DATA PRIVACY AND PORTABILITY AT VA: PROTECTING VETERANS' PERSONAL DATA

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION

OF THE

COMMITTEE ON VETERANS' AFFAIRS

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

WEDNESDAY, FEBRUARY 12, 2020

Serial No. 116–56

Printed for the use of the Committee on Veterans' Affairs

Available via http://govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
48–994 WASHINGTON : 2023

COMMITTEE ON VETERANS' AFFAIRS

MARK TAKANO, California, *Chairman*

JULIA BROWNLEY, California
KATHLEEN M. RICE, New York
CONOR LAMB, Pennsylvania, *Vice-Chairman*
MIKE LEVIN, California
MAX ROSE, New York
CHRIS PAPPAS, New Hampshire
ELAINE G. LURIA, Virginia
SUSIE LEE, Nevada
JOE CUNNINGHAM, South Carolina
GILBERT RAY CISNEROS, JR., California
COLLIN C. PETERSON, Minnesota
GREGORIO KILILI CAMACHO SABLAN, Northern Mariana Islands
COLIN Z. ALLRED, Texas
LAUREN UNDERWOOD, Illinois
ANTHONY BRINDISI, New York

DAVID P. ROE, Tennessee, *Ranking Member*
GUS M. BILIRAKIS, Florida
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
MIKE BOST, Illinois
NEAL P. DUNN, Florida
JACK BERGMAN, Michigan
JIM BANKS, Indiana
ANDY BARR, Kentucky
DANIEL MEUSER, Pennsylvania
STEVE WATKINS, Kansas
CHIP ROY, Texas
W. GREGORY STEUBE, Florida

RAY KELLEY, *Democratic Staff Director*
JON TOWERS, *Republican Staff Director*

SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION

SUSIE LEE, Nevada, *Chairwoman*

JULIA BROWNLEY, California
CONOR LAMB, Pennsylvania
JOE CUNNINGHAM, South Carolina

JIM BANKS, Indiana, *Ranking Member*
STEVE WATKINS, Kansas
CHIP ROY, Texas

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Veterans' Affairs are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

C O N T E N T S

WEDNESDAY, FEBRUARY 12, 2020

DATA PRIVACY AND PORTABILITY AT VA: PROTECTING VETERANS' PERSONAL DATA

WEDNESDAY, FEBRUARY 12, 2020

U.S. HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION
COMMITTEE ON VETERANS' AFFAIRS
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room 210, House Visitors Center, Hon. Susie Lee [chairwoman of the subcommittee] presiding.

Present: Representatives Lee, Cunningham, Banks, and Watkins.

Also present: Representatives Takano and Roe.

OPENING STATEMENT OF SUSIE LEE, CHAIRWOMAN

Mrs. LEE. Good morning. This hearing will come to order.

Before we get started, I want to say something briefly about the announcement by the VA earlier this week in delaying the go-live of the electronic health record project in Spokane, Washington. I have long said that getting it right is far more important than hitting a date on a calendar and, if there needs to be a delay to get the system to a place where veterans' lives are not at risk and the VA staff are ready to use it, then that is the right thing to do.

However, I am concerned that, as we move closer to the go-live date, we have been told repeatedly that there were no show stoppers in the implementation, that testing was going great, and things were on track. I get that in software development and testing conditions can change rapidly, but I require that the VA be as transparent and accountable for its actions. There are many questions that remain and the subcommittee needs answers in order to continue its oversight of the $16 billion project, especially as the President's budget proposes a speedup of the rollout.

Therefore, the subcommittee will be scheduling a hearing on this topic in the coming weeks and will request to hear from decision-makers at the VA, but now on to other aspects of VA's management of its technology portfolio.

The Department of Veterans Affairs has long struggled with aging legacy IT systems and the need to invest in new and innovative technology is necessary if the VA is going to continue delivering quality health care and benefits to our Nation's veterans. However, implementing new technology is not simply a matter of buying new software or new tools, the VA must also ensure that its policies and business rules keep pace with the changing technology and, most importantly, ensure that veterans are confident in its ability to protect their highly sensitive information.

I acknowledge that this is a difficult task, especially in the rapidly changing technology landscape. In the health care sector, the gray space in how we manage, use, and exchange data is growing more quickly than policymakers can keep up, but it is critical that we try. The VA is well situated to be a leader in this space. The electronic health record modernization initiative, coupled with this 4-year, $1 billion Department-wide technology refresh, gives the VA the opportunity to set standards in rules from the outset. The requirements will not only benefit veterans, but might also serve as a nationwide example of balancing privacy with interoperability and big-data innovation with confidentiality.

Health information and consumer data can be used to great benefit. VA's robust research and innovation programs have the potential to revolutionize care, reach more veterans, engage them in new spaces, and empower them with their own health care. Veterans can use their data to manage their care, find economic opportunity, and access the benefits they have earned; however, these advances are not without risk. The attractiveness of big data for monetary and marketing purposes is clear. In the first half of 2019, nearly 32 million health care records were breached and, as we examined at our hearing cybersecurity issues last October, that data is also attractive to bad actors that may seek to commit crimes or cause harms, as well as companies looking to monetize veterans' health information.

We cannot assume that data is safe or secure, nor do we want to keep data static to avoid any risk. However, with the changing technology landscape, we need to be deliberate in our assessment and decisions about how data is used, who gets to access it, where that access occurs, and why.

I want to hear from the VA about the process of vetting partners and vendors that participate in technology initiatives or develop apps. It seems to me that when the VA provides an app in its app store or promotes an app, a wearable device, or a medical technology, we expect the VA to assess the value of that technology or the benefit of that app and determine that the benefit to veterans outweighs the data security and privacy risk. I would like more information from the VA about this process and what it entails.

However, there is another critical question. What protections exist or should exist in the space beyond the VA? If a veteran chooses to download health information from the VA and share it with a third party, may that third party use that—or sell that information for other purposes? What responsibility does the VA have?

I am also concerned about the VA's increasingly widespread use of apps and potential risks to privacy that they pose. When a veteran downloads an app from the VA's app store, how much personal information does the VA receive, what is the process used to determine what is minimally required?

In the lead-up to this hearing, the subcommittee has studied some of VA's apps. Many require significant elevated permissions and access to a user's data or device. For example, I have a chart behind me of apps and their permissions. Here we go. The Post Traumatic Stress Disorder (PTSD) Coach requires full network access, the ability to read all of your contacts and view any file on

your phone. Concussion Coach allows access to a user's entire calendar. These permissions may be excessive and unnecessary invasion of a veteran's privacy, and may put the veteran at risk for identity theft.

Why do these apps need access to location, a user's photos, calendars, contacts, and other information? Are these permissions necessary for its function? Does requiring excessive permissions lower the app usage rates and decrease their efficacy?

In speaking with veterans and Veterans Service Organizations, I have heard repeatedly that transparency regarding data is a key concern. Here, we are also concerned about the VA's activity. The privacy policy for ACT Coach is 988 words, it is right here in the blue, of legalese with clauses about incidental or consequential damages and a non-exclusive license in consideration of your acceptance. Can we expect anyone to realistically read these and understand their terms?

I would like this to be a conversation where we can assess the data landscape at the VA and in the larger health IT space, and understand where protections exist or do not exist, and whether we need more guardrails on that data highway. We need to understand if the VA is doing enough to protect veterans' privacy or if more needs to be done. Most importantly, we need to ensure that future decisions on strengthening, keeping, or perhaps even loosening privacy rules are made in an educated manner with input from all stakeholders.

Today, we have two panels, one with VA officials, who are here now, and another with experts from health informatics, technology startup, and Veterans Service Organizations space. I look forward to engaging on these important topics and I thank all of the witnesses for being here.

I would now like to recognize my colleague Ranking Member Banks to deliver any opening remarks he has.

OPENING STATEMENT OF JIM BANKS, RANKING MEMBER

Mr. BANKS. Thank you, Madam Chair.

First of all, I want to thank all of our witnesses on both panels for joining us here today. This is a distinguished group of VA and private sector privacy experts.

On the other hand, I have to say that I am extremely disappointed that there is no VA witness here today to discuss electronic health record modernization, especially in light of the Department's recent decision to take more time to prepare for the implementation in Spokane. Dr. Roe, Mr. Watkins, and Mr. Roy and I felt strongly that the Office of EHR Modernization should be represented here today and we requested a minority witness, which the VA did not provide.

I wholeheartedly, though, support Secretary Wilkie's decision to delay. I said in our previous hearing that I was cautiously optimistic that a March 28 go-live was still achievable, but developments to the contrary over the last several months are undeniable. I am glad, though, that we will have an opportunity to question VA very soon about how exactly the additional time will be used to make the implementation more effective.

Turning to this morning's topic, there was a time when VA was a closed system that could exercise complete control of veterans' personal and health data; even then, privacy breaches happened. Many of us remember 2007 when a laptop and external hard drive containing 26 million veterans' records were stolen from a VA employee's home. Even though the records were eventually recovered untouched, the incident led to then Secretary Nicholson's resignation.

Today, small-scale privacy breaches are common in VA, as elsewhere. They are usually attributed to email phishing scams and careless document handling at individual medical centers. However, VA has not been a closed system for many years. As in sophisticated private sector health systems, personally identifiable information and protected health information are increasingly stored in the cloud and provided to external apps.

I want to say up front that I believe the Health Insurance Portability and Accountability Act (HIPAA) privacy rules need an update and I am glad to see the Department of Health and Human Services soliciting comments on how best to do it. When the privacy rule was written 20 years ago, there were far fewer entities accessing protected health information. There was a good reason to allow insurance companies and claims processors to access patient's data without written authorization every single time; there is no way our health system could function otherwise.

Today some of HIPAA's permitted purposes to access patient's records when applied in new context may become loopholes. A health care provider's business associate agreements with its partners stipulate how patient data will be used, but patients rarely have any idea what those agreements say. Similarly, health care providers' notices of their privacy practices are often vague.

The health technology landscape is evolving quickly. Mobile apps have already taken over the software marketplace and in a few years most health records will be stored in the cloud as well. It would be foolish to resist change and try to return to an earlier technology environment when fewer entities handle protected health information, privacy safeguards have to evolve as well.

As we discussed in our cybersecurity hearing in November, the health care sector has become a hacking target somewhat later than other parts of the economy. Unfortunately, for most Americans personally identifiable information and often their financial information has been exposed in a list of data breaches that are too numerous to name.

Earlier this week, Attorney General Barr unveiled criminal charges against the perpetrators of the Equifax hack of 145 million Americans' personal information. Unsurprisingly, they were members of the People's Liberation Army. It would be naive to think that China and other nation-State cyber criminals are not already targeting protected health information. Protections for health information must remain strong in the realm of cybersecurity as well as privacy. They can never be allowed to deteriorate as protections for personally identifiable information clearly have into a State of widespread vulnerability.

The question before us is whether VA has a unique role in protecting health information apart from HIPAA and other laws gov-

erning the entire health care sector, and apart from Health and Human Services (HHS). Without a doubt, VA must make smart strategic decisions with respect to its technology partners; however, I am skeptical that VA can or should drive the regulatory environment unilaterally. I look forward to exploring those issues with our witnesses here today.

With that, Madam Chair, I yield back.

Mrs. LEE. Thank you, Mr. Banks.

I will now introduce the witnesses we have on our first panel. Paul Cunningham is the Deputy Assistant Secretary, Information Security, Chief Information Security Officer and Chief Privacy Officer at the Department of Veterans Affairs.

Mr. Cunningham is accompanied by Martha Orr, Deputy CIO for Quality, Performance and Risk, Office of Information and Technology, and LaShaunne David, Director for Privacy Service, the Office of Information Security.

We will now hear the prepared statements from our panel members. Your written statements in full will be included in the hearing record, without objection.

Mr. Cunningham, you are now recognized for 5 minutes.

STATEMENT OF PAUL CUNNINGHAM

Mr. CUNNINGHAM. Good morning, Madam Chair Lee, Ranking Member Banks, and distinguished members of the subcommittee. Thank you for the opportunity to speak to you today about the Department of Veterans Affairs' mission to protect personal sensitive information of our Nation's veterans. As the VA Chief Information Security Officer and Chief Privacy Officer, I am pleased to represent the Department here today. I am here with my colleagues, Ms. Martha Orr, Deputy Chief Information Officer for the Office of Quality, Performance and Risk, or QPR, and Ms. LaShaunne David, Director of VA Privacy Service.

First, I would like to thank the subcommittee for its continued support of VA and commitment to veterans. Because of your cooperation and commitment, veterans can continue to trust VA to protect and serve their interests. As the Chief Privacy Officer, I lead VA's efforts to secure and protect veterans' personal information.

As a veteran, I have seen the value and impact VA has on so many that faithfully served. We can only provide that value through trust. That is why I am personally vested in protecting veterans' information from exploitation and misuse.

Secretary Robert Wilkie is committed to promoting innovation, transformation, and technology to enhance the veteran experience. However, large organizations like VA face challenges as they modernize their IT environments. With new technologies come new risks. VA's privacy program must adapt and remain vigilant protectors of veterans' information as an environment of greater and faster access to data emerges.

In the course of accessing VA benefits and services, veterans voluntarily share their personal information to the Department. To protect this data, VA establishes acceptable use policies, implements security controls, and proposes consequences for any violation of policy or agreement. We follow strict rules governing how

the Department creates, stores, transfers, and destroys sensitive data. QPR's Enterprise Record Service oversees these activities and Office of Information Services (OIS) VA Privacy Service helps safeguard that data by partnering with QPR to conduct privacy risk assessments, compliance monitoring of systems that contain personally identifiable information and protected health information.

The Department also implements a role-based access control system, which means that it only grants access to those who need the information to perform essential job duties or provide benefits or services. Each system is closely evaluated, equipped with appropriate access controls, and monitored for abnormal activity. When data is improperly accessed, VA takes appropriate action to limit further compromise and determine the root cause of the incident. If it is determined that human error or improper behavior is a causal factor, VA will take additional actions, including remedial training or revoking access to the user.

VA is expanding access to information for veterans, especially through new digital technologies and platforms. However, ease of access should not mean less privacy or confidentiality. VA only collects information when necessary to provide care and services. VA will never sell or share veterans' information, and will only disclose information with veterans' consent or as authorized by law. Violations of these policies will result in consequences from possible dismissal to criminal charges.

