Testimony of

Tina O. Grande
Executive VP, Policy, Healthcare Leadership Council and
Chair, Confidentiality Coalition

Before the
House Committee on Veterans' Affairs
Subcommittee on Technology Modernization

Data Privacy and Portability at VA: Protecting Veterans' Personal Data.

February 12, 2020

Chairwoman Lee, Ranking Member Banks, and Members of the House Committee on Veterans' Affairs Subcommittee on Technology and Modernization (Subcommittee), thank you for the opportunity to testify today.

My name is Tina Grande. I am Executive Vice President of Policy of the Healthcare Leadership Council (HLC) and Chair of the Confidentiality Coalition (Coalition).

HLC is a coalition of chief executives representing all disciplines within American healthcare, including hospitals, academic health centers, health plans, pharmaceutical companies, medical device manufacturers, laboratories, biotech firms, health product distributors, post-acute care providers, home care providers, and information technology companies. It is the exclusive forum for the nation's healthcare leaders to jointly develop policies, plans, and programs to achieve their vision of a 21st century healthcare system that makes affordable high-quality care accessible to all Americans.

The Confidentiality Coalition, founded to advance effective patient confidentiality protections, is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others. The Coalition's mission is to advocate for policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions. I have attached to my testimony information about the Coalition, HLC and the membership of each.

Through the breadth and diversity of our membership, HLC and the Coalition are able to provide a broad-based and nuanced perspective on any legislation or regulation affecting the privacy and security of health consumers. We work closely with key legislators and regulators to help strike the right balance between protecting privacy and allowing the appropriate sharing of health information to ensure safe, high-quality, and coordinated healthcare.

We understand that the Subcommittee is examining how the Department of Veterans Affairs (VA) manages veteran's data, including interoperability, privacy and security issues, in light of the challenges posed by changes in technology and the increasing monetization of data.

This examination is especially timely as new technologies are being marketed every day that allow for not only the generation of new data not previously available, but the ability to transmit and share data more easily, and to use it for purposes as varied as targeted advertising to developing artificial intelligence (AI) tools for the early detection of cancer and other debilitating diseases. For every promising health information technological development there is the risk of its misuse, and as the value of data increases, so does the incentive to misappropriate it. The more consumers are able to control and direct the sharing of their health data, the greater the likelihood of the data finding its way into the hands of third parties not committed or bound to protect it.

The Coalition's members having been grappling with these same challenges as they seek to use data to improve healthcare outcomes, quality and efficiencies, and to facilitate data sharing among patients, healthcare providers and other healthcare organization. Congress too, through the 21st Century Cures Act, has sought to address some of these challenges by directing the Department of Health and Human Services (HHS) to implement regulations to advance interoperability, support patient access to their electronic health records, and eliminate information blocking.

While these steps are laudable and essential, there remains the glaring oddity in our current health data regulatory scheme that certain health data is subject to robust federal privacy protections while other health data is not. As long as this disparate treatment exists, the challenges faced by an organization such as the VA to manage health data in a way that harnesses new technological innovations while maintaining the privacy and security of all this data will remain formidable, if not insurmountable.

My testimony, therefore, focuses on how this regulatory gap should be addressed, and the principles that we believe the Subcommittee and others in Congress should consider in seeking to ensure that all consumer health data is appropriately protected while at the same time being available as seamlessly as possible for necessary healthcare functions and activities.

Health data that is governed by the Health Insurance Portability and Accountability Act (HIPAA), including data held by VA covered entities, is protected by a framework that has for over 20 years provided individuals with strong privacy rights and protections.

HIPAA's well-established rules and guidance, together with its robust and consistent enforcement by HHS, has made it a trusted and accepted national standard for the protection of personal health information. It has also provided HIPAA covered entities and their business associates with a clearly delineated framework and parameters within which to operate. Therefore, any approach to health data privacy should preserve the existing HIPAA framework, and new legislation should apply only to health data not governed by HIPAA.

We support the development of new health information technologies, whether at the consumer level in the form of mobile health apps and wearable devices, or at the enterprise level, such as sophisticated new tools that aggregate and analyze vast quantities of data that can transform healthcare. These new innovations in health information technology are not only empowering consumers to be more engaged in managing their health outside of traditional healthcare settings, but are enabling healthcare organizations to develop new treatments and cures that will deliver enormous benefits to patients and greatly improve our healthcare system.

