responsible for overseeing compliance. It is crucial to ensure that if the scope of HIPAA protections is extended, commensurate resources are allocated to enforcement. This is essential to transform the reforms into meaningful and effective protections for health data.

5. Are existing safeguards on the disclosure of health care data to law enforcement officials sufficient?

The safeguards proposed in the Office for Civil Rights (OCR)'s recent Notice of Proposed Rulemaking (NPRM), particularly those related to preventing disclosures to law enforcement for services that are lawfully rendered in the jurisdiction, appear to be a positive step in balancing healthcare data privacy and law enforcement's need for information. Therefore, the EHR Association supports finalizing this proposed rule.

There is a question surrounding whether health information could be considered self-incrimination, which is constitutionally protected. The EHR Association notes that clear guidance is necessary regarding when and how health data can be used against a patient, to ensure that health data is appropriately handled concerning constitutional rights.

6. How should the sharing of health data across state lines be structured to account for different legal frameworks?

Avoiding overly detailed restrictions that vary from state to state is key to simplifying the data-sharing process and ultimately improving patient care.

HIPAA should play a central role in standardizing the data-sharing framework across states. This standardization should include a consistent set of consent expectations and restrictions on how states can impose additional data-sharing rules within a unified framework to ensure the feasibility and efficiency of data sharing. Much like standardized train tracks ensure seamless travel between states, a consistent framework for data sharing allows for interoperability across state lines.

It is essential to differentiate between use cases that are necessary for data exchange across states and areas where states may have more flexibility to impose additional restrictions or share data more liberally. This differentiation helps strike a balance between ensuring data exchange for critical healthcare needs while respecting states' rights to define specific data-sharing rules based on their unique legal frameworks.

A valuable starting point for standardizing data sharing across states could be the examples provided in the recent NPRM by the OCR. These examples offer expectations for how data sharing can function effectively across varying state laws, providing a foundation for uniformity.

## Collection of Health Data

1. How should consumer/ patient consent to an entity to collect information be structured to minimize unnecessary data gathering? When should consent be required and where should it be implied?

Implementing standardized consent expectations is a practical approach to ensure consistency and clarity across various entities collecting health data and would help to reduce burden on healthcare providers and software developers. These standards should prioritize transparency, making it clear to patients in plain, easily understandable language to ensure patients fully comprehend how their data will be collected and used.

Consent processes should be designed to be low-burden and easily digestible by patients. They should not require patients to wade through lengthy documents or click through numerous paragraphs of legalese. Optimally, the process could include a brief, plain-language overview that clearly outlines what patients are consenting to. Simultaneously, they should ensure that patients do not experience "consent burnout" from having to repeatedly navigate opt-out processes or make decisions that have an ambiguous impact on their privacy.

With respect to Personal Health Information (PHI) regulated under HIPAA, the current regulatory scheme provides an effective consent framework that minimizes unnecessary data gathering, allows patients to exercise appropriate levels of autonomy over their PHI, and facilitates healthcare research and innovation.

- HIPAA provides clear parameters for when express consent is required (e.g., sale of PHI, use of PHI for marketing purposes) and outlines exactly what must be contained within such consent/authorization.
- HIPAA identifies scenarios in which explicit consent is not the appropriate legal basis for data gathering (e.g., for treatment, payment, and healthcare operations), provided patients have received and agreed to a Covered Entities' HIPAA-mandated Notice of Privacy Practices.
- HIPAA has established an effective and time-tested consent framework for the use and disclosure of PHI for research purposes, which recognizes both the importance of patient control over their data and the need to facilitate healthcare research.

2. How should information about data collection practices be conveyed to patients (i.e., plain language notice prior to consent, etc.)?

To effectively communicate data collection practices to patients, it is crucial to strike a balance between transparency and simplicity. Upfront, clear explanations in plain language about how data will be used should be provided. The initial consent process can be simplified by starting from the premise of presumed consent in cases where an individual would choose to use an app, smart device, or other service that collects their data. One approach is to offer an easy opt-out option, assuming patients are generally comfortable with data collection, but respecting individual preferences. To the extent consent is the appropriate legal basis for data collection, consent preferences should be easily accessible for patients to manage, allowing them to easily modify data-sharing choices. This approach ensures patients can make informed decisions about their data while facilitating straightforward and convenient consent procedures.

3. The European Union (EU) General Data Protection Regulation (GDPR) requires entities that collect personal data to delete it under certain circumstances if a consumer makes such a request. Should non-HIPAA-covered entities be required to delete certain data at a consumer/patient's request?

The right to delete data should be contingent on how essential that data is for ensuring the safety and quality of future patient care. If the data plays a crucial role in delivering safe and effective care, it may not be practical or advisable to allow for its deletion. However, in situations where the data no longer serves a purpose in the patient's care or treatment, it could be reasonable to consider requests for deletion.

## **Biometric Data**

1. To what extent should biometric data be considered health care information when not used for health care purposes?

In many cases, the distinction between health care and non-health care purposes can be blurred, and these purposes can transition rapidly. Therefore, the EHR Association suggests it may be more practical to regulate data protections based on the type of data itself rather than attempting to delineate specific use cases. By focusing on the inherent nature of the data and ensuring robust protections regardless of the context, we can better safeguard individual privacy and maintain data security.

## **Genetic Information**

1. How should genetic information collected by commercial services be safeguarded?

The difference between "commercial services" and healthcare is unclear – as is the significance of the distinction. The EHR Association suggests treating individually identifiable genetic data as health data and applying appropriate protections accordingly.

## **Location Data**

1. How should location data that is being collected at a healthcare facility or website or other digital presence maintained by a healthcare entity be treated? For example, location data could potentially disclose a patient's health condition or treatment plan. Should this data be treated differently from the same data collected by non-healthcare entities?

Location data that reveals individually identifiable information related to an individual's past, present, or future behavioral or physical health or health conditions (such as the collection of an IP address for a patient signing into a dialysis care patient portal or location services that indicate when a patient has arrived at a clinic) should be classified as health data. Such data warrants the corresponding level of protection and security measures to ensure patient privacy.

## **Financial Information**

1. How should financial information for health care services not covered by HIPAA (i.e., claims data, billing) be treated?

Claims data and billing information are already considered health information regulated by HIPAA. To the extent that other financial information would be used to provide healthcare services to individuals, it would be regulated by HIPAA. Other financial information should not

be regulated by HIPAA and should instead continue to be regulated by other financial privacy rules.

## Sharing of Health Data

1. Should there be an opt-in method of data collection for health data outside of the HIPAA framework versus an opt-out method? Please explain.

When individuals actively choose to use a particular product or service, there may not be a direct need for opt-in or opt-out mechanisms. The act of choosing to use the product or service inherently implies consent for data collection, given that individuals are making a conscious decision. In such cases, the primary emphasis should be on transparency and providing clear, plain-language explanations regarding how health data will be collected and used.

However, in situations where individuals do not make an explicit decision to use a product or service, but health data would still be collected, it becomes crucial to notify the individual about this data collection. In these cases, individuals should have the opportunity to opt out if they have concerns about their health data being collected without their active consent. This approach respects individuals' autonomy and privacy while ensuring that they are aware of and can control the collection of their health data in situations where they might not have initially opted in.

2. HIPAA permits the sharing of protected health information (PHI) under limited circumstances, provided the information is de-identified. Should this permissive framework be extended to the sharing of non-HIPAA-covered data and what guardrails should be imposed?

If HIPAA's scope is expanded to encompass additional types of entities that handle health data, it is logical and consistent to subject these entities to the same expectations for de-identification.

3. Which, if any, obligations imposed on HIPAA Covered Entities should also be imposed on non-HIPAA Covered Entities handling health data? Please explain.

Obligations that are imposed on HIPAA Covered Entities should also be extended to non-HIPAA Covered Entities that handle health data. HIPAA establishes a robust baseline of expectations for the handling of health data, and these should be applied uniformly to safeguard health information regardless of the entity's regulatory status.

## Artificial Intelligence

1. What privacy challenges and benefits does the use of artificial intelligence pose for entities that collect, maintain, or disclose health care data, whether within the HIPAA framework or without?

One key challenge of artificial intelligence (AI) in the context of health care data is that AI systems may be trained on datasets that include identifiable health information, which can complicate the de-identification of health data. This poses a significant privacy risk as it may increase the potential for data breaches or re-identification of individuals.

New frameworks should be designed to assess the privacy risks associated with AI applications, ensuring that they are used responsibly and with adequate safeguards. Guardrails must be put in place to mitigate these risks, such as robust data anonymization techniques and stringent security measures.

2. How should artificial intelligence-enabled software and applications implement privacy by design? What can be done to mitigate privacy vulnerabilities when developing algorithms for health care purposes?

Privacy by design in artificial intelligence-enabled healthcare software and applications can be implemented by ensuring that data used for AI model training cannot be used to re-identify individuals. An effective strategy for mitigating privacy vulnerabilities is a risk-based approach, akin to existing HIPAA risk assessments, that analyzes the privacy threats posed by AI and implements guardrails to mitigate risks.

3. To what extent should patients be able to opt out of datasets used to inform algorithmic development? How could an opt-out mechanism be structured?

Opt-outs should be structured to enable patients to prospectively opt out of a dataset used to inform algorithmic development when identifiable health data is involved. However, if the training of an AI model or algorithm exclusively depends on de-identified data or a limited dataset, patients should not have the option to opt out, provided that the algorithm is not to be used for patient re-identification purposes.

## State and International Privacy Frameworks

1. Currently, 137 countries have a data or privacy framework in place. What have been the greatest challenges in complying with these frameworks for the governance of health data? Are there any policies that have been effective in safeguarding health data? What should be improved? How should the United States proceed, considering the existing international patchwork?

One of the primary challenges is the lack of coordination between countries, which hampers cross-border data exchange critical for improved treatment and research. To address this, there is a need for greater international coordination, including alignment in regulatory definitions and the establishment of common technical standards for data exchange.

Privacy laws that necessitate data segmentation have also posed substantial challenges. These laws hinder progress in interoperability and often create barriers to designing innovative tools that could enhance healthcare and prevent harm. To safeguard health data more effectively, policies should be revised to strike a balance between data protection and facilitating responsible data sharing for medical advancements.

The U.S. should explore ways to streamline privacy regulations and data segmentation requirements, ensuring that they do not unduly impede the development of innovative healthcare solutions and the sharing of critical health data for the benefit of patients worldwide.

2. Nine states have passed data or privacy laws since 2018. What have been the greatest challenges in complying with these frameworks for the governance of health data? Have there been any lessons learned as states have implemented these laws on best practices to safeguard health data? How should the federal government proceed, considering the existing state patchwork?

The greatest challenges in complying with the data and privacy frameworks for the governance of health data include the fragmentation of requirements imposed on health systems and EHR developers and the resulting technical implications that add complexity and cost (and frequently cause confusion). While many of these state laws are well-intentioned, they often become overly specific or yield unintended consequences that can hinder providers' ability to access complete medical histories or utilize advanced health IT tools effectively.

Extending the privacy requirements of HIPAA to entities that are currently not regulated by HIPAA would raise privacy standards in a way that will potentially eliminate the need for disparate state laws. This would create a more cohesive and effective approach to health data governance, benefitting both providers and patients while reducing regulatory complexity.

## **Enforcement**

2. OCR has primary authority over enforcement of HIPAA. However, other federal agencies such as the Federal Trade Commission (FTC) have oversight of certain health data that can implicate HIPAA. To what extent should these agencies have a role in the safeguarding of health data? What duplication or conflict currently exists between how different agencies enforce violations of health laws?

Having a single framework to enforce privacy and security requirements for health data would streamline enforcement and clarify expectations for all involved stakeholders. Individuals often struggle to discern when their health data is protected by HIPAA and when it falls outside its scope, if they understand that at all, and this can lead to frustration during the enforcement process. By unifying the expectations for safeguarding health data and standardizing enforcement, we can provide greater clarity and simplicity, benefiting both individuals and organizations handling health data.