VA closely guards veterans' information; however, we often must share data with our third party partners to provide exceptional health care and benefits. In these cases, VA stipulates the term for acceptable use of VA systems and any veteran's information. Our partners must meet these requirements and protect our data as closely as we do.

As with any organization that handles sensitive information, there is always risk. This risk can be reduced through effective policies, training, and technical controls; however, these safeguards will not fully prevent an incident from occurring, especially when humans are involved. Should an incident occur, VA will respond to and determine the severity of the incident, and be transparent and forthcoming in reporting to Congress. Together, these policies and activities ensure that veterans' information is kept safe on every platform, in every system, and even when shared. With this strategy in place, VA is making sure veterans' information remains safe and secure, which is an important part of the exceptional service that veterans so rightly earned.

Madam Chair, Ranking Member, and members of the subcommittee, thank you again for this opportunity. I am ready to answer your questions.

[THE PREPARED STATEMENT OF PAUL CUNNINGHAM APPEARS IN THE APPENDIX]

Mrs. LEE. Thank you, Mr. Cunningham. I will now recognize myself for 5 minutes for questions.

Just getting off to a start with some background information. Who owns the veterans' data, Mr. Cunningham?

Mr. CUNNINGHAM. Veterans own the veterans' data. VA is charged with protecting that data in performance of providing the benefits and services under our mission.

Mrs. LEE. Does the VA treat health data differently than benefit or vocational data?

Mr. CUNNINGHAM. Yes, we do. Personal identifiable information, PII, is protected under the Privacy Act; however, when it comes to medical records or health information, it falls under HIPAA.

Mrs. LEE. Is there a difference between ownership and stewardship of data, and what is that difference?

Mr. CUNNINGHAM. There is a difference. The difference resides in, at the end of the day, the veteran can decide who has access to that data. For instance, they turn their records over to VA to be custodians, and they also trust that VA is looking out for their interests in deciding who has further access under the laws and regulations.

However, a veteran can provide consent to other third parties outside of VA's purview to gain access to their information, in some cases—in those cases we have no real authority or control over that.

Mrs. LEE. Do you have concerns about that? I mean, are there areas along here where you are looking at what the VA can do to make sure that veterans really understand what that means?

Mr. CUNNINGHAM. Certainly that is a challenge that we are concerned about. At the end, veterans do not work for VA, it is hard to impose regulations or requirements for them for annual training. We send out notifications or in our fliers, we give pamphlets, when they are visiting our sites and waiting for appointments, there are public announcements that talk about how to protect your data or how you should be concerned. It is difficult, as across the industry or across the United States, to make sure that people really understand, when they click an app and accept that app, do they fully understand the full access that they have and how that information is going to be used downstream.

Mrs. LEE. What are the requirements for outside parties to access VA data?

Mr. CUNNINGHAM. For third parties that are accessing VA data, they must meet the same standard as a VA system. As they connect to our networks, they also get scanned and checked.

Mrs. LEE. I sent a letter to the VA on January 7th, 2020, asking about the VA's knowledge of the Ascension Health Partnership with Google and about how the VA oversees its community care provider, their third party data sharing. When can I expect a response to that letter?

Mr. CUNNINGHAM. I will ask our congressional liaison to follow up on that.

Mrs. LEE. Okay. Ms. Orr, what role does the VA have when a third party, whether it is a medical device, community partnership, Veteran Service Organization (VSO), enters the veteran health care space?

Ms. ORR. The role that the VA would have I think goes back to your question about custodian and doing what we can if the data is in our purview to protect it.

Mrs. LEE. Back to you, Mr. Cunningham, what are the VA's policies regarding the monetization of veterans' data by third party partners?

Mr. CUNNINGHAM. The Department's position is it is not to be sold. Third party access through our networks, they have to agree to those standards. As through—there are also any sort of contracts that apply or any sort of contractors applying to our networks or using our networks' data, they have to agree to acceptable use, which includes not selling that information.

Mrs. LEE. Does the VA have the capability, technical, organizational capability to monitor compliance with these restrictions, and have there been any examples where there has been a violation of that contractual agreement?

Mr. CUNNINGHAM. I am not aware of any instance where we have been informed that a third party has taken VA-managed data and sold it. In cases where—I mean, we certainly review the records and the performance of a contract, as it is required in the contract law in Federal Acquisition Regulations System (FARS), and if there is an issue, it is identified and appropriate action is taken. Again, I am not aware of any case where an approved third party has sold VA's information.

Mrs. LEE. You do have the ability and the technical capability and the organizational capability to monitor this performance for such breaches?

Mr. CUNNINGHAM. Outside the——

Mrs. LEE. Or are you being informed by a veteran who has been—like, how do you find out if that has happened?

Mr. CUNNINGHAM. Well, certainly, if a third party was doing it outside of the contract or in a lot of cases these third parties are health care corporations that understand the value of protecting that data, but if that is occurring, they are not informing us and we are not policing their networks. With that said, if a case does come forward where an individual says their information was sold from a third party that is endorsed by the Veterans Department of Veterans Affairs, I would say that we will take swift action to investigate it and take appropriate actions accordingly.

Mrs. LEE. Thank you. I am over time. I now yield to Mr. Banks.

Mr. BANKS. Thank you, Madam Chair.

Mr. Cunningham, I want to return to an issue from our cybersecurity hearing last year. I asked you then whether the VA had ever purchased equipment from a list of Chinese technology companies and you took those questions back for the record. The VA provided answers from those questions just last week that, based on searches of the Federal Procurement Data System, the FPDS, there were a few contracts for equipment from Chinese companies that are now prohibited. I want to know more about those circumstances and that discussion should probably happen between us in private at some point soon.

I have to say that the VA's answer gives me absolutely no confidence. FPDS is a public data base that contains at best a scant amount of details about what was actually purchased. If the VA is relying on FPDS to know whether blacklisted Chinese IT equipment was bought, I do not believe anyone in the Department knows what is really going on.

Mr. Cunningham, my question is, is there a more authoritative record or is FPDS truly what you are relying on?

Mr. CUNNINGHAM. I stand behind the response that we provided to you. I will be glad to have another opportunity to come talk to you specifically about how we manage our assets and in particular these blacklisted companies.

As far as the response, we stand beside that as being the best way for us to provide the definitive answer to you.

Mr. BANKS. Okay, that is good to hear, but can you tell me more about why did the VA's official response cite FPDS and no other sources of information?

Mr. CUNNINGHAM. Well, again, we were answering the question that you asked, was there purchase of blacklisted companies inside VA. We used the source that was most relevant to us and we feel we answered that question completely. Again, I would be glad to come back and talk more in depth about our processes of asset acquisitions, as well as how we manage our assets.

Mr. BANKS. Okay. Section 889 of the Fiscal Year 2019 National Defense Authorization Act (NDAA) is coming into force in August. I strongly supported it in the Armed Services Committee, which I am a member of as well. As I am sure you know, it stops Federal agencies from contracting with any entity that uses blacklisted telecom equipment or services. Is the VA prepared to comply with that law?

Mr. CUNNINGHAM. Yes, we are.

Mr. BANKS. How does the VA know whether a company is using blacklisted equipment or services? Now, I want to point out that the law applies to existing contracts as well as contracts in the future.

Mr. CUNNINGHAM. It will take some time to go back through our contracts and work with our third parties to identify where this has occurred. Like you, I believe that there is probably equipment being used by our third parties because it was not restricted at the time they purchased it for use. We need to make sure that in contract language it is prohibited and it is removed if it is on our contracts.

Mr. BANKS. The HIPAA privacy rule was written before mobile apps and Application Programming Interfaces (APIs) existed. Do you think the HIPAA privacy rule is sufficient to stop technology companies from monetizing protected health information?

Mr. CUNNINGHAM. There is not a clear statement in HIPAA regarding that. I think there is opportunity for us to expand on HIPAA laws to include how electronic records are managed, stored, and then downstream support from third parties or subcontractors.

Mr. BANKS. Does the VA individually or specifically have any role in stopping technology companies from monetizing veterans' health records—health care data?

Mr. CUNNINGHAM. In contracts—and we kind of talked about this before—in order for them to access our networks, they have to meet the same agreements and standards that VA has, and that VA's policy is not to sell or share information outside of the roles that they are designed to do. In that case, if you are talking do we have the technology to monitor third parties, we do not, it is outside that contract. If they do it, we can definitely look at doing a review and figuring out how we are going to remediate that, whether it is remove them from contract or hold them liable for losses.

Mr. BANKS. Okay. With that, I yield back.

Mrs. LEE. Thank you, Mr. Banks.

I now recognize Mr. Roe for 5 minutes.

Mr. ROE. Thank you, Madam Chair.

Data privacy is an important issue in the VA and, as the ranking member mentioned, especially with the data breach with Equifax. Obviously, it became clear to most Americans it was a huge problem, and it is a problem throughout the entire health care and private sector. I am glad we are able to have this discussion, I have learned a lot already. However, I repeatedly asked that today's hearing be focused at least on part the electronic health record modernization and include a witness from that office. I am encouraged and I appreciate, the chair and I discussed before the hearing started, that they are now going to have a meeting, we are going to have a meeting very soon, and I appreciate that.

Bill and I were in Seattle and Madigan recently, and then been to Spokane twice to see the rollout and there are issues there, which we will discuss later. Ranking Member Walz, my friend Ranking Member Walz, now Governor Walz, and I created this subcommittee with the intent of overseeing the EHR to be the core of its responsibility. I now recognize that parties can change along with the events, but even before Secretary Wilkie communicated his decision to delay the Cerner implementation in Spokane, this was already a pivotal month in that project. One of the delays that DOD incurred was security, that held up the DOD rollout. I expected us to be here either questioning VA about the Cerner deployment and what it was going to look like on March 28th or about what the delay would entail.

I firmly believe Secretary Wilkie's decision to delay was the right call. I also believe strongly that the committee now needs to ramp up, not ramp down, its oversight of the project, and I look forward to that hearing, Madam Chair.

I am going to go over several things quickly. I was just looking, I appreciate the chair's putting up on the whiteboard here, this is disturbing to me. When you look at the app here, the PTSD Coach, and I punch an "Allow," well, what I allow to happen when I punch the PTSD Coach, which I may not know, is access to my contacts in my phone and "Other," whatever that is, my storage, and along with the Concussion Coach. I give my calendar up, my contacts, photos, media files, microphone, I mean, on and on. The PTSD Coach has access to the mike on this. I find that very disturbing, because you might inadvertently hit that and not know. This disclaimer, obviously written by a horde of attorneys, nobody reads.

I think we have got to simplify this. Certainly I think a lot of people, including me, could make a mistake and access to your entire phone could be here and it could be your financial information, other information on here. I think we have to be very, very careful with that and revise. I can not imagine why the PTSD Coach needs access to my microphone or my contacts or my schedule. Anyway, that said, I think we need to rethink that out.

Mr. Cunningham, the VA sent out a notice of privacy practices, which I have here, in September, and it caused a lot of confusion with the veterans. I got a call when—Bill was pointing out when we were in Seattle about this—from a constituent—and I am sure

many of my colleagues did too—apparently the notice was written in a confusing way. It seemed to conflate VA's longstanding privacy practices under HIPAA with a change made by the MISSION Act that allows information about drug and alcohol use, HIV, sickle cell anemia to be shared with community care providers unless a veteran opts out. Can you explain what the VA meant with that?

Mr. CUNNINGHAM. So——

Mr. ROE. Here it is. It is a lengthy, front-and-back, eight-page—I just read it just a minute ago, a good bit of it on here, so I could see why a veteran was confused when they got this.

Mr. CUNNINGHAM. It is certainly not the intent to confuse veterans; it is the intent to inform veterans. I am sure it has gone through numerous reviews for readability and, if we missed the mark on that, we can go back and find another way as well to relay what we are trying to convey.

Mr. ROE. I guess probably a lot of people, Mr. Cunningham, why did I get this? I think, you know, and then when they read it, they thought, well—I mean, if you read on here, it is about your organ transplant, health care oversight, coroner, funeral services, national security workers, I mean, on and on. I guess a veteran would be asking, what in the world did I get this for?

Mr. CUNNINGHAM. Well, I think it is important that, you know, for the MISSION Act, it opened up new avenues for the veteran, and we were trying to inform them on what that new avenues means and what information we were sharing in support of those new avenues and new capabilities. In so, if we confused them, you know, my sincere apologies. I am glad to take it back and see if there is a better way for us to convey when we go and add new capabilities, new benefits, and share information with new venues, that we make sure that the veterans understand what we are doing on their behalf.

Mr. ROE. Yes, my time has expired. I think we just sort of overwhelmed them with too much information.

I yield back.

Mrs. LEE. Thank you, Mr. Roe.

Mr. Cunningham, along this point with respect to the notification for veterans, you made the statement that veterans are not employees of the VA, so you do not have control. However, I do think that there is a trust relationship that veterans understand that, if there is something being promoted or endorsed or, you know, endorsed by the VA, that there is a trust relationship there.

I do think that there is a higher level of accountability and responsibility to making sure that veterans understand in a clear, concise, easily understandable way. And what we are seeing again and again is it seems that we are getting caught up in all the legalese without this clear—you know, like I would expect that if you download an app and you are about to release all of your contact information that there is like a clear warning, you understand what you are doing here. I hope that we can look at that moving forward, because what is happening right now, we are hearing from our veterans in the field that there is, you know, ultimately a lack of trust, especially when it comes to this incredibly sensitive information.

Ms. Orr, I wanted to ask you, before—does the VA—and this goes back to the apps, primarily because when a veteran downloads their data into a third party app, HIPAA no longer applies, and so I want to know, does the VA vet apps before recommending them or putting them on the app store?

Mr. CUNNINGHAM. I would like to take a first glance at this. VA apps that are—apps that are on the VA store have been reviewed by VA. We see them as a value to the veteran and we look to make sure that they are meeting our acceptable use policy. In most cases, they are attaching to an API, that means that they are getting information from VA as part of that service to the veteran through that application.

I will ask Ms. Orr——

Mrs. LEE. What are the criteria for that app to pass this vetting process?

Mr. CUNNINGHAM. Well, we are looking at where is the benefit for the veteran. Again, is it accessing our networks and does it meet those standards that we briefly talked about earlier? Then what is the intent of the company in providing that act. If they are selling that information, obviously, we would not endorse that sort of application.

We do want veterans to look at those applications and know that VA is supporting those applications and reviewing them to get on that app.

Mrs. LEE. Are there any requirements in terms of the app security, you know, including access to the VA-controlled data? Like, what are the criteria for that?

Mr. CUNNINGHAM. VA-controlled data—and we would probably have to look at each app as it goes through, and we can come back and give you a more detailed decision process tree on apps, but in general we are looking to make sure that, if they are accessing personal information, personal identifiable information, or PHI, that they meet the same standards that we have, that they have to be protected and they have to agree to that standard in order to access the API.

As far as non-PII-related applications—for instance, there might be an application that says where is the closest hospital and we want to make sure that veterans clinics and hospitals are on that application and it is out for the public, that in itself is not reviewed that close, but we see the value of it for the veteran and we would hope that they would look at that as a service that we are providing them.

Mrs. LEE. Okay. Well, we will look forward to having some more information along those lines.

I just wanted to ask, so given what we have heard today and your processes, are there any areas of concern? Are there any areas—how can we be helpful? What can we do to help the VA to make sure that veterans' data is secure?

Mr. CUNNINGHAM. At this time, I do not think we are asking for any specific legislation or resources. You know, patience as we are trying to solve this bigger problem around this greater access of data. I thought this morning's comments were on mark and described the challenges that we have in this environment, especially as they relate to how do we make the risk-based decision. If we go

strictly by compliance and if zero tolerance is what we are going for, we are going to miss out on a lot of opportunity that technology brings and even life improvement opportunities if we are not being able to share information with our third parties that are trusted, to the extent that we are trying to bring better value, better customer experience to the veteran, and that also includes security and privacy in that risk decision.

Mrs. LEE. Thank you.

I would now like to recognize Mr. Banks for 5 minutes.

Mr. BANKS. Thank you, Madam Chair. I will be quick.

Mr. Cunningham, I want to read you part of the VA's terms of services for its API platform. Quote, "When records regarding an individual are obtained through a VA API, you may not expose that content to other individual or third parties without specific explicit consent from the individual or his or her authorized representative, or as permitted by applicable law," end quote.

Mr. Cunningham, is consent from the veteran always required or only required when there is not a law permitting the disclosure?

Mr. CUNNINGHAM. If it is in line with what—for the APIs, it would be that they would have to consent to that data, unless it is provided by veterans—or Veterans Affairs, in regards that we have contracted with a third party to provide a specific app for Veterans Affairs.

If it is a VA-built application, then we would not ask necessarily in every case that the veteran would have to click to it. However, if it is outside of our management, it would require the veteran to approve it.

Mr. BANKS. What exactly does a third party mean here and is it non-VA software? How about another API?

Mr. CUNNINGHAM. If you are building an application and you are wanting to get data from an information source, in this case the one that VA actually owns, you are going to be accessing an API, and I would have to bring some of our more experienced API developers in here to talk to you about that exchange. In principle of that, before they can connect, they have to get approval between the VA and that third party that is requesting information, and in that case third parties can be a separate organization outside of VA's purview.

Mr. BANKS. It sounds like VA's partner that is using the API is responsible for getting the consent from the veteran. What role does the VA have in making sure that happens correctly?

Mr. CUNNINGHAM. If it is on our application, our app store, we do verify that they are asking it. We do test and walk through it as if we are a veteran to ensure that it is there. Other than that, if a third party is providing an app to a veteran and it is outside of VA's purview, we have no real control of validating whether they are asking for that consent or how they use that information in agreement with that veteran.

Mr. BANKS. Okay, that is all I got. I yield back.

Mrs. LEE. Thank you.

I now recognize the chairman of the committee, Mr. Takano.

Mr. TAKANO. Thank you, Chairwoman Lee.

Mr. Cunningham, welcome. I recognize you are from the Office of OIT, but since you are the one from VA before us today, I would

like to echo what Chairwoman Lee said earlier about the VA needing to be more transparent with us. It is very important that as we continue to move forward through the integration process that VA is as transparent as—you know, not just as possible, just plain transparent.

Here is the thing. I was told last week by Secretary Wilkie that everything was on track with the electronic health record modernization rollout, but yet on Monday I am told that the go-live was going to be postponed with no definitive time line about how long it will be delayed.

You know, just with that as a sort of preface, what does VA need to get things back on track; is there anything that you need?

Mr. CUNNINGHAM. As far as EHRM and Cerner, that is outside of my purview. From my understanding that we have what we need. We are partnered with DOD, we are sharing information, and the decision to delay was more a tactical one and not necessarily a resource-limiting issue.

Mr. TAKANO. Okay. I realize that you are not the point here, but if you could take back to the Department, I want to know when you and others were first made aware that the EHRM go-live would be delayed. Just, you know, you do not have to answer that—if you know now, please, you yourself can answer that question, but I just want to know when this became apparent, because last week the Secretary himself said this was all moving forward and did not anticipate any issues. Go ahead.

Mr. CUNNINGHAM. I will be glad to take that back. Personally, myself, I was aware of it yesterday.

Mr. TAKANO. You became aware of it yesterday?

Mr. CUNNINGHAM. That is correct.

Mr. TAKANO. Okay. All right, thank you.

Madam Chair, I yield back.

Mrs. LEE. Thank you.

I now recognize Mr. Watkins for 5 minutes.

Mr. WATKINS. Thank you, Madam Chair.

Mr. Cunningham, I want to ask about VA's partnership with Apple Health. My understanding is that iPhones have memory chips that are physically separate for different kinds of information, how does that work in practice and what cybersecurity protections does that provide?

Mr. CUNNINGHAM. I am not an Apple engineer and I think that might be outside my scope of experience. I would say that on premise, on theory, having a separate chip that manages data from the Apple applications themselves is wise in design.

Mr. WATKINS. Apple says it does not control any of its user's data that it transmits on its iPhone. When the company says that, it seems to be referring to third party apps. In other words, the iPhone is just a vessel for other apps, but Apple Health is actually one of the few apps that the company directly owns.

What privacy protections specific to the VA are in place when veterans access VA medical records on Apple Health?

Mr. CUNNINGHAM. For Apple Health, like any other third party that is accessing veterans' information, would have to meet the same standards for privacy and HIPAA.

Mr. WATKINS. Your testimony discusses a privacy threshold analysis, which is a tool the VA uses to ID privacy issues in new IT systems or projects. Can you explain what this is, how it works, and give some examples of privacy issues that you have identified in the past and how you have resolved them?

Mr. CUNNINGHAM. National Institute of Standards and Technology (NIST) has a set of controls as it relates to privacy, as well as cybersecurity. Those controls are part of the system development and their system security plans. They are assessed in development, as well as in operations, and provided to the authorizing official to make a determination on whether the system meets the standards and what are the associated risks if not meeting the standards through either mitigating controls or possible POA&Ms or plan of actions, milestones to resolve them.

How it works and some additional information, I will ask Ms. David if she would like to answer that.

Ms. DAVID. Sure, yes. The privacy threshold analysis is actually the vehicle for assessing systems, programs, operations for privacy impacts. It is a templated document that goes through the life cycle of the effort itself and discusses, for example, privacy risk, those risk mitigations, any other connected systems. Basically, any and everything having to do with point-in-time activity and then as the effort develops.

It is a living document that gets revisited throughout the life cycle of the effort, and it also takes into consideration records, records retention, uses, and things of that such.

Mr. WATKINS. Understood, Ms. David. What are your specific privacy concerns?

Ms. DAVID. Generally, the privacy concerns would be how information is being shared. Is it being shared in accordance with routine uses, which are outlined in, for example, a system of record notice. The privacy concerns would also be how the information, based on its level of sensitivity, how it is being protected so that the protections are commensurate with the sensitivity of the information. Then also how information is handled in, for example, the incidence of a potential breach. We talk about that, as well.

Mr. WATKINS. Thank you. Thanks to the panel. I yield back.

Mrs. LEE. Thank you. I now recognize Mr. Roe for 5 minutes.

Mr. ROE. Thank you. Just to show you some of the confusion. Very quickly, Mr. Cunningham, I was reading, "When we offer you the opportunity to decline the use or disclosure of your health information, patient directories, unless you opt out of the VA Medical Center patient directory when being admitted to a VA healthcare facility, we may list your general condition, religious affiliation, and the location of where you are receiving care. This information may be disclosed to people who ask for you by name. Your religious affiliation will only be disclosed to members of the clergy who ask for you by name.

"Note. If you do object to being listed in the patient directory, no information will be given out about you unless there is other legal authority. This means your family and friends will not be able to find what room you are in while you are in the hospital. It also means you will not be able to receive flowers or mail, including Federal benefits checks, while you are an in-patient in the hospital

or nursing home. All flowers and mail will be returned to the sender."

That means if somebody thinks they are not going to get paid, they are always going to opt in. I think those are the kind of things I think that cause some confusion with veterans.

My suggestion is, Madam Chair, do not opt into anything. That would be my—after listening to this. Maybe go back to carrier pigeons, because you do not have any privacy anymore. There is no such thing as privacy. As a physician, I got, this is years ago, because of access insurance companies had to very sensitive information, I would sometimes even limit what I put in a medical record, because I was afraid even then, before the access to hackers and all that people have. With these opt-ins, you have just opened the book on your life. I mean, as an OBGYN doctor, I got told some very private things, which I just had to leave between my ears because I was concerned with the privacy. That leads to my question.

How does the VA decide which technology company it will collaborate with? Are there particular companies that the VA would be uncomfortable with? Or what specific privacy practices do the Department consider a red flag, because we know that the Chinese—we know this. The People's Liberation Army (PLA) is always looking for a back door into somewhere, which may lead to someplace else. How do you guys make that decision?

Mr. CUNNINGHAM. Well, I think, one, we have to balance the availability and access. I mean, certainly, there is many veterans that benefit from the applications and the APIs that are being provided today.

Mr. ROE. Yes.

Mr. CUNNINGHAM. Quicker information. How we figure out who we work with, we do not have a black list of companies. We do not pick winners and losers in the market. We have an API that provides information when it is requested in the proper protocol. In there, we are verifying that the proper protocol is there. Obviously, if there is a known—I do not think there is a litmus test for what organizations are in or out. Certainly, we can talk a little bit more and go back for the record and provide more detail on what is the decision tree that we use in connecting with APIs. I hope that answers your question.

Mr. ROE. Yes. I think, obviously, they have to bring a lot of advantages to people. I use them. We all do, that you can find a restaurant, or gas, whatever you may be using it for. I got that.

The question is that is an advantage. I look at a risk/benefit ratio. What are the risks you take? How can this information—I think both the chair and the ranking member have asked this question. How is this information shared? Is it accessible? How can it be used? Is it sold? I mean, when you purchase something on Amazon, I like to backpack. Well, I will have four tents on here today that Amazon is trying to sell me.

Those are questions that I guess we as a society need to answer. Is VA protecting it, and really looking at who you partner with?

Mr. CUNNINGHAM. We are looking at who we partner with. We look at who has connections to our APIs. What do they plan on using that information for? They have to sign acceptable use agree-

ment. We police—when we find out that there is information that is being wrongly used, we police appropriately.

With that said, what information are we talking about? If we are talking about health care information, obviously there is a higher standard of security that goes along with it. If you are talking about access to files, pictures, calendars on your phone, most users probably have, I am just estimating, probably 30 or 40 applications on their phone at any given time. They also carry two phones. How many of those applications are also providing that same sort of data and access to the information that they reside on their phone.

Mr. ROE. My time is up. I did not say we were smart. I am just saying——

Mr. CUNNINGHAM. Thank you.

Mr. ROE. I yield back.

Mrs. LEE. Thank you. Thank you. I just want to thank all of the witnesses for being here today. I would now like to—you are excused and I will call up the second panel. Thank you.

We can take a brief recess while we set that up.

(Recess.)

Mrs. LEE. Thank you. I will now call this back to order. I would like to introduce the witnesses on our second panel. Nick Culbertson is CEO and co-founder of Protenus. Is that right? Protenus. And is an Army veteran. Tina Olson Grande is the executive vice president for policy at the healthcare leadership counsel and chair of the confidentiality coalition. Ramsey Sulayman is the associate director, National Legislative Service for Veterans of Foreign Wars and is a Marine Corps veteran. Harold Wolf is the president and chief executive officer of Health Care Information and Management System Society (HIMSS).

We will now hear the prepared statement from our panel members. Your written statements in full will be included in the hearing record. Without objection, Mr. Culbertson, you are now recognized for 5 minutes. You can put your volume. Thank you.

STATEMENT OF NICK CULBERTSON

Mr. CULBERTSON. There. Does that work? Great. Thank you, ma'am. I appreciate the opportunity to present. I am here today under three prefaces. I am a former, as you mentioned, a former non-commissioned officer in the United States Army. I was also treated as part of the Veterans Affairs. I sit here now as a entrepreneur and CEO of Protenus, which specializes in health data security.

I think the data privacy is in constant juxtaposition with data sharing. We have heard much of that throughout testimony today. I think it is really important that this issue be addressed.

Our research has shown that every year data breaches have increased. Just last year alone, 41 million medical records were breached in the United States and that is only what we know about or what has been discovered. The more we share data, the more of a threat we create to our patient's data, particularly our veterans' data.

I have had experience with both the limitations of data being a challenge, but also seeing how the data sharing creates more of a challenge. My story goes back to when I was last stationed in Af-

ghanistan. I was assigned to use this device called the MC–4 that was supposed to take patient data from combat casualties that I could wirelessly send to a flight medic, that would then transfer that information all the way back to retirement and VA. It was a seamless integrated network that data would persist from DOD all the way to VA.

Unfortunately, we got trained many hours on this device, and then we took it into the field and then found out it did not work. We had to manually rewrite the medical notes to our flight medics and pass it off on pieces of paper that would fly away in the wind.

I think that program is still being developed. I hope that it continues to persist. After I got out of the military, I sought treatment through VA for my wrist that I fractured in the military. I was a little bit shocked to hear from my VA physician that since my wrist had healed and there was no x-ray in my record, my wrist was never broken in the first place, and so I could not get my document updated to show that I had broken my wrist, and make sure that I had long term care for that. I had to seek physical therapy through private practice, through private insurance, which is unfortunate.

