AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

HEARING ON SAFEGUARDING VETERANS' MEDICAL INFORMATION WITHIN THE VETERANS HEALTH ADMINISTRATION

HEARING

BEFORE THE

SUBCOMMITTEE ON HEALTH

OF THE

COMMITTEE ON VETERANS' AFFAIRS

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JUNE 21, 2006

Serial No. 109–55

Printed for the use of the Committee on Veterans' Affairs

U.S. GOVERNMENT PRINTING OFFICE

28–451 WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON VETERANS' AFFAIRS

STEVE BUYER, Indiana, *Chairman*

MICHAEL BILIRAKIS, Florida
TERRY EVERETT, Alabama
CLIFF STEARNS, Florida
DAN BURTON, Indiana
JERRY MORAN, Kansas
RICHARD H. BAKER, Louisiana
HENRY E. BROWN, Jr., South Carolina
JEFF MILLER, Florida
JOHN BOOZMAN, Arkansas
JEB BRADLEY, New Hampshire
GINNY BROWN-WAITE, Florida
MICHAEL R. TURNER, Ohio
JOHN CAMPBELL, California

LANE EVANS, Illinois,
Ranking Member
BOB FILNER, California
LUIS V. GUTIERREZ, Illinois
CORRINE BROWN, Florida
VIC SNYDER, Arkansas
MICHAEL H. MICHAUD, Maine
STEPHANIE HERSETH, South Dakota
TED STRICKLAND, Ohio
DARLENE HOOLEY, Oregon
SILVESTRE REYES, Texas
SHELLEY BERKLEY, Nevada
TOM UDALL, New Mexico
JOHN T. SALAZAR, Colorado

JAMES M. LARIVIERE, *Staff Director*

SUBCOMMITTEE ON HEALTH

HENRY E. BROWN, Jr., South Carolina, *Chairman*

CLIFF STEARNS, Florida
RICHARD H. BAKER, Louisiana
JERRY MORAN, Kansas
JEFF MILLER, Florida
MICHAEL R. TURNER, Ohio
JOHN CAMPBELL, California

MICHAEL H. MICHAUD, Maine,
Ranking Member
BOB FILNER, California
LUIS V. GUTIERREZ, Illinois
CORRINE BROWN, Florida
VIC SNYDER, Arkansas

CONTENTS

JUNE 21, 2006—HEARING ON SAFEGUARDING VETERANS' MEDICAL INFORMATION WITH THE VETERANS HEALTH ADMINISTRATION

Page

OPENING STATEMENