September 28, 2023

The Honorable Bill Cassidy
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate
Washington, DC 20510

Dear Senator Cassidy:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to provide written comments in response to the request for feedback on how to leverage technology to improve patient care, while safeguarding the privacy of protected health information (PHI). We appreciate this opportunity to utilize our members' expertise in offering feedback on this request for information with the goal of developing and maintaining a global transparent trust framework through awareness, management, enforcement, and refinement of uniform privacy principles and risk-based security practices. We look forward to continued dialogue with the Committee on these important topics.

HIMSS is a global advisor, thought leader and member-based society committed to reforming the global health ecosystem through the power of information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research, and analytics to advise global leaders, stakeholders, and influencers on best practices in health information and technology driven by health equity. Through our innovation engine, HIMSS delivers key insights, education and engaging events to healthcare providers, governments, and market suppliers, ensuring they have the right information at the point of decision. HIMSS serves the global health information and technology communities with focused operations across North America, Europe, the United Kingdom, the Middle East, and Asia Pacific. Our members include more than 125,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations. Our global headquarters is in Rotterdam, The Netherlands and our Americas headquarters is in Chicago, Illinois.

General Privacy Questions and Health Information Under HIPAA

HIMSS has a long history of contributing feedback to the federal government as it updates and addresses necessary modifications to health data privacy. Nearly thirty years have passed since the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted. In this time, we have seen dramatic changes in technology and data usage. As innovations are introduced to healthcare, the manner in how the government regulates data privacy will need to evolve   Our goal is to find a balance between removing barriers, while ensuring the confidentiality, integrity, and availability of patient data.

Our nation needs a robust, comprehensive privacy law that is universally implementable, applicable to all entities that access protected health information regardless of site or platform and offers the flexibility that may be required to deliver appropriate care to an individual.

How HIPAA is interpreted, enforced, and intersects with other privacy laws has created significant layers of complexity in compliance and enforcement. Given the current technology landscape, and the emerging roles of entities that handle personal health information that falls outside the scope of HIPAA privacy and security requirements need to be broader and more encompassing. The explosion of health apps and other direct-to-consumer health technologies, such as fitness trackers, lead to an increase in both the amount of health data collected from consumers and the incentive for companies to use or disclose that sensitive data for marketing and other purposes. Actors who access PHI but operate outside of HIPAA's purview should be required by applicable federal laws to protect personal health information, notify impacted parties in a timely manner when a breach occurs, and take appropriate action to mitigate the impact of the breach consistent with the manner HIPAA-covered entities are required.

Currently, several regulatory agencies have jurisdiction over personal health information. The FTC covers "personal health records" accessing personal health information that are outside of HIPAA's scope. The HHS Office of Civil Rights (OCR) and the Substance Abuse and Mental Health Services Administration (SAMHSA) oversee personal health information compliance requirements related to substance abuse treatment and mental health. All data covered under these three areas of scope should encompass a broader category of personal health information, regardless of the platform or manner the way the data is transacted and should have and aligned and appropriate privacy and security framework and breach notification responsibilities.

HIMSS also supports patients and authorized caregivers having broad access to their data to become knowledgeable partners in their care and wellness. However, there are situations where data may typically be subject to a specific authorization, in writing, which may not always be realistically maintained. This can present a barrier to the patient getting the right treatment at the right time. We support legislation that maintains a balance between what is required or permitted to be disclosed and used with what is realistic in times of emergent circumstances. For example, the data subject is not always able to provide a specific written authorization in every instance and/or it may not be feasible to obtain the authorization. That said, we do not believe in oversharing or overuse of information considering the patient's rights to privacy and to otherwise ensure that the personal information is not misused, especially if this is not in the best interest of the patient.

Biometric, Genetic, Location, and Financial Data

As noted in the previous section, HIMSS calls for consistent standards to protect all identifiable patient information; biometric, genetic, location, and financial data should have the same protections as those afforded for other forms of PHI. HIMSS acknowledges that states can mandate additional protections regarding the robust protection of biometric information, such as the Biometric Information Privacy Act, but federal law should align requirements across federal entities, ensuring a minimum baseline detailing the responsibilities of actors creating and accessing patient data, breach notification requirements, and required corrective actions.

Sharing of Health Data

As a matter of principle, HIMSS believes that seamless, secure, ubiquitous, and nationwide data access and interoperable health information exchange should ensure the right people have the right access to the right health information in a usable format at the right time to provide the optimal level of care. Reducing barriers to the appropriate exchange of health information through harmonizing privacy and security laws, regulations, directives, and industry-led guidelines is paramount to transforming the health ecosystem, modernizing care delivery, driving health innovation at the institutional and personal level, and enabling health research.