On the other side of things, I have seen how health data becoming more accessible and shared creates more of a risk and more of a concern. As a medical student at Johns Hopkins, I saw how Hopkins rolled out the Epic integration, similar to what VA is doing now with Cerner on a different scale.

Decades ago, the only person who had access to your medical record was the physician at the foot of your bed. Now anyone throughout the hospital system, any business associate, any partner health system, any other Epic clients can now access that data. Technology has created this great increase in access that helps improve patient care and outcomes, but at the same time drastically increases the risk.

I think that—my belief is that while technology has created greater access, it also—there is an opportunity to create better assurance and better privacy with technology alone. I do not think this can be addressed just through policy and regulation. I think that we need to have security devices put in place, specifically with the VA as well.

Our company developed an artificial intelligence that understands how any end user is accessing PHI and whether they are using it appropriately. And we send proactive alerts to privacy risk compliance officers that identify those threats so that they can deal with them in relative real time proactively, rather than waiting for something to happen.

I know that this is an incredibly needed technology because of the amount of violations that we find. We estimate that 1 in 300 workforce members in health care violates privacy per month. Unless a monitoring solution is put in place, or unless regulations are appropriately addressed or policies are put in place, that only will continue and get worse.

I thank you all for taking the time to address this and I am looking forward to the conversation.

[THE PREPARED STATEMENT OF NICK CULBERTSON APPEARS IN THE APPENDIX]

Mrs. LEE. Thank you, Mr. Culbertson. I now recognize Ms. Grande.

STATEMENT OF TINA OLSON GRANDE

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

My name is Tina Grande. I am executive vice president of policy for the Healthcare Leadership Council, and chair of HLC's Confidentiality Coalition.

HLC is an association of chief executives representing all disciplines within American health care. The Confidentiality Coalition advocates for policies and practices that safeguard the privacy of patients and health care consumers, while enabling the essential flow of patient information.

The subcommittee's examination of how the Department of Veterans Affairs manages veterans' health data is especially timely, as new technologies continue to be introduced to the market. For every promising health information technological development, there is a risk of its misuse.

There is a 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 harness new technological innovations, while maintaining the privacy and security of data, will remain formidable. Any approach to health data privacy should preserve the existing HIPAA framework, which applies to treatment, payment, and health care operations for all patients, including veterans. New legislation should apply only to health data not governed by HIPAA.

New innovations, while beneficial, have 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 health app to their smartphone that sends a summary report to their doctor. As long as the doctor did not hire the app developer to provide its services to patients, the data in the app is not protected by HIPAA, even if the app is recommended by the patient's doctor.

Under HIPAA, covered entities are required to provide individuals with a notice that describes the entity's privacy practices, the purposes for which it uses and discloses protected health information, or 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. This same approach should be taken in addressing non-HIPAA health data.

Any new privacy framework should be consistent with HIPAA definitions. Conflicting or inconsistent terminology could have unintended consequences that could seriously and adversely impact the ability of health care organizations to aggregate and share health data for important care delivery and population health purposes.

Equally important, security safeguards should be commensurate with the safeguards required by the HIPAA security rule. Robust security requirements for non-HIPAA health data are critical, not only for sophisticated businesses that collect vast amounts of data, but also for startups, developing new products and services, which should be incorporating security by design practices in their product development process.

The promise of interoperability 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. Interoperability 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 is particularly critical for veterans who may seek care in community health systems in addition to the VA health system.

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, HLC and the confidentiality coalition commend the subcommittee for seeking to address the challenges faced by the VA in managing veterans' health data. 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. Thank you.

[THE PREPARED STATEMENT OF TINA OLSON GRANDE APPEARS IN THE APPENDIX]

Mrs. LEE. Thank you, Ms. Grande. I now recognize Mr. Sulayman.

STATEMENT OF RAMSEY SULAYMAN

Mr. SULAYMAN. Chairwoman Lee, Ranking Member Banks, and members of the subcommittee, on behalf of the men and women of the Veterans of Foreign Wars and its auxiliary, thank you for the opportunity to address our members' concerns about data privacy and portability, and VA's responsibility to protect veterans' privacy.

The commercialization of date crept up on Americans and pounced like a tiger. You have covered the data breaches that revealed information, vulnerabilities, and systems and institutions we presumed were secure. Health care data breaches often occur through malicious attacks, as well as non-malicious errors, such as the loss of the laptop.

Rarely do we focus on self-disclosed and user generated data, which accounts for a staggering amount of information on the average American. One's Facebook profile, Instagram picture, Spotify playlist, supermarket discount card, Fitbit data, pictures taken by

a Ring door cam, internet service provider data. Yes, the one site that your friend told you about that you looked at just for a second, just that one time. All of that information is available and brokered.

Companies scrape the internet for more photos and information on people who have no idea that this is happening, and certainly never consented. You have covered earlier the permissions that veterans are required to consent to use VA apps.

Veterans live in this information and technology ecosystem and the same concerns apply. However, because veterans have access to a comprehensive suite of services from the VA, everything from health care to home loans, veteran sensitive information is concentrated in one location, the Department of Veterans Affairs.

The requirement to consent to terms that are broad, rarely understood, and without alternative is a major concern. Changes in ambitious products at VA, the integration of health records with DOD, the Million Veteran Project, MISSION Act, and implementation present great opportunities, but data security challenges.

VA partners with entities outside its IT ecosystem, and this seam is where vulnerabilities also lie. Veterans expect VA to set the tone and place data security and privacy as a foundational priority. You have already touched on past breaches and security lapses, such as the 2006 theft of a VA laptop that exposed the data of 26 and a half million veterans in active duty military.

2015 OIG report detailed Chinese nationals accessing the VA network from China. In October 2019, OIG report detailed security lapses, including placing veterans' PHI and PII, their personally identifiable information and personal health information, on thumb drives and personal computers. The 2019 OIG report on VA's ability to meet the Federal Information Security Modernization Act requirements noted significant challenges.

This leads us to believe that data security management and protocols may not be at the level necessary. VA's transfer of information to entities outside its ecosystem through record sharing and simple IT processes like the single VA log on through ID Me are of concern. As noted in our written testimony, end user license agreements leave questions of access to and retention of veterans' information open. You also touched on that earlier in your questions and comments.

It is not a question of understanding the terms. It is a question of what are the alternatives. Most often, there are none.

We also noted the instance of Ascension's partnership with Google on a massive health data project, known as Project Nightingale, where Google collected sensitive health data as a HIPAA compliant business partner of the health system, without the explicit opt in of patients.

As Ascension often marketed toward veterans and encouraged them to use Ascension with the Veterans Choice Program, it is unclear whether veteran medical records shared with Ascension as part of community care programs ended up in Google's hands.

Let me be clear that just because I use an iPhone SE still does not make me a Luddite or a conspiracy theorist. I just really like small phones. Great good can come from data sharing, especially health data, and VA is in a very unique position. Access to health

care data means that providers can apply artificial intelligence and machine learning to make diagnosis faster and better, as well as treat more effectively.

Nick testified to the artificial intelligence capabilities of his platform. The trove of veterans he identified health data offers game changing research possibilities. These worthy goals must be pursued. To Dr. Roe's point about risk versus benefit, though, the Veterans of Foreign Wars of the U.S. (VFW) believes in these foundational priorities.

The use of veteran's information should require informed consent and a plain language explanation of exactly what the veteran is consenting to, what will be used and collected, and how that data may be used. VFW and the other VSOs are more than willing to consult with VA on making VA communications easily understandable to veterans.

Our executive director, BJ Lawrence, has directly offered that assistance and the offer stands. The VFW also believes that the minimum amount of veteran data should be collected through VA platforms, including by third party partners. VA and contractors should not pass on any more information than is necessary to their subcontractors or partners. Information should be retained for the minimum amount of time necessary, and then deleted. Veteran information should be de-identified where possible.

I thank you for your attention to this important matter and look forward to answering any questions.

[THE PREPARED STATEMENT OF RAMSEY SULAYMAN APPEARS IN THE APPENDIX]

Mrs. LEE. Thank you, Mr. Sulayman. I now recognize Mr. Wolf for 5 minutes.

STATEMENT OF HAROLD F. WOLF, III

Mr. WOLF. Chairwoman Lee, Ranking Member Banks, and distinguished members of the subcommittee. Thank you for the opportunity to testify today. My name is Hal Wolf. I am the president and chief executive officer of the Health Care Information and Management System Society (HIMSS). HIMSS is a global non-profit advisor and thought leader supporting the transformation of the health ecosystem through information and technology, with a membership that includes more than 80,000 individuals and hundreds of partners and organizations.

We appreciate the committee holding today's hearings and addressing the role of Congress and the Department of Veteran Affairs in ensuring the confidentiality, integrity, security, interoperability, and availability of veterans' personal data.

As significant advances in technological innovation in health care have allowed us to capture data and use information in unprecedented ways, we must ensure the proper processes are in place to protect the privacy and the security of the patient's most sensitive information without losing the potential benefit of its use.

Our health care ecosystem has come to rely on an increasing number of tools and capabilities, which depend upon secure access to and use of patient data. The industry's fundamental goal is improved outcomes at a lower cost per episode. To meet this goal, we must have technology-enabled data collection and interoperable

data sharing. Given the large population receiving services through the Department of Veterans Affairs health care system, it is not a stretch to see that the VA is facing the same pressures as the rest of the industry to use data-driven capabilities to help them better manage the health and the healthcare of their patient population.

We believe the recently proposed Federal regulations, including the Centers for Medicare and Medicaid Services (CMS) interoperability and patient access rule, and Office of the National Coordiantor for Health Information Technology (ONC) information blocking rules will advance interoperability and support safe and secure access to health information and data-driven tools that allow for more provider and consumer choice in care and in treatment.

Now, any discussion around access to 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 it is granted, and what are the stewardship responsibilities over the data?

It is imperative that our mind set shifts to the access and the appropriate usage of data that is needed or information that benefits patient or individual health outcomes. Generally speaking, data ownership refers to the entity or individual who owns or originates the data. However, the data may not be in the originator's possession when needed or having already been passed on. Most decision support tools, for example, use data from multiple entities that may begin to use more than just clinical data, such as social determinant information to make recommendations to the user.

Data access simply refers to being granted permission of the data in some way or possession. This might include the ability to read, edit, or copy data for a variety of purposes. Its data usage and how the data could be transformed into information, storage of the data is permission for primary and secondary use, both short and long term. Rules around primary and secondary usage of data are where significant attention needs to be focused.

Data stewardship largely focuses on providing a secure and trackable environment. Cybersecurity is an important component of data stewardship. In order to ensure 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. Access rights with clear usage guidelines are mission critical.

HIPAA remains an integral part of our Nation's information security and privacy infrastructure for both veterans in the broader patient populations. With regard to the public dialog on possible HIPAA changes, HIMSS is focused on encouraging the safe portability of data.

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. Thank you and we look forward to your questions.

[THE PREPARED STATEMENT OF HAROLD F. WOLF, III APPEARS IN THE APPENDIX]

Mrs. LEE. Thank you. I now recognize myself for 5 minutes for questions. Mr. Wolf, given when we talk about data management,

data privacy, what should we really be looking at in how should the VA measure its success regarding patient protection?

Mr. WOLF. A wonderfully complex question. I think we hit on a number of the challenges earlier. The initial point of data protection is the data that you have stewardship over at that particular moment and how you must protect it, but more importantly, how you use it in the care treatment and the pathways to ensure that the best possible treatment and recommendations are happening to the individual patient and we are getting the best recommendations to the clinicians that are there.

We have to be able to look at that multi-tiered safeguard that was already been brought forward. Am I storing the information that I have possession of at that time with all of the appropriate safeguards? To whomever I am passing that information, we need to know their security on their side and where that information can and cannot go.

The points about secondary use of information or its potential sale, those are huge issues. They really need to be legislated on a full scale basis. The VA can do what it should be doing in terms of protecting the information. But it also becomes an important congressional pieces.

Mrs. LEE. How should the VA measures its success?

Mr. WOLF. I think you measure your success, first of all, by are there any breaches that are occurring? That is the simple part of it. The second is measuring its success in its review of secondary apps or organizations that the information is passed to. Then, of course, in the end, how is that information being used to better the treatment of the patients that it has accountability for.

That relies on understanding the use of the applications and how it is transmitted, and whether there is success protocols on value-based care being delivered.

Mrs. LEE. Great. Thank you. Ms. Grande and Mr. Sulayman, could you please give me an example of in your experience in mind, what a worst case scenario would be with respect to how the VA treats its patient's data?

Ms. GRANDE. Sure. A worst case scenario, we could consider—I think there could be many. I think largely falls outside of the non-HIPAA covered data that is identifiable, it is sensitive. It is related to detailed health care information that an organization who is not bound by HIPAA or strict State privacy laws either sells, monetizes, or mishandles information that A) the patient or consumer has no knowledge of because there is simply no—they are not aware that their information is not protected. Because consumers generally do not distinguish between, "I am at a place where I have got HIPAA coverage," and—we just know we have our health information.

We have trusted hospitals and health plans and pharmacies with our information, because largely HIPAA has worked pretty well. I think a terrible scenario would be information that is sensitive about our health care has been bought, sold, used, analyzed without our knowledge, and has trickled downstream for a number of years, and comes back to potentially discriminate against us in the long run. I think that that is a real risk that is occurring in a

largely unregulated market that has access to identifiable information about us.

Mrs. LEE. Thank you.

Mr. SULAYMAN. I would tend to agree with Ms. Grande on that point. I mean, I think that HIPAA provides a framework, and it provides penalties, and it provides some clear guidance on what is and what is not acceptable. As I mentioned in my testimony, in both the written and the oral, the user generated data that we have, I mean the information that is collected off of the apps that you were talking about, you know, with the privacy policies written by committees of lawyers, "hordes of lawyers" I think is how Dr. Roe referred to it, having that information leak out and then being collated with other information that is out there.