These innovations have also resulted in more and more health data falling outside the protections of HIPAA. This will be the case when the technology or services are not offered by or on behalf of a HIPAA covered entity, but rather, by developers or technology companies directly to the consumer. For example, a consumer may download a third party app to their smartphone that tracks diet, exercise and weight, and uses the app to send a summary report to their doctor before their next appointment. As long as the doctor did not hire the app developer to provide its services to the doctor's patients, the data in the app is not protected by HIPAA, even if the app is recommended by the patient's doctor.[1]

Today, consumers may not fully appreciate which of their health data is collected by an entity subject to HIPAA, and so protected by HIPAA, and which is not. To the extent personal health information is not already covered by HIPAA ("non-HIPAA health data"), privacy and security rules comparable to HIPAA should apply to it. This is not only vital to maintain consumer trust, but also necessary to honor the rightful expectations of all consumers that their health information, among the most sensitive of personal information, is appropriately safeguarded, and that they may exercise the same types of privacy rights with respect to it as they enjoy with respect to data covered by HIPAA. As the Subcommittee continues to assess the management of veterans' health data, we are pleased to share the Confidentiality Coalition's "Beyond HIPAA" Privacy Principles that outline our views on the protection of non-HIPAA health data. A copy of these principles is attached to my testimony.

[1] See The Department of Health and Human Services Office of Civil Rights Guidance documents, Health App Use Scenarios & HIPPA. February 2016 ("Developer is not creating, receiving, maintaining or transmitting protected health information (PHI) on behalf of a covered entity or another business associate. The doctor's recommendation implies her trust in the app, but there is no indication that the doctor hired the app developer to provide services to patients involving the handling of PHI. The consumer's use of an app to transmit data to a covered entity does not by itself make the app developer a [business associate] of the covered entity.")

The Coalition believes that any federal legislation to protect non-HIPAA health data should do so in a manner that harmonizes with the existing HIPAA framework. This includes HIPAA's implied consent for the use and disclosure of health information for treatment purposes, and minimum necessary information for payment and health care operation purposes. It also includes the requirement to obtain an individual's written authorization to use or disclose their protected health information (PHI) for marketing purposes or to sell their PHI. HIPAA authorizations put individuals on notice that, once disclosed, their data may no longer be protected by HIPAA. They also require HIPAA covered entities to be transparent and disclose if their marketing communications are funded by the entity whose product or services are being marketed. In addition, covered entities are required to provide individuals with a notice of privacy practices that describes the entity's privacy practices, the purposes for which it uses and discloses PHI, and the individual's privacy rights and how to exercise those rights. This transparency is an important protection that is particularly relevant as businesses seek to monetize health data.

At the same time, the HIPAA framework recognizes that health information is not a commodity, the flow of which is determined by the highest bidder. Great care was taken when establishing the HIPAA framework to balance various competing interests -- the privacy rights of the individual, the public interest served, the need for information to be used for essential health activities consistent with consumer expectations, and the burden on covered entities – and HHS repeatedly cited this balancing approach when it first issued its Privacy Rule[2] and in subsequent modifications to it. This same approach should be taken in addressing non-HIPAA health data.

Harmonization, including alignment with HIPAA concepts, definitions and standards, is critical to provide consumers with the assurance of consistent protection of all their health information, and to ensure the appropriate exchange of health information by health organizations, whether covered by HIPAA or not, is not impeded. For example, even as seemingly technical an issue as the definition of de-identified data could have potentially major ramifications if the HIPAA definition is not used. This is because data that is considered de-identified under HIPAA may not be considered de-identified under a new law and so potentially not covered by it. The unintended consequence of this is that it could seriously and adversely impact the ability of healthcare organizations to aggregate and share health data for important public policy purposes such as developing evidence-based standards, quality metrics and standards, medical research, and management of healthcare delivery, to name only a few.

