Testimony before the United States House of Representatives

Committee on Veterans' Affairs

Subcommittee on Technology Modernization

Hearing on "Data Privacy and Portability at VA: Protecting Veterans' Personal Data"

February 12, 2020

Statement of Harold F. Wolf III

President & Chief Executive Officer

Healthcare Information and Management Systems Society

Chairwoman Lee, Ranking Member Banks and Members of the Subcommittee - thank you for the opportunity to testify today on behalf of the Healthcare Information and Management Systems Society (HIMSS) on how to safely and securely manage veterans' health data.

My name is Hal Wolf, and I am the President and Chief Executive Officer of HIMSS. I represent more than 80,000 members globally who are dedicated to transforming the health ecosystem through 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. Headquartered in Chicago, Illinois, 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.

We appreciate the Committee holding today's hearing on "Data Privacy and Portability at the VA: Protecting Veterans' Personal Data." Today's hearing around the role of Congress and the Department of Veterans Affairs in ensuring the confidentiality, integrity, security, interoperability, and availability of patient data reflects a larger conversation occurring across the healthcare ecosystem. Namely, as the significant investment in technological advancements in healthcare now allows us to capture and use data and the ensuing information it provides in unprecedented ways, to realize the full potential of that data to improve health outcomes, we must ensure the proper processes around privacy and security are in place to protect the patient's most sensitive data and information.

Before joining HIMSS, I served at The Chartis Group as Director; Practice Leader of Information and Digital Health Strategy, and prior to that I was Senior Vice President and Chief Operating Officer of Kaiser Permanente's The Permanente Federation. During this time, I was responsible for the development and implementation of critical care delivery strategies, data management and governance, population care management environments and the implementation of unique innovations and large-scale programs that impacted end-to-end operations. Critical to the innovations introduced within these functions was maintaining the security and protection of the confidential information entrusted to us by our patients. These responsibilities require the same vigilance in all systems undergoing strategic change.

Changes in the Digital Health Ecosystem Driving Data Availability, Access, and Use

Our healthcare ecosystem is undergoing a profound transformation that is increasing pressure on all stakeholders to drive innovation. A significant piece of that change is in the digital health space,

particularly around the need to provide patients access to and use of their data and information to derive meaningful benefits for their own health.

As a matter of principle, HIMSS firmly 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.

However, until you take data, that is essentially ones and zeros, categorize it, and put it into digestible pieces to create information, we do not have the ability to use it in the way that we want. Data alone isn't the solution – it is fundamentally useless until you turn it into information.

For example, the health app on your smartphone takes data and turns it into information that is then used by the individual. Subsequently, when you do a comparative analysis, that information becomes knowledge that can provide real health benefits to the patient and to the ecosystem at large.

As we transition from volume to value-based care to achieve the goals of improved care outcomes, lower cost per episode, and enhanced delivery of care, technology-enabled data collection and interoperable data sharing will play a vital role in supporting these efforts. Given the large population receiving services through the Department of Veterans Affairs healthcare system, it is not a stretch to see that VA is facing the same external pressures to make more data available to and for veterans and help them better manage their health.

Technology has advanced to the point that it is ubiquitous in most healthcare interactions, and it plays such a critical role in how we connect clinicians, patients, caregivers, and applications. Further, based on the convenience of mobile apps and devices in other industries, patients are growing more sophisticated in their knowledge of the health system, and ability to understand and act upon the

information shared through these technologies. As a result, patients are more resolute in their needs and expectations—they expect the same level of access, connectedness and engagement with their healthcare that they experience in other facets of their lives.

Particularly, in the last several years, we have seen an incredible attention shift to a consumer-based approach regarding integrated care. With greater incorporation of technology into the healthcare ecosystem, and as more information becomes readily available and accessible, many in the health ecosystem have been looking toward the use of data and available information as a means to solve the multitude of problems we have in healthcare. This data is particularly important, for instance, when a patient goes for a second opinion.