I mean, I think that that is really the danger just large across the entire—for the entire population, but for veterans especially if you are talking about Traumatic Brain Injury (TBI), PTSD, other sensitive information. Having that sort of health information be able to be gleaned from the purchases that you make through a doctor's use of the Zelth (phonetic) platform, for instance. You bought compression socks and syringes, so a machine looks at that and says, "A diabetic." That sort of amalgamation of information that you didn't even know was out there and is not covered by HIPAA is the main danger.

Mrs. LEE. Thank you. I now recognize Mr. Banks for 5 minutes.

Mr. BANKS. Thank you, Madam Chair. This question is for anyone who wants to answer it. Do you believe the HIPAA privacy rules—the rule is adequate to govern apps that receive patients' protected health information?

Ms. GRANDE. I am happy to start. I think that is a very complex question. The HIPAA privacy rule was promulgated many years ago. It was crafted very meticulously for a health care caregiving and payment system. As such, it was applied very specifically to that type of system that is directly in contact with patients, their payment, their claims.

When we are looking at HIPAA as a potential framework for tech companies, who do not necessarily fit into the very precise definitions for a covered entity, and may not be functioning as a business associate, because they are not working directly for a covered entity, maybe sandwiching those companies into HIPAA as a new covered entity, it is very complicated and I do not think it is going to be easy at all.

You could look at potentially a larger national privacy framework that would apply to those companies. Our recommendation is that when it comes to health information, that it harmonize with HIPAA. The last thing we want to do is to bottleneck important health information, because it stops because you have got two different privacy laws that are in play that could conflict or be confusing.

If, for example, the Veterans Affairs Committee is considering new privacy legislation as it relates to veterans' health information and non-HIPAA covered data, we would suggest that you also work with other committees of jurisdiction that are overseeing the commercial and Medicare and Medicaid markets, so that as veterans flow in and out of the commercial and the VA system, their infor-

mation is not getting bottlenecked because you have got two separate privacy laws at play.

Mr. BANKS. Okay. Let me move on to another question. This is for anyone who wants to answer it as well. If you agree that Apple and Google essential control software distribution through their app stores, what is their responsibility to police the apps they allow into their stores, not only for cybersecurity but also for privacy protection?

Mr. SULAYMAN. I will take a stab at this first. I think that if you walked into a brick and mortar store and a product lopped your hand off when you went and grabbed for it, you would agree that the store is probably responsible for being negligent and offering that.

I think that by and large, the tech sector's abdication of responsibility for the products that they carry in their virtual stores is something that really needs to be looked at and addressed. I mean, if you are carrying something that is a purveyor of malicious software or yesterday there was a report about three email clients that scrape data off phones, just by virtue of loading them and consenting through the data and privacy policy, the thing that you do not read and click accept. You know, one of them scrape the data and send it back to Rakuten, an online shopping platform.

Literally, same sort of consent that you have with some of these apps: your microphone, your contacts, your pictures. Literally anything and everything that they want.

Now, the response was, "We only collect certain things." Again, it is not transparent. I think having the transparency and having the accountability, there needs to be some verification system that what you are downloading through a trusted platform is, indeed, trusted.

Mr. BANKS. I will move on to another question. Or anybody else? Yes.

Mr. CULBERTSON. Could I just add onto that, that I think health data should—we could take a step further, that really should not be compared to other types of data that you might find on an iphone, just because of how valuable it is and how immutable it is.

Just because we say something is appropriate or suitable for an iphone app, I think we should even go beyond that for health data.

Mr. BANKS. Very good. I do not have a lot of time yet, so I will yield back and save questions for later.

Mrs. LEE. Thank you. This question is for Mr. Culbertson. How should the VA compare to private industry in areas of data privacy, consumer protection, and security?

Mr. CULBERTSON. Well, I think if we ask that question today and we look at the top five offenders of HIPAA violation according to the Office of Civil Rights, the VA ranks among those top five. I think with this opportunity to modernize technology, I think there is an opportunity to correct that image.

I know that what health systems outside of the VA are doing now, back to the question you asked for Mr. Wolf in terms of demonstrating a good privacy program, is not only are we looking at whether good policies are in place, do we have a business associate for every partnership, are we ensuring appropriate transfer of date according to HIPAA and other regulations.

Health systems are also auditing proactively every access and accounting for all of those disclosures to ensure that they are being appropriately used under treatment and payment operations.

I think there is an opportunity here to match that higher level of standard and additionally go beyond.

Mrs. LEE. Thank you. Mr. Sulayman, should the VA be responsible for educating veterans on protecting their privacy?

Mr. SULAYMAN. I think that is a great question, ma'am. I think that the obvious answer is yes, particularly as it related to any data that the VA is using or has in their possession.

I mean, if you are talking about just general education, I think it would be helpful and certainly falls within the VA's purview on many of the programs that it manages. Certainly for IT and health care data, that as we said, the plain language explanation of what is being collected, how it is being used, what will be done with it, and any opt in or opt out options are something that the VA should clearly define.

As I had said, we are happy to help the VA review that process for readability and understandability for your average veteran.

Mrs. LEE. Thank you. Ms. Grande or Mr. Wolf, how far should that VA obligation to protect data extend?

Mr. WOLF. Well, I will take a pass. I think that the—coming back to this issue about the VA and the consistency of its needs and protecting the data has to be consistent with all of the other health systems that exist in the U.S.

The harmonization point around HIPAA is a critical point as well. You do not want to create bifurcated environments. The reality is, of course, is that a person who is receiving care through the VA may well be also receiving care from other entities. The free passage of that information is critical for their own health, as well as future use of information.

The simple point is that the VA has to be extraordinarily vigilant, as does every health care system on the use of that information and where it goes. Not just within its domain, but when it is passed, you have a responsibility to pass it to a quality organization.

The testing and the variability, if you would, of the application that is receiving, falls to the responsibility of the VA, as it should with every health system.

Ms. GRANDE. I agree completely. The VA does have a responsibility for those it oversees as it relates to their health information and how it is being used. I think consumers just simply do not distinguish between information that is protected by their hospitals, health plans, pharmacies, and that which is not.

I think there had got to be more of an education, just nationwide for consumers about how their information is protected and not—and the ramifications of it, if it is not.

Mr. WOLF. I would just tag on in our last 30 seconds that it is very important for establishing criteria, if you would, around where that information is going to go and how it is going to be used. There is a baseline assumption on the part of every consumer that they are protected. Even if they are looking at these incredibly long agreements, their underlying assumption is that their information is under proper stewardship.

Ms. GRANDE. Concur.

Mrs. LEE. I agree. I actually believe that veterans even have a higher level of expectation when it comes to the VA as well. I am going to recognize Mr. Banks for 5 minutes.

Mr. BANKS. Thank you, Madam Chair. Ms. Grande, is HIPAA's minimum necessary principal intention with the 21st Century Cures Act penalties for information blocking?

Ms. GRANDE. Well, I know that the Office for Civil Rights sort of hinted around that in their HIPAA Request for Information (RFI) that came out last fall. We certainly will be commenting on that when the notice of proposed rulemaking comes out in short time.

Our member organizations do believe that the minimum necessary standard is appropriate, that sharing only what is necessary to promote better health outcomes is the right way to manage health information.

For example, in some of these scenarios where you have got to hand over your photos, your calendar, your contacts, that flies way beyond the minimum necessary standard under HIPAA. I think our member organizations have all agreed that that is way too much information to be sharing.

That said, though, there is value in analyzing large data sets to find treatments and cures. That is one of the wonderful aspects of advances in technology so we can speed up treatments and cures. I think motive matters and really focusing on the motives behind what is trying to be done needs to be paid a lot of attention to.

Mr. BANKS. Okay. Let me move on. So far, our HIPAA conversation has been mostly about covered entities business associates that happen to be technology companies or apps. Your testimony, Ms. Grande, you highlight the lack of legal protections when patients opt to provide their health data to an app. Should HIPAA or something very similar be extended to these apps, or should it be something different?

Ms. GRANDE. Well, the Federal Trade Commission (FTC) does have some authority in the non-HIPAA space. It is not there is no legal protection, but I think many feel that the FTC's limited authority is a problem and that the FTC should have more authority over the non-HIPAA space.

In terms of legal protections in the non-HIPAA space, we do believe that regulation is necessary, that the information blocking rule out of ONC and the interoperability rule out of CMS, which both of which we very clearly support the move toward interoperability. It is necessary and imperative to improve health outcomes.

At the same time, there are provisions in those two rules that require health plans and providers to direct protected health information under HIPAA into an API and third party app of a patient's choice. That does get back to the fact that people do not distinguish what is under HIPAA and what is not.

If there is any way we could look at some kind of authority within those agencies where we could do a better job, perhaps some sort of a certification process, or something whereby you have at least a semblance of good data stewardship going on with these third party apps, we would recommend that. We do believe that there is

a role for Congress in this place to ensure that penalties and enforcement that are meaningful are brought to the forefront.

Mr. BANKS. Let me finish with this final question for you, Ms. Grande. What are some specific privacy considerations for the medical device industry, especially concerning medical devices that are integrated with apps?

Ms. GRANDE. If a medical device is not operating as a business associate, and many of them do, so therefore come under HIPAA, they are really working closely with doctors, hospitals, those that are in the HIPAA environment. I think, again, it gets to the point that while we do support regulation outside of HIPAA, but in this particular case, it is especially important to note that it really needs to harmonize so that you are not creating a new barrier to information flow that really matters for a beating heart, an insulin pump, things that are maybe tacked on through an app or something that helps support that, that may not be within the purview of a covered entity and therefore a business associate relationship. It has got to harmonize. You do not want to——

Mr. WOLF. Terribly close to the Food Drug Administration (FDA)——

Ms. GRANDE. Yes. Then you have got the FDA is really starting to look at some of this now too. Right.

Mr. CULBERTSON. Could I just add on that one complication here is that data that may exist within the app that is not covered under the covered entity, once it touches data that came from that covered entity, then falls under that purview. I think that is a lot—that is a nuance that a lot of app providers do not really take into consideration.

Mr. SULAYMAN. If I could just take 20 seconds to echo the comments that both you and the chairwoman made earlier, HIPAA was created in an era when it was paper records, when analyzing data sets was extremely difficult, when my Mac LC–3 with 80 megabytes was really impressive. It really has not taken into—it was not created and did not take into account the environment that we are in now. The harmonization of HIPAA and not blocking the flow of information, and allowing all of the good things that can happen with the analysis of big data sets and artificial intelligence and machine learning to health care issues is very important. We also need to remember that this was created 23 years ago in an entirely different world that was not foreseen at the time. Amazon was still just a bookseller that everybody thought was going to fail.

Mrs. LEE. Thank you.

Mr. BANKS. Thank you. I yield back.

Mrs. LEE. Thank you. We are now going to adjourn. I wanted to thank all of the panelists for being here. Thank you, ranking member. What do I have to say here? Here is my statement. Hold on. There is something I need to say.

First of all, thank you at the VA for sticking around for this testimony, and I certainly think there is space for us to continue to look at this issue, especially as technology is accelerating and making sure that we are looking out for innovation and patient results and care results, but also taking into effect protecting our veterans from what could potentially long down the road be used for workforce discrimination, all sorts of things that could happen that

would have incredibly negative impact, not just on the health care of our veterans, but on their entire life and employment, et cetera.

I hope that this will be an ongoing conversation as this subcommittee continues oversight of the VA's innovation or technology modernization efforts.

All members will have 5 legislative days to revise and extend their remarks and include extraneous material. This hearing is now adjourned.

[Whereupon, at 11:50 a.m., the subcommittee was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF WITNESSES

Prepared Statement of Paul Cunningham

Good morning Madam Chair Lee, Ranking Member Banks, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify today about the Department of Veterans Affairs' (VA) mission to secure and protect the personal and sensitive information of our Nation's Veterans. I am Paul Cunningham, the Deputy Assistant Secretary for Information Security, Chief Information Security Officer (CISO) and Chief Privacy Officer. I am accompanied by Martha Orr, Deputy Chief Information Officer, Office of Quality, Performance, and Risk (QPR) within the Office of Information and Technology, and LaShaunne David, Director of VA Privacy Service within the Office of Information and Technology.

I want to thank Congress, and especially this Subcommittee, for its support of VA's work to ensure Veterans' privacy. Because of your steadfast cooperation, Veterans can continue to trust that their information is safe and secure. As the Chief Privacy Officer, I lead the VA's privacy program that protects Veterans' personal information. This aspect of VA's mission is personal to me. As a Veteran of the U.S. Navy, I fully share the concerns of my fellow Veterans who receive VA benefits, care, and services. For this reason, I am personally committed to ensuring Veterans' information is protected from exploitation and is handled with care.

Introduction

VA Secretary Robert Wilkie has pushed forward a Department-wide modernization strategy to transform the Veteran experience, including increased access to services and information and interoperability with the Department of Defense (DoD). To achieve this, VA must extend its digital footprint, introduce new technologies, and increase data sharing. However, such efforts bring new privacy and security considerations. VA understands that with IT modernization must come modernized privacy and security policies. VA's Assistant Secretary for Information and Technology and Chief Information Officer (CIO), Mr. James Gfrerer, and OIT are responsible for striking this balance among information technology (IT) modernization, IT operations, and privacy and security. Specifically, OIT's Office of Information Security (OIS) manages security and privacy policy and related activities Department-wide, while OIT's QPR division manages the VA Records Management program, which provides oversight of VA's compliance with those policies.

VA's mission is to provide Veterans the care, benefits, and exceptional service they have earned. In the course of that mission, Veterans voluntarily share their personal information with the Department. This information may include personally identifiable information (PII) such as an address or Social Security Number or protected health information (PHI) such as data captured during health care visits as well as PHI and PII information collected as part of their application benefits. Veterans may also provide information about their families or caregivers. An important part of VA's mission is to ensure we are good stewards of Veteran data.

VA has a robust set of policies and regulations governing privacy, access control, data and records management, and data sharing. It employs a rigorous framework of clauses and agreements that enforce these policies within VA and with our partners. VA also boasts strong incident response protocols to address any violation of these policies. In general, VA has policies and Business Associate Agreements that govern its activity or relationship with partners; conducts activities to enforce the policies; and imposes consequences for any violation of policy or contract agreement. With this strategy, VA effectively ensures the privacy of Veterans and the security of their personal information.

VA and many similar large organizations face challenges. As the Department moves to adopt and implement new technologies, its privacy and security policies and practices must keep pace and change accordingly. Emerging issues in technology require that VA continually emphasize the importance of privacy for our Veterans, the Department, and our Federal and commercial partners. As the Depart-

ment rises to meet these challenges, VA remains a vigilant protector of Veterans' information.

Privacy Policy and Compliance

As part of VA's efforts to create a more seamless experience for Veterans, VA has increased ease of access to information on such sites as VA.gov. VA does not solicit personal information and only asks Veterans for information necessary to provide care or services. VA directly communicates to Veterans about the PII it collects and how that information will be used. The Department's policy regarding the privacy and security protection of Veteran data is accessible to Veterans on VA.gov and includes information about how VA collects, stores, uses, and discloses Veterans' information. It also details Veterans' legal rights and information about how VA complies with Federal regulations and user agreements. Like all Federal agencies, VA must comply with the Privacy Act, which provides protections for Veterans' personal information.

An example of proactive and tailored implementation of privacy policy is VA's Webpage privacy. VA maintains a general Webpage privacy policy, known as the "General Policy," that applies to all VA.gov Webpages. Some pages have additional guidance, called "Limited Privacy Policies," which are compatible with the General Policy. VA's Websites generally do not require registration or request personal information, but some portals require Veterans to input PII to register for access. When Veterans do provide information, VA will not disclose that information to outside parties except at the request of the Veteran or as authorized by law. Additionally, VA.gov will never sell or rent personal information to outside parties. Violation of any part of this policy within the Department would result in corrective actions including possible dismissal and could result in a criminal charge against the offending employee or contractor. These policies ensure that Veterans' digital experience remains as secure and confidential as a visit with their care provider.

VA also has a review process in place to ensure that Administrations and staff offices integrate privacy compliance into their development and use of IT systems. The VA Privacy Service implemented the Privacy Threshold Analysis (PTA), a tool to help identify potential privacy issues within each new IT system or project. In certain cases, VA staff may be required to complete a Privacy Impact Assessment, which helps Veterans understand what information VA is collecting and how the information will be used and stored. This process ensures that system owners and privacy officers work in tandem so that any new IT system or project addresses all privacy concerns for the Veteran. As VA modernizes old systems and develops new systems, this specific review process establishes a Department-wide consideration of privacy.

Access Control

VA has policies and practices to ensure that access to Veterans' information is strictly controlled. VA implements a role-based access control system, which means that the Department grants access only to those employees or contractors with an official need to know to perform essential job duties or health care functions. Often, VA must allow contractors or other third parties to access Veteran information in order to provide care or services; in these cases, the party enters into a clear, comprehensive, and strict agreement with VA about how it may or may not use that information. System owners under each of VA's Administrations must determine the level of access control to implement for the system containing VA data. Systems are not authorized to operate until a designated authorizing official reviews and determines the control configuration is acceptable. To maintain access to sensitive information, non-Department entities must protect VA data from access by any other outside party.

To enforce these policies and use agreements, system owners conduct regular audits for compliance with the Federal Information Security Management Act (FISMA) and routine checks to ensure the system is compliant. Additionally, audit logs contain information about who accesses the system, when the system was accessed, and what data were accessed.

Should data ever be improperly accessed, VA will act to restrict access to the system and initiate an incident review process to determine what happened. When the improper access was a result of human error or improper behavior, VA will take corrective actions which could range from remedial training to revocation of access. VA requires that all personnel including contractors undergo mandatory privacy and security awareness training and sign a National or Contractor Rules of Behavior agreement. The Department takes appropriate steps to enforce these agreements.

Data and Records Management

VA's Records Management policy governs the storage, transfer, and destruction of sensitive data within the Department. Sensitive information may only be stored on and transferred between approved systems or repositories or those which are governed by the appropriate access controls. Contractors and other third parties must also comply with VA requirements regarding media sanitization, and destruction must often be supervised by a Federal employee. From collection to destruction, Veterans' information is handled with the greatest possible care.

VA's QPR Enterprise Records Service oversees activities related to the creation, maintenance, and use of records and ensures compliance with National Archives and Records Administration VA Records Management policy and Federal regulations that allow the release of limited Veteran information under the Release of Names and Addresses (RONA) program. When required by law, VA also provides information to the Veteran and the public in responding to requests submitted under the Freedom of Information Act (FOIA). Protecting Veteran data during this release is an extremely high priority. VA's OIS Privacy Service oversees activities related to safeguarding the PII and PHI of Veterans and employees. VA OIS Privacy Service's duties include:

- conducting privacy risk assessments and ongoing compliance monitoring of VA systems;
- overseeing information storage and VA's system of records;
- tracking access to PHI; and
- delivering privacy training, orientation, and ongoing awareness campaigns.

Should the VA OIS Privacy Service identify issues or receive complaints in the course of its oversight and monitoring, it will investigate and take corrective actions to enforce the Department's privacy policies in coordination with similar VA stakeholders and, when necessary, legal counsel.

QPR's Privacy and Records Assessment Division (PRAD) and its Administration partners perform onsite assessments on privacy and records management compliance at VA facilities and staff offices. Assessment findings that cannot be remediated onsite are reported to facility leadership for action. Issues that are not corrected as part of this ongoing continuous monitoring effort are further elevated to senior leadership as potential risk issues that could impact overall compliance. QPR's Risk Management Division will assign risk analysts to make determinations on the level of risk and determine overall required remediation actions.

Data Sharing and Portability

VA closely safeguards Veterans' information, but often must share data with partners to provide health care and exceptional service to Veterans. In general, VA does not share Veterans' information with non-Department entities, except when sharing is necessary to provide care or services to the Veteran or in accordance with routine uses as described in applicable system of records notices. In these cases, VA agrees with its partners about acceptable use of VA's systems and any Veteran information contained in those systems. That contract or agreement contains VA's requirements related to data protection and media sanitization, which the partner must meet to access Veterans' information. Once granted access to VA and/or Veteran information, it must protect that information as closely as VA does. These requirements are in place to ensure that Veterans' personal information is guarded just as closely, even when shared.

Conclusion

VA continues to improve the Veteran experience by consolidating health and benefits information in convenient digital platforms and increasing Veterans' access to their health records and data. However, VA understands that accessibility and sharing must not come at the expense of safety, security, and confidentiality. Additionally, emerging challenges in technology call for increased attention to data protection and privacy.

In response to these challenges, VA maintains a comprehensive security and privacy program. The Department strives to achieve the highest standards for safeguarding the sensitive information of our Nation's Veterans. We comply with Federal regulations, maintain an organizational structure focused on data protection and records management, and facilitate ongoing privacy assessments, reviews, and monitoring based on strict access controls.

Madam Chair, Ranking Member, and Members of the Subcommittee, thank you again for the opportunity to testify on behalf of the Department about the privacy safeguards we employ on behalf of the Veterans we serve and the exceptional service we strive to provide in the process.

Prepared Statement of Nick Culbertson

Good morning, my name is Nicholas Culbertson and I'm the CEO of Protenus. I bring testimony today to the Committee on Veterans' Affairs Subcommittee on Technology Modernization with three different perspectives: that of a former non-commissioned officer of the US Army, that of a patient treated by Veteran Affairs, and that of a former medical student turned CEO of a healthcare compliance analytics and health data privacy firm called Protenus.

In these roles, particularly in my current one, I have learned that health data privacy and security requirements are in constant juxtaposition of the need for health data sharing, interoperability, and innovation. On one hand, we need to make health data accessible to help improve direct patient care delivery speed and effectiveness as well as spur novel innovations, further accelerating the quality and capabilities of our healthcare industry. On the other hand, the more accessible health data becomes, the larger the threat surface becomes, exposing health data to privacy and security breaches, as well as misuse of data and fraud.

The tension between protecting health data and sharing health data is not something that should be addressed lightly. We need to share data and we need to protect it. Any standard that tips favor in one direction will either stifle innovation or compromise the integrity of arguably one of the most valuable types of data in the world. I want to thank the Subcommittee for its efforts to consider setting a higher standard for health data privacy while modernizing VAs electronic health record system and hearing my testimony on the topic.

In 2009, I prepped for my last deployment to Afghanistan with the 20th Special Forces Group where I served as a Special Operations Medic and Advanced Tactical Practitioner. As an SF Medic on pre-deployment, I was trained to use a tactical palm-pilot device and laptop system, known as the MC–4, that was intended to capture SOAP notes and other medical documentation on the battlefield. The intent of this program was that medical documentation could be electronically transferred to flight medics during a rushed MEDEVAC and that documentation would persist in the soldier's medical record all the way from theatre to VA. I was disappointed to learn, however, that despite the time we spent on training, this program did not work and the notes I drafted never left the expensive device I carried in theatre. Instead, I had to re-draft documentation that was filed manually and, hopefully, not lost during a soldier's trip through recovery.

As a veteran, I experienced the challenges associated with health data lost due to a lack of interoperability between the DoD and VA. After I left the military, I sought physical therapy from VA to continue treatment on my wrist that I fractured on my last deployment. Despite being certain of my broken wrist diagnosis, having seen the Xrays of the fracture myself, my VA physician told me that my wrist was never broken because there was no documentation for it and no copy of the Xray image in my file. As a result, I had to seek physical therapy through private insurance.

As a civilian, I have seen how the digitization of medical records has greatly accelerated patient care and innovation. While in medical school at Johns Hopkins University, I was fortunate to be able to participate in research using electronic medical records during Hopkins transition from multiple electronic health record systems to one central system that currently spans the entire enterprise. While this upgrade made it easier to share health information, the magnitude of sharing is quite expansive. Not only do immediate care team members have access to a patient's record, but also any workforce member across the enterprise can now access any patient's record. Partner, affiliate, other business associates can also access patient data through health exchanges or other data-sharing programs. Both this increase in exposure and Hopkins's goal of being an innovation hub for health data allowed the opportunity to launch the startup that I now run.

At Protenus, we've developed artificial intelligence that proactively audits how every end-user accesses and uses electronic health information to ensure health systems are compliant with regulations designed to protect patient privacy. With our technology, we've seen first-hand how access to health data can be abused, causing harm to the health system and patients alike. And we've also seen how access to health data, when governed correctly, can spur amazing innovations that ultimately help improve patient care overall.

I've seen, first-hand, the limitations and risks associated with antiquated health technology systems. I've also seen how using technology in healthcare can create a slew of privacy and security challenges. So, privacy or innovation? The answer is both. We must find a way to promote innovation through accessibility and sharing. But we also must ensure that we do everything we can to protect health data from falling into the wrong hands. This is especially true of our veterans who deserve the best we can offer. The best we can offer combines both innovation and privacy.

This is an opportunity for VA to set a higher standard. As technology continues to improve and create better access, so too must our standards for security and privacy continue to meet that standard, as well.

Prepared Statement of Tina Olson Grande

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.

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

[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.")

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 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 startups 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 dis-

[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").

ease, 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 decisionmaking 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

2020 HLC MEMBERS

Neil de Crescenzo - Chair
President & CEO
Change Healthcare

Terry Shaw
President & CEO
AdventHealth

Karen Lynch
EVP CVS Health & President Aetna Business Unit
Aetna

Steve Collis
Chairman & CEO
AmerisourceBergen

Corinne Le Goff
SVP, GM, U.S. General Medicine
Amgen

Susan Salka
President & CEO
AMN Healthcare

Gail Boudreaux
President & CEO
Anthem

Joseph Impicciche
President & CEO
Ascension

Gerald Petkau
Interim CEO & COO
BlueCross BlueShield of North Carolina

J. D. Hickey
CEO
BlueCross BlueShield of Tennessee

Adam Lenkowsky
General Manager, Head US Commercial
Bristol-Myers Squibb

Brent Shafer
Chairman & CEO
Cerner

Robert Stone
President & CEO
City of Hope

Tom Mihaljevic, M.D.
President & CEO
Cleveland Clinic

Harry Totonis
CEO
ConnectiveRx

Emad Rizk
CEO
Cotiviti

James Hereford
President & CEO
Fairview Health Services

Alexander Hardy
CEO
Genentech

Marc Grodamn, M.D.
Founder & CEO
Genosity

Helmy Eltoukhy
CEO
Guardant Health

Bill Lucia
President & CEO
Health Management Systems

Hossam Sadek
President, US & Canada
IQVIA

Calvin Schmidt
Sr. Vice President and Worldwide Leader, Government Affairs & Policy
Johnson & Johnson

Jonathan Scholl
President, Health
Leidos

Hugh O'Neill
EVP & Chief Commercial Officer
Mallinckrodt

Susan Turney, M.D.
CEO
Marshfield Clinic Health System

Gianrico Farrugia, M.D.
President & CEO
Mayo Clinic

Brian Tyler
CEO
McKesson

Tarek Sherif
Chairman & CEO
Medidata Solutions

Omar Ishrak
Chairman & CEO
Medtronic

Barry Arbuckle, Ph.D.
President & CEO
MemorialCare Health System

Riad El-Dada
President, Global Human Health,
U.S. Market
Merck

Andrew Lukowiak
CEO
Millennium Health

Steven Corwin, M.D.
CEO
NewYork-Presbyterian Hospital

J.P. Gallagher
President & CEO
NorthShore University HealthSystem

Mike Gladstone
Global President, Internal Medicine
Pfizer

Susan DeVore
CEO
Premier healthcare alliance

Chris Wing
CEO
SCAN Health Plan

Peter Ross
CEO & Co-Founder
Senior Helpers

Laura Kaiser
President & CEO
SSM Health

Tim Scannell
President & COO
Stryker

Tom Skelton
CEO
Surescripts

Jason Gorevic
CEO
Teladoc Health

Barclay Berdan
CEO
Texas Health Resources

Donaton Tramuto
CEO
Tivity Health

Duane Barnes
President
UCB

Neil Kurtz, M.D.
Executive Chairman
Vineti

Byron Jobe
President & CEO
Vizient

Jaideep Bajaj
Chairman
ZS Associates

ABOUT THE CONFIDENTIALITY COALITION

The Confidentiality Coalition is a broad group of organizations working to ensure that we as a nation find the right balance between the protection of confidential health information and the efficient and interoperable systems needed to provide the very best quality of care.