To facilitate this goal while protecting patient privacy, HIMSS has consistently recommended using opt-out mechanisms for patients who choose for their data not to be included in electronic exchange or for use in data sets. Opt-out should be applicable to all HIPAA covered entities and non-HIPAA covered entities who access protected patient information. For example, HIMSS supported the Department of Veterans Affairs transition to an opt-out methodology, as their opt-in mechanism created a significant amount of burden with little benefit to patient privacy. The Department of Veterans Affairs found that opt-in required every patient to be trained on the ramifications of opt-in on an annual basis. This is consistent with, for example, VA Form 10-10164 ("Opt-out of Sharing Protected Health Information through Health Information Exchanges").

HIMSS acknowledges that the European Union General Data Protection Regulation (GDPR) requires explicit consent, *inter alia*, for the processing of those personal data for one or more specified purposes pursuant to Article 9. However, the US healthcare system features significant differences from the European Union, and opt-in requirements will create significantly more burden for providers with little benefits to patients.

Artificial Intelligence and Patient Privacy

HIMSS appreciates the Committee's including the impact artificial intelligence and machine learning will have on privacy in the RFI. Understanding and harnessing AI and ML have become increasingly important for our membership, and have been topics of great discussion at each of our HIMSS23 conferences around the globe. The use of artificial intelligence (AI) poses the following privacy challenges for entities that collect, maintain, or disclose health care data:

- Informed Consent: By its nature, AI produces a model based on algorithms that are trained on data sets. One of the primary principles of informed consent is that an individual must be made aware of the nature and purpose of the AI application, in addition to its benefits, risks, and limitations – especially when compared to traditional

(I.e., non-AI based) methods. A patient may or may not be capable of understanding the possibility of data being used by AI if the model transitions beyond the model's original intended use, and second, an organization may or may not be able to define the purpose of the data and how it will be used. Collecting data for training AI sometimes amounts to mixing an individual's data with others' data and seeing what happens. That ill-defined outcome conflicts with a person's ability to truly offer informed consent and a basic data governance principle of "collecting data for a defined purpose.

- Maintaining Anonymity/Privacy: Ensuring that protected health information has truly been de-identified continues to be a challenge for the healthcare community. Some researchers have demonstrated that it is possible to re-identify data using one or more sources of publicly available data. Using techniques including, but are not limited to, data linkage attacks and inference attacks, (Model inversion attacks may also be used on AI models to discern the original training data), it is possible to re-identify information. Large clinical data sources present attractive targets for these kinds of attacks.

AI can also enhance privacy protection for entities that collect, maintain, or disclose health care data. Thoughtfully constructed, AI can enhance privacy through:

- Advanced Data Protection: AI tools can prevent data theft and nefarious activity. AI can detect and proactively block potentially anomalous network traffic.

- Better Deidentification: Specific to the data identification challenge above, AI tools can assist in providing more rigorous de-identification of health information.

State and International Privacy Frameworks

Many companies have started to migrate information and data to cloud based settings. Many of these conduct business in multiple countries and some countries prohibit offshore data storage of health data. Other countries have different regulatory requirements. The time, expense, and staff resources required to ensure compliance with disparate international requirements is burdensome to all healthcare stakeholders.

Disparate state privacy law compliance requirements create similar challenges. Conflicting privacy standards, and breach notification responsibilities create a significant burden for business associates which conduct business in multiple states, and health systems and provider practices which deliver care in multiple states. A national privacy law, as described above, that creates a baseline for privacy protections and breach notifications for both HIPAA covered entities and non-HIPAA covered actors would mitigate the burden of disparate requirements.

Several states have adopted comprehensive health data privacy laws, including the California Privacy Right Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, and the

Utah Consumer Privacy Act. These state privacy laws, and lessons learned from their implementation should be assessed when developing a national privacy law that will provide needed conformity across state and local jurisdictions. Such a national privacy law should also consider current federal requirements under the Trusted Exchange Framework and Common Agreement (TEFCA), efforts to promote data modernization for public health, and health equity initiatives.

We look forward to the opportunity to discuss these issues in more depth. Please feel free to contact David Gray, Director of Government Relations, at David.Gray@HIMSS.org with questions or to request more information.

Thank you for your consideration.

Sincerely,

Harold F Wolf

Harold F. Wolf III, FHIMSS
President & CEO