The federal government, particularly the Department of Health and Human Services (HHS), Centers for Medicare and Medicaid Services, and Office of the National Coordinator for Health IT, has played a vital role in helping the healthcare ecosystem prepare for the continuing increase in data and information access and usage. Through recent proposed regulations that we believe will advance interoperability and support greater patient access to data, HHS is seeking to increase innovation and competition by giving patients and their healthcare providers safe and secure access to health information and new tools that will allow for more choice in care and treatment. The regulations also propose to adopt standardized application programming interfaces (APIs) in the healthcare industry to help allow individuals to securely and easily access structured electronic health information (EHI) using smartphone applications. This advancement places a strong focus on a patient's ability to access their health information through a provision requiring that patients can electronically access all of their EHI at no cost.

Healthcare stakeholders should demand integration among all interoperability approaches, entities, and trusted exchange frameworks, and support combining administrative and clinical data to enhance transparency and enable value-based care delivery for the public good.

Moreover, health IT systems must be designed to ensure patients and consumers are at the center of care delivery and obtain the right information at the right time to enable them to make informed decisions about the delivery and coordination of their care and seamlessly communicate with their providers.

Growing Challenges and Opportunities Around Patient's Personal Healthcare Data

Differences and Distinctions Between Data Access, Ownership, Usage and Stewardship

Any discussion around a patient's health data inevitably leads to questions around who owns the data, who can access the data, what can be done with the data once access is granted and what are the stewardship responsibilities over the data when it is in possession of any entity. . An obstacle we often hit is getting bogged down in ownership – we spend time arguing over who owns the data, resulting in an unwillingness to share. This construct does neither the patient and caregiver nor the provider any good. It is imperative that our mindset shifts to that which benefits patient or individual health, and that includes sharing across multiple platforms and systems to realize the full potential of data in improving health outcomes.

Generally speaking, **data ownership** refers to the entity or individual who owns the data. For example, in the current way of thinking, healthcare providers own the designated record set, and health plans may own the data of its members. It is important to note however, that data may not necessarily be in the "possession" of someone/something, but it can flow through an entity, for example, like a conduit. Possession does not imply ownership. Additionally, the complexity of applications, such as

electronic decision-support (EDS), use not only clinical data, but also social data such as lifestyle information to help guide individual recommendations. Those data sources can be numerous and often involve multiple pass throughs.

Data access simply refers to being in possession of data in some way. This might include the ability to read, edit, or copy data for a variety of purposes. From a security standpoint, access is controlled according to rules based on "need to know." Access control is frequently based on the role of the person requesting the data. Thinking beyond individual access - it isn't just a person who may have access to the data, but also an entity, such as an intelligent artificial agent that performs tasks on behalf of a larger entity such as a health system. And access control issues are further nuanced, moving beyond who has the need or right to access the data to include the more important concept of what that person or entity can do with the data once in their possession. This idea of what can be done with the data falls to the concept of data usage – which is where I think the conversation should center.

Data usage is basically the rules and rights of how the data can be appropriately stored, movement of the data, and its secondary use both short and long term. Rules around usage have impact on many areas such as secondary research, resale of data for commercial purposes as well as impacts on access hierarchy as mentioned above. The goal of data usage is to achieve the greatest possible benefit that may be realized from the effective and appropriate access to the data, while, at the same time, protecting the rights of the individual and originating data entity.

Data stewardship focuses on minimizing the risk to patients and to the organization in both the access and use of the data by providing a secure and trackable environment. Cybersecurity is an important component of data stewardship. Data use and stewardship falls squarely in the realm of governance.

Personal Healthcare Data– Who has access? Who should have access? Who shouldn't?

It is safe to say that there is nothing more personal and valuable to an individual than their health information. When you look at the fact that healthcare, which is the largest industry in the world from a Gross Domestic Product standpoint, is being driven by data and the use of information, it stands to reason that the information and data held by this sector is a valuable asset. Data has to be protected at the human level, and the economic level, which creates complications. In order to ensure that both veterans and broader patient populations receive the best possible care, providers, patients, and caregivers must be able to access the right information at the right time to allow for the most accurate decisions about the delivery and coordination of care for our veterans.

There are several public policy levers in place that the Department and the veteran community can leverage to achieve true data access and use by this population. Alignment of data access and use paradigms across VA as well as the broader healthcare delivery system will prove beneficial to veterans that receive some care in VA facilities, but also utilize community providers.

The Health Insurance Portability and Accountability Act (HIPAA) remains an integral part of our nation's information security and privacy infrastructure for both veterans and the broader patient and consumer populations. A Proposed Regulation with changes to HIPAA is under development in the HHS Office for Civil Rights. With respect to the public dialogue on possible HIPAA changes, HIMSS has focused on encouraging the safe portability of data. Specifically, HIMSS believes:

- It is imperative that HIPAA Regulations work in concert with the 21st Century Cures Act Information Blocking Rules
- Any Changes to HIPAA Rules Should Prioritize the Needs and Role of the Patient in Care Coordination Activities

- Rule Modifications Should Ensure Alignment and Eliminate Regulatory Gaps Between HIPAA and State Laws as well as Other Measures
- HHS Must Redouble Efforts to Educate the Public and Providers About the Scope and Reach of HIPAA

Ultimately, HIMSS would like to keep HIPAA focused on articulating the standard ways that individuals' health information is to be used and disclosed. Our broader perspective on interoperability remains focused on ensuring the right people have the right access to the right health information at the right time. While we have made great strides over the past generation, seamless, secure, nationwide interoperable health information exchange has continued to elude us. Ensuring that VA continues to build on the advances undertaken by HIPAA as well as other measures promulgated at HHS will be huge steps in the right direction for the veteran community and could lead the larger health ecosystem.

In addition, HIMSS wants to continue working towards creating a healthcare ecosystem that reinforces the secure access to, exchange of, and use of electronic health information. This includes building upon these existing protections and helping to ensure patient privacy as well as access in a HIPAA-regulated world and for non-covered entities under HIPAA.

Addressing Patient's Privacy and Security Concerns

We are all in agreement that patient data needs to be protected, for both information privacy and security purposes. However, healthcare delivery and coordination of care cannot be achieved without data shared in an interoperable manner across various systems. Thus, a careful balance must be made between the need to keep the data private and secure, while remaining shareable across various environments to help ensure that patient care is not impeded.

The HIPAA Privacy and Security Rules govern how protected health information may be used and disclosed, as well as how it may be secured in terms of physical, technical, and administrative

safeguards to ensure the confidentiality, integrity, and availability of information. Good cybersecurity practices help to ensure that data will indeed be kept confidential, have integrity, and be available on demand.

Cybersecurity, a key responsibility to data stewardship, is a necessary predicate to data privacy, access, and usage. These elements cannot exist were it not for cybersecurity, especially within an electronic environment. Additionally, data should be protected, not just to preserve data privacy, but also to protect the patient and preserve patient safety. Recognizing the value of such data, we need to have robust cybersecurity practices (and policies) in order to ensure interoperability of healthcare data as well. People, processes, and technology must work in tandem with each other.

HIMSS has long believed that maturing and advancing the state of the art for security and information privacy across the global health sector should be supported to: (1) protect the confidentiality, integrity, and availability of patient data and other sensitive information and assets of stakeholders, (2) ensure the continued and effective delivery of patient care and coordination of care, (3) protect patient safety and privacy, and (4) further the delivery of safe, secure, and effective technology-enabled care-delivery across disparate health systems.

I would like to thank Chairwoman Lee and Ranking Member Banks for this opportunity to testify today, and all members of the Subcommittee for prioritizing such a critical issue. The VA has no greater priority than ensuring that our veterans receive the best possible care, and this cannot be done without ensuring the safety and security of their personal data and health information.