The Confidentiality Coalition brings together 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, clinical laboratories, home care providers, patient groups, and others. Through this diversity, we are able to develop a nuanced perspective on the impact of any legislation or regulation affecting the privacy and security of health consumers.

We advocate for policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, supporting policies that enable the essential flow of information that is critical to the timely and effective delivery of healthcare. Timely and accurate patient information leads to both improvements in quality and safety and the development of new lifesaving and life-enhancing medical interventions.

Membership in the Confidentiality Coalition gives individual organizations a broader voice on privacy and security-related issues. The coalition website, www.confidentialitycoalition.org, features legislative and regulatory developments in health privacy policy and security and highlights the Coalition's ongoing activities.

For more information about the Confidentiality Coalition, please contact Tina Grande at tgrande@hlc.org or 202.449.3433.

MEMBERSHIP

AdvaMed
AdventHealth
America's Health Insurance Plans
American Hospital Association
American Society for Radiation Oncology
AmerisourceBergen
Amgen
AMN Healthcare
Anthem
Ascension
Association of American Medical Colleges
Association of Clinical Research Organizations
athenahealth
Augmedix
Blue Cross Blue Shield Association
BlueCross BlueShield of North Carolina
BlueCross BlueShield of Tennessee
Cerner
Change Healthcare
CHIME
Cigna
Ciox Health
City of Hope
CLEAR
Cleveland Clinic Foundation
College of American Pathologists
ConnectiveRx
Cotiviti
CVS Health
Datavant
dEpid/dt Consulting Inc.
Electronic Healthcare Network Accreditation Commission
EMD Serono
Express Scripts
Fairview Health Services
Federation of American Hospitals
Genentech
Genetic Alliance
Genosity
Guardant
Healthcare Leadership Council
Health Management Systems
HITRUST
Intermountain Healthcare
IQVIA
Johnson & Johnson
Kaiser Permanente
Leidos
Mallinckrodt
Marshfield Clinic Health System
Mayo Clinic
McKesson Corporation
Medical Group Management Association
Medidata Solutions
Medtronic
MemorialCare Health System
Millennium Health
Memorial Sloan Kettering Cancer Center
Merck
MetLife
National Association of Chain Drug Stores
National Community Pharmacists Association
NewYork-Presbyterian Hospital
NorthShore University HealthSystem
Pfizer
Pharmaceutical Care Management Association
Premier healthcare alliance
SCAN Health Plan
Senior Helpers
SSM Health
State Farm
Stryker
Surescripts
Teladoc Health
Texas Health Resources
Tivity Health
UCB
UnitedHealth Group
Vineti
Vizient
Workgroup for Electronic Data Interchange
ZS Associates

Revised February 2020

PRINCIPLES ON PRIVACY

1. All care providers have a responsibility to take necessary steps to maintain the confidentiality and trust of patients as we strive to improve healthcare quality.

2. The framework established by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule should be maintained. HIPAA established a uniform framework for acceptable uses and disclosures of individually-identifiable health information within healthcare delivery and payment systems for the privacy and security of health information to enable the provision of health care services to patients. HIPAA follows the widely accepted Fair Information Practices standards (FIPS.)

    a. The HIPAA Privacy Rule, through "implied consent," permits the sharing of medical information for specified identified healthcare priorities which include treatment, payment and healthcare operations (as expected by patients seeking medical care.) This model has served patients well by ensuring quick and appropriate access to medical care, especially in emergency situations where the patient may be unable to give written consent.

    b. The HIPAA Privacy Rule requires that healthcare providers and health plans limit disclosure of protected health information to the minimum necessary to pay for healthcare claims and other essential healthcare operations. This practice provides privacy protection while allowing for continued operations. Minimum necessary is relatively easy and simple to administer and practice.

3. Personal health information must be secured and protected from misuses and inappropriate disclosures under applicable laws and regulations.

4. Providers should have as complete a patient's record as necessary to provide care. Having access to a complete and timely medical record allows providers to remain confident that they are well-informed in the clinical decision-making process.

5. Privacy frameworks should be consistent nationally and across sectors so that providers, health plans, and researchers working across state lines and with entities governed by other privacy frameworks may exchange information efficiently and effectively in order to provide treatment, extend coverage, and advance medical knowledge, whether through a national health information network or another means of health information exchange.

6. The timely and accurate flow of de-identified data is crucial to achieving the quality-improving benefits of national health information exchange while protecting individuals' privacy. Federal privacy policy should be consistent with the HIPAA regulations for the de-identification and/or aggregation of data to allow access to properly de-identified information. This allows researchers, public health officials, and others to assess quality of care, investigate threats to the public's health, respond quickly in emergency situations, and collect information vital to improving healthcare safety and quality.

7. For the last 20 years, the HIPAA privacy standards have engendered consumer trust. Any future legislation or rulemaking that addresses identifiable health information should conform with consumers' expectations.

Beyond HIPAA Privacy Principles

1. For the last 20 years, the HIPAA Privacy and Security Rules have engendered public trust that individually identifiable health information collected by providers and insurers (HIPAA covered entities) would be disclosed only for health functions like treatment, payment processing, and safety, and not used or disclosed for other purposes without an individual's authorization. Any future legislation or rulemaking that addresses individually identifiable health information should not conflict with HIPAA's Privacy and Security Rules.

    a. HIPAA's required "Notice of Privacy Practices" provides an overview of individuals' rights as well as permitted and required uses and disclosures of identifiable health information.

    b. HIPAA's approach requires use of risk-based administrative, technical, and physical safeguards allowing organizations the flexibility to implement policies and controls commensurate with the level of risks they have identified.

2. Congress should establish a single national privacy and security standard for *all* health information *not* subject to HIPAA. This single standard:

    a. Should not conflict with HIPAA,
    b. Should not disrupt day to day practices for HIPAA Covered Entities and Business Associates,
    c. Should align with HIPAA's definitions of health information, and
    d. Should adopt a risk-based approach like HIPAA.

3. Individuals may not fully appreciate that individually identifiable health information collected outside of a HIPAA Covered Entity or Business Associate Agreement are not afforded HIPAA privacy and security protections. Individuals should be given clear, succinct notice concerning collection, use, disclosure, and protection of individually identifiable health information that is not subject to HIPAA.

4. Individual authorization processes (including revocation of authorization) for use and disclosure of identifiable health information not covered by HIPAA should be written in a meaningful and understandable manner and should be easily accessible to individuals prior to and after information is used or shared.

5. Entities that hold or collect identifiable health information have a responsibility to take necessary steps to maintain the trust of individuals. Entities that are not HIPAA Covered Entities or Business Associates that hold identifiable health information should clearly stipulate the purposes for which they collect, use, and disclose identifiable health information.

6. Individuals must provide authorization for entities outside of HIPAA to collect individually identifiable health information. Such information collected, used or disclosed by entities outside of HIPAA should be limited to only that information needed to accomplish the purposes for data collection. This practice provides privacy protection while allowing for continued innovation.

7. Individuals should be informed of their right to seek redress – from the entity and from regulators – in the case of unauthorized access, misuse, or harm attributable to how their identifiable health information was collected, used or disclosed.

8. Penalties and enforcement must be meaningful in order to discourage misuse and unpermitted collection, use or disclosure of identifiable health information.

Prepared Statement of Ramsey Sulayman

Chairwoman Lee, Ranking Member Banks, and members of the subcommittee, on behalf of the men and women of the Veterans of Foreign Wars of the United States (VFW) and its Auxiliary, thank you for the opportunity to address the issues of data privacy and portability and our members' expectations of the Department of Veterans Affairs' (VA) responsibilities to protection their privacy.

As the Department of Defense (DOD) and VA move toward a joint electronic health care record (EHR), veterans' information will become more accessible for VA and DOD providers and their community partners. This is a good thing. The concentration of personal data in a joint electronic health care record also makes the record more desirable for nefarious actors from foreign governments, non-State actors, and criminals acting as part of organized crime groups or individually. In 2018, the White House Council of Economic Advisers estimated that cybercrime cost the United States' economy between $57–109 billion. A person's health record contains a vast amount of personally identifiable information that can be used for ill.

While the loss or compromise of veterans' health care data certainly comes with an economic cost, it also carries the non-quantifiable costs in the loss of dignity, trust, and confidence. In creating an EHR that can communicate and easily exchange data with other government agencies, as well as commercial health care systems, insurers, and private providers, VA must ensure that veterans' information remains secure when it leaves the VA ecosystem. VA must also ensure that control of data remains with VA and the veteran, and define the expectations for data retention and control with community partners. VA is responsible for ensuring that sufficient protocols are in place to guard against an unthinkable trusted insider intrusion or even simple unauthorized access.

The VFW is not opposed to commercial off-the-shelf solutions; there is no need for VA to reinvent the wheel when it comes to technological solutions. Creating information technology (IT) solutions is not the VA's core strength. Therefore, the strongest possible privacy protections from third-party vendors must be in place. Very specific policies and procedures must be in place that address data collection, data use, transfer of information, and information retention, in particular through End User License Agreements (EULA). EULA are the terms of service that must be accepted, often unilaterally, for a veteran to use an app or website. EULAs generally incorporate a privacy policy that specifies the four criteria above. As mentioned, EULAs are often "take it or leave it" terms. The difference between the effects of a EULA on a commercial site and a EULA on a VA site is that veterans who opt to "leave it," risk losing access to benefits and services earned through service. VA has a monopoly on administration of veterans' health care and benefits. Whereas monopolies in the commercial market are largely outlawed, so consumers are able to seek service from a competitor if they "leave it" in the private sector.

Beginning with EULAs, VA must ensure that partners collect the minimum amount of information, have the shortest retention time possible, and provide clear opt-in criteria. Opt-in was not a slip of the tongue. Veterans and service members should have to opt-in to data *collection* rather than opt-out; the strictest criteria and the most minimal collection should be the standard. We will address health care data sharing, which the VFW supports as an opt-out, later in this testimony. Data collection must be limited to only necessary and pertinent data. Tracking a veteran's data from usage of specific sites is not necessary to the conduct of that veteran or service member's business with VA or DOD.

As an example, VA is in the process of consolidating all its veteran facing websites into its updated VA.gov portal. To access their VA.gov portal, veterans are prompted to sign up with ID.me, without a reliable alternative. The use of the ID.me login credentials places veterans in the unique position of having to accept the terms of service and privacy policy in the EULA in order to log on and access VA benefits earned through service. The ID.me process is much easier and reliable, for example, than acquiring a DSLogon account or other VA log on if the veteran is not enrolled in the VA health care system or with the Veterans Benefits Administration, or is no longer active in the Defense Enrollment Eligibility Reporting System (DEERS) or the Defense Financial and Accounting Service (DFAS). While the ID.me EULA and privacy policy specifically states that no veteran information will be sold by ID.me, it also specifically states that data may be transferred to partner websites that have a different privacy policy over which ID.me has no control. In other words, to use ID.me services, a veteran's information may be transferred to a trusted ID.me partner. However, the EULA does not guarantee ID.me's partners will not sell or utilize that data for a commercial purpose, including aggregating it with other sources that may personally identify the veteran.

The security of veterans' health information is of paramount importance. As health care technology advances and more details become available through diagnostic and genetic testing, that information will become more concentrated in locations like the EHR. The VFW urges VA to place the highest priority on security and utilizing the strongest possible technological solutions to safeguard veterans' health data.

Project Nightingale, a joint commercial venture between Google and Ascension Health, the Nation's second-largest health care system, underscores some of these issues surrounding data collection and utilization. Google partnered with Ascension to digitize the health records of Ascension's patients and then apply tools such as artificial intelligence (AI) to look for patterns. While some of these patterns related to early prediction of disease or better treatments for existing conditions, one of the goals of the program was also to see where more revenue could be squeezed out of care. While the attempt to use health care data to generate new revenue streams is of concern, the larger philosophical concern is that patients' private health care data may migrate to Google *without the prior consent of patients*. Ascension could provide these records because, under the *Health Insurance Portability and Accountability Act of 1996* (HIPPA), Google is a business associate of Ascension helping Ascension execute administrative functions necessary to the provision of health care. I use Ascension as an example because Ascension very actively marketed its services to veterans participating in the VA Veterans Choice Program. Ascension is a fine health care system noted for its quality of care, but what is important for VA and veterans is that a veteran who uses Ascension (or any other health care system that has external partners with big data programs) does not automatically have his or her health care information vacuumed into a program to which he or she did not consent by virtue of existing business partners or covered entity relationships between health care providers, systems, or insurers and data focused enterprises.

Provider records, however, is not the only kind of health care information that people generate. User-generated data, such as that from wearable devices like FitBit, are not covered by HIPAA. I pick on FitBit versus Apple Health or Huawei Health because FitBit is owned by Google. One can see that the acquisition of health care data from HIPAA-protected sources and unprotected user generated data is a major effort for Google. Google is not alone, though. Apple, Amazon, Facebook, and Microsoft are but a few of the major established information technology players also working on cornering the big data market in health care. The combination of data from FitBit users whose data is also contained in Project Nightingale leads to questions about what that data and its commercialization will lead to.

Smaller players like Xealth are also in the market and working on similar products and initiatives. Xealth, which has attracted investors that include the Cleveland clinic, University of Pittsburgh Medical Center, Atrium Health, and Amazon, has developed a product where health care providers can check off products and services from a digital shopping list, and offer or prescribe them to patients as part of the visit or consultation. Patients can then use the recommendations from Xealth to order products, services, and prescriptions directly from vendors, including Amazon. Even excluding the sharing or leakage of health data, purchasing patterns of consumer goods can lead to predictions about health conditions. For example, the purchase of compression socks, syringes, and testing strips can be analyzed to determine that a consumer suffers from diabetes – all from non-HIPAA protected information.

Genetic information adds to the mix and can present daunting questions of privacy. While major commercial providers of DNA testing for purposes of determining ancestry and genealogy are pretty good about requiring opt-in for certain information sharing, and informed consent for research purposes, they also note that they are not required to comply with HIPAA and that they may store and share information, including genetic information, with their service or business partners. As with EULAs, these partners may have different privacy policies, and one has to review *all* the privacy policies of *all* partners. Other sites, for instance GEDmatch, make all genetic information submitted publicly available. It is estimated that 60 percent of Americans who are of Northern European descent can be identified through data in public data bases, with that figure expected to rise to 90 percent in the next few years.