The same can be said for other HIPAA definitions and concepts, including permissible uses and disclosures without explicit authorization, the requirement to be transparent

[2] See, for example, 65 Fed. Reg. 82462 (December 28, 2000) at 82464 ("The rule seeks to balance the needs of the individual with the needs of the society"); 82468 ("The task of society and its government is to create a balance in which the individual's needs and rights are balanced against the needs and rights of society as a whole"); 82471("Neither privacy, nor the important social goals described by the commenters, are absolutes. In this regulation, we are asking health providers and institutions to add privacy into the balance, and we are asking individuals to add social goals into the balance"); and 82472(" The need to balance these competing interests—the necessity of protecting privacy and the public interest in using identifiable health information for vital public and private purposes—in a way that is also workable for the varied stakeholders causes much of the complexity in the rule").

about uses and disclosures in the form of a notice of privacy practices, and the right of individuals to access and receive portable copies of their electronic health records, among other things. Aligning any new legislation to govern non-HIPAA health data with the HIPAA definitions and requirements will also provide consumers with a more coherent and seamless privacy framework, allowing them to more easily understand how their health data is protected and exercise their privacy rights.

Equally important, security safeguards should be commensurate with the safeguards required by the HIPAA privacy and security standards. These require reasonable and appropriate administrative, technical, and physical safeguards to protect the confidentiality of all protected health information, and the integrity and availability of electronic health information. Like the HIPAA Security Rule, any security standard should be technology neutral, scalable, and allow for a flexible risk-based approach. Robust security requirements for non-HIPAA health data are critical not only for large and sophisticated businesses that collect vast amounts of data, but also for smaller companies and start-ups developing new products and services, which should be incorporating security-by-design practices in their product development process. Whether their personal health data is covered by HIPAA or not, consumers should know that those to whom they entrust this data will keep it secure in accordance with well-vetted and accepted national security standards.

The Coalition strongly supports efforts to increase interoperability to facilitate the appropriate sharing of health data among healthcare organizations, as well as the access and availability of electronic health records to consumers themselves. This is another reason to ensure harmonization between laws governing PHI and non-HIPAA health data and to have national standards for health information privacy and security. The great promise of interoperability – using technology to engage patients, deliver meaningful insights to help in the identification and diagnosis of disease, and guide treatment decisions - depends on the ability to appropriately share health data among HIPAA covered entities and others for these purposes. This promise cannot come to fruition if these organizations are subject to, and constrained by, different standards that do not align or, potentially even conflict, with one another. This has proven to be a challenge for the appropriate sharing of patient substance use disorder information. The investment of effort at the outset when crafting legislation so as to avoid this type of misalignment will yield significant dividends in the form of improved healthcare outcomes and quality of care, not to mention a more seamless and workable privacy framework for veterans, healthcare organizations and service providers. This is particularly pertinent today as the Administration seeks to execute on the requirements of the 21st Century Cures Act to improve health information interoperability with the goal of promoting greater data sharing among patients, healthcare providers, payers, researchers, and other healthcare entities. As the Office of the National Coordinator of Health Information Technology stated in its recently released draft 2020-2025 Federal Health IT Strategic Plan:

[N]ew technologies, along with existing claims and EHR data, mean that the volume of health and health-related data being generated and available for improving care quality

has never been greater. Collecting, organizing, analyzing, interpreting, and applying this "big data" to clinical decision making is both a challenge and a significant opportunity.[3]

For the same reasons, as healthcare organizations make the transition to a nationwide, interoperable system of electronic health information, we believe it is essential to replace the current mosaic of sometimes conflicting state privacy laws, rules, and guidelines with strong, comprehensive national standards.

In closing, the HLC and Coalition commend the Subcommittee for seeking to address the challenges faced by the VA in managing veterans' health data in a world where the value of this data has never been greater, the risks posed to it more serious, or the opportunities for its beneficial use more abundant. We believe a balanced approach, compatible with and modeled upon the existing HIPAA framework, and that provides protections for non-HIPAA health data similar to that provided for PHI under HIPAA, is the best way to address these challenges and provide a comprehensive, consistent and transparent health information privacy framework for the health data of those in service and beyond.

Attachments

[3] See The Department of Health and Human Services Office of the National Coordinator of Health Information Technology document, 2020-2025 Federal Health IT Strategic Plan. January 2020