How does this affect veterans? VA's Million Veteran Program (MVP) immediately comes to mind. VA is merging the health care and genetic data of veterans who opt-in in a landmark study that has revolutionary implications for the provision of health care. However, little is discussed about data security, and what is available is not in plain language. However, VA does note that "There could be a slight risk of a breach of confidentiality, and if information about you does leak out, the VA

will not be able to guarantee that it will be protected." VA must do what it takes to ensure a breach does not occur. The VFW also urges VA to be more transparent about the policies and procedures in place to assure data safety, and provide prominent links to the full policies, as well as plain language translations.

While all this when placed in a certain context may be Orwellian, we must not see a conspiracy around every corner. Health care data sharing can yield immense benefits. As much as we believe that medicine is science, it is also art and relies heavily on providers' experience and judgment. At a certain point, the symptoms of a common cold can look an awful lot like those of a life-threatening disease, or a major medical event such as an aneurysm, heart attack, or stroke. Growing up in a medical family, I have heard enough anecdotes about medical miracles and missed diagnoses that I could churn out scripts for tearjerkers on the Hallmark Channel indefinitely into the future. Often, these missed moments or life-saving revelations were the result of experience and noticing details that may have been overlooked, or were not in a provider's experience base. Technology can help solve this.

A doctor can have a patient's entire medical history at hand without relying on the limitations of a patient's memory or self-reporting. The availability of the complete medical record can allow the doctor to make a more informed diagnosis. That diagnosis can be checked by an impartial AI system that might see patterns missed in the rush of an emergency room visit on a busy day. User-generated information from health trackers can objectively report a patient's activity levels, sleep, and other vitals without having to rely on memory and self-reporting from patients who may be in crisis or less than one hundred percent. Amalgamated, de-identified patient data can be searched, and research populations identified, with big data tools in a fraction of the time as in the past by hand. There are benefits, but the benefits must balance the risks, and we must look at what may be possible in the future versus what we merely see as possible today.

The laws governing privacy rights, particularly with electronic data, are more of a patchwork than a comprehensive whole. HIPAA was passed in 1996, in an era before big data when records were kept locally and on paper before today's computing power was available. For reference, Amazon was merely an online book seller and my Apple Macintosh LC 3 had a whopping 80 megabytes of memory. The VFW applauds this subcommittee for looking at this issue intently and, ever so importantly, with an eye to the effects from the perspective of veterans. As institutions that safeguard the rights for which our veterans fought, and as organizations that represent our veterans' best interests, we must ensure that privacy and security, or information, particularly health data, is paramount and that veterans remain in control.

This concludes my statement. Thank you for your time and I look forward to answering any questions you may have.

Prepared Statement of Harold F. Wolf, III

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 dialog 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 toward 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.

If you are a non-governmental witness, please list any federal grants or contracts (including subgrants or subcontracts) related to the hearing's subject matter that you or the organization(s) you represent at this hearing received in the current calendar year and previous two calendar years. Include the source and amount of each grant or contract. If necessary, attach additional sheet(s) to provide more information.

Government Grants time frame of January 1, 2018 through January 31, 2020					
Grant Name	**HIMSS Amount**	**Domestic/Foreign**	**Grant Period**	**Government Agency**	**Description**
CNI/Chickasaw Nation (CDC grant #200-2016-92117)	394,337.00	Domestic	Jan 1 2018 - Jan 31 2020	Center for Disease Control	Subcontractor - HIMSS works with CNI to provide Immunization Guidance and Test Scripts. HIMSS has been a subcontractor since Phase IV in 2016. The team is currently on Phase 7.
IHE/ONC (IHE/ONC Cooperative Agreement #90AX0027)	129,620.00	Domestic	Sept 5 2019 - Sept 30 2024	Department of Health & Human Services	Subcontractor - HIMSS personnel supporting the IHE USA grant focused on coordination with ONC, HL7, IHE members, and industry partners to lead and participate in testing the updated IHE profiles at connect-a-thons and other events that promote and sustain the adoption of FHIR standard.

Government Contracts time frame of January 1, 2018 through January 31, 2020					
Company Name	**Domestic**	**Total Amount**	**Analytics/Maturity Model**	**Events/Thought Leadership**	**Membership**
ACT Government, Digital Solutions Dept	Domestic	34,800.00			x
Alabama Medicaid Agency	Domestic	10,275.00			x
Alameda County Medical Center	Domestic	6,750.00			x

Arkansas Department of Health	Domestic	3,375.00			x
California Dept of Health Care Serv, Ofc of HIPAA Compliance	Domestic	6,750.00			x
Cook County Health & Hospitals System	Domestic	19,050.00			x
County of Santa Clara Health System	Domestic	3,375.00			x
Cuyahoga County	Domestic	10,000.00		x	
Defense Health Agency	Domestic	370,000.00			x
Department of Veteran Affairs	Domestic	14,000.00		x	x
DHHS/ONC	Domestic	205,695.00	x		
Georgia Department of Community Health	Domestic	6,750.00			x
Georgia, USA	Domestic	168,250.00		x	x
Harris Health System	Domestic	10,125.00			x
Hennepin County Medical Center	Domestic	6,750.00			x
HRSA: Health Resources Services Administration	Domestic	6,865.00			x
Indian Health Service	Domestic	28,990.00			x
Indiana Health Information Exchange	Domestic	3,900.00			x
Lake County Health Department and Community Health Center	Domestic	3,375.00			x
Los Angeles County Dept of Health Serv	Domestic	3,375.00			x

MaineHealth	Domestic	19,050.00			x
Michigan Health Information Network Shared Services	Domestic	20,825.00		x	x
Michigan Public Health Institute	Domestic	16,785.00			x
National Association of County & City Health Officials	Domestic	12,000.00		x	
National Center For Health Statistics	Domestic	9,725.00		x	
National Consortium of Telehealth Resource Centers	Domestic	20,700.00		x	
National Government Services	Domestic	89,100.00		x	x
National Institutes of Health	Domestic	40,000.00	x		
New Mexico Human Services Department	Domestic	6,750.00			x
New York City Health and Hospitals Corporation	Domestic	11,190.00			x
San Francisco Health Plan	Domestic	6,750.00			x
San Mateo County Health System	Domestic	7,925.00			x
Social Security Administration	Domestic	6,750.00			x
Texas Health & Human Services	Domestic	5,595.00			x
Veterans Administration – Office of Health Informatics	Domestic	9,525.00			x
Veterans Administration – Office of Informatics	Domestic	9,525.00			x
Washington State	Domestic	14,330.00		x	

Wisconsin Department of Health Services	Domestic	6,750.00			x

If you are a non-governmental witness, please list any contracts or payments originating with a foreign government and related to the hearing's subject matter that you or the organization(s) you represent at this hearing received in the current year and previous two calendar years. Include the amount and country of origin of each contract or payment. If necessary, attach additional sheet(s) to provide more information.

Government Contracts time frame of January 1, 2018 through January 31, 2020					
Company Name	Foreign	Total Amount	Analytics/Maturity Model	Events/Thought Leadership	Membership
Airedale NHS FT	Foreign	1,163.94	x		
Alberta Health Services	Foreign	28,990.00			x
Alder Hey Children's NHS	Foreign	13,429.28	x		
AOU Policlinico Bologna	Foreign	999.18	x		
ASST di Vimercate	Foreign	12,223.30	x		
ASST Papa Giovanni	Foreign	1,332.24	x		
Auckland District Health Board	Foreign	6,850.00			x
AUSL Reggio Emilia ASMN - IRCCS	Foreign	144.17	x		
Australian Defence Force	Foreign	32,400.00			x
Australian Digital Heath Agency (ADHA)	Foreign	15,000.00		x	

Bedford Hospital NHS Trust	Foreign	6,954.47	x		
Berkshire Healthcare NHS	Foreign	2,316.27	x		
Berlin Partner für Wirtschaft und Technologie GmbH	Foreign	9,096.04			x
Birmingham & Solihull Mental Health NHS FT	Foreign	1,163.98	x		
Bradford Teaching Hospitals NHS Foundation Trust	Foreign	1,167.74	x		
Cambridge University Hospital NHS	Foreign	25,893.47	x		
Centre Hospitalier de Nord	Foreign	1,310.04	x		
Centro Hospitalar do Porto	Foreign	999.18	x		
Chelsea & Westminster NHS	Foreign	1,176.23	x		
Clatterbridge Cancer Center NHS	Foreign	6,264.53	x		
Direccion General de Agenda Digital del Gobierno de la Rioja	Foreign	13,322.40	x		
Dubai Health Authority	Foreign	87,657.00	x		
eHealth Aargau	Foreign	264.87		x	
EOC - Ente Ospedaliero Cantonale	Foreign	999.18	x		
Finnish Ministry of Social Affairs and Health	Foreign	140,903.07		x	
Frimley Health NHS Foundation Trust	Foreign	1,001.81	x		
Gateshead Health NHS	Foreign	7,594.18	x		

Glintt Healthcare Solutions SA	Foreign	22,204.00	x		
Gloucester NHS FT	Foreign	1,163.94	x		
Government of Quebec	Foreign	36,800.00		x	
Guy's and St. Thomas NHS Foundation Trust	Foreign	7,655.21	x		
Health Informatics New Zealand	Foreign	4,933.21	x	x	
Helse-Sorost	Foreign	1,937.30	x		
Hopital du Valais	Foreign	999.18	x		
Hospital 12 de Octubre	Foreign	6,550.18	x		
Hospital Cascais Dr. Jose de Almeida	Foreign	1,217.94	x		
Hospital de Denia	Foreign	15,143.13	x		
Hospital Universitario 12 de Octubre	Foreign	6,075.56	x		
IKEM - Institute of Clinical and Experimental Medicine	Foreign	6,328.14	x		
Imperial College Healthcare NHS Trust	Foreign	6,400.28	x		
INSIEL S.p.A.	Foreign	13,322.40	x		
Instituto Portugues de Oncologia do Port (PT) HE19-0065	Foreign	2,021.94	x		
IRCCS Instituto Ortopedico Rizzoli	Foreign	999.18	x		
IRCCS Istituto Nazionale dei Tumori	Foreign	999.18	x		

ISMETT	Foreign	999.18	x		
Joint Health Command, Australian Defence Force	Foreign	12,000.00			x
Kantonsspital Winterthur	Foreign	999.18	x		
Korea Health Industry Development Institute	Foreign	92,590.79	x		
Lancashire Care NHS Doundation Trust	Foreign	1,021.00	x		
Lancashire Teaching FT	Foreign	999.18	x		
Leeds Teaching Hospitals NHS Trust	Foreign	999.18	x		
Liverpool University Hospitals	Foreign	2,586.63	x		
Liverpool Womens NHS	Foreign	6,890.98	x		
Luton and Dunstable University Hospital NHS	Foreign	24,489.30	x		
MCL Leeuwarden	Foreign	5,551.00	x		
Medipol	Foreign	264,682.42	x		
Milton Keynes University Hospital NHS	Foreign	11,813.02	x		
Ministry of Health - New Zealand	Foreign	125,200.00	x		
Ministry of Health Republic of Slovakia	Foreign	17,318.08	x		
Ministry of Health Republic of Slovakia	Foreign	16,097.90	x		
MOH Office For Healthcare Transformation	Foreign	7,000.00			x

National Guard Health Affairs	Foreign	95,333.56	x		x
National Healthcare Group Pte Ltd	Foreign	21,600.00			x
Nemocnice Na Homolce Hospital	Foreign	2,775.50	x		
Newcastle upon Tyne Hospitals NHS Trust	Foreign	11,829.58	x		
NHS Birmingham CrossCity CCG	Foreign	66,906.97	x		
NHS South Worcestershire CCG	Foreign	42,625.03	x		
Norfolk and Norwich University Hospitals NHS FT	Foreign	28,914.35	x		
North Tees Hospital	Foreign	1,164.21	x		
Northampton General Hospital NHS	Foreign	2,322.08	x		
Norwegian Centre For Ehealth Research	Foreign	16,149.20		x	
Nottinghamshire Healthcare NHS Foundation Trust	Foreign	49,959.00	x		
Ontario Government	Foreign	67,975.00		x	x
Oslo Universitetssykenhus HF	Foreign	5,551.00	x		
Oxford University Hospitals	Foreign	999.18	x		
Pennine Acute Hospitals NHS Trsut	Foreign	6,359.99	x		
Queensland Health	Foreign	184,567.25		x	
Region Skane	Foreign	11,324.04	x		

Region Uppsala	Foreign	7,662.60	x		
Royal Berkshire NHS Trust	Foreign	7,316.45	x		
Royal Free London NHS Foundation Trust	Foreign	7,816.81	x		
Royal Liverpool Broadgreen University Hospitals NHS Trust	Foreign	11,102.00	x		
Salford Royal NHS	Foreign	5,939.95	x		
Service de la promotion économique et du commerce (SPECo)	Foreign	29,732.19		x	
Sheffield Health & Social Care NHS FT	Foreign	1,939.97	x		
South Tyneside and Sunderland NHS Foundation Trust	Foreign	12,501.72	x		
Spital Region Oberaargau	Foreign	999.18	x		
St. Antonius Ziekehuis	Foreign	999.18	x		
St. Helens & Knowsley Hospitals	Foreign	6,467.81	x		
Taunton & Somerset NHS FT	Foreign	8,791.60	x		
Taunton and Sommerset NHS Trust	Foreign	359.02	x		
The Christie NHS Foundation Trust	Foreign	20,551.35	x		
The Royal Liverpool and Broadgreen University Hospitals NHS Trust	Foreign	1,058.50	x		
Turkish National Pavilion - METU TTO	Foreign	42,025.00		x	
ULB Hospital Erasme	Foreign	999.18	x		

Uni Hospital Southampton NHS	Foreign	6,594.67	x		
University Hospital Southampton NHS FT	Foreign	1,616.60	x		
West Suffolk NHS Foundation Trust	Foreign	7,921.76	x		
Wirral University Teaching Hospital NHS	Foreign	6,940.54	x		
Worcester Health & Care NHS Trust	Foreign	12,674.47	x		
Wye Valley NHS Trust	Foreign	7,113.00	x		
York Teaching Hospitals NHS Foundation Trust	Foreign	6,487.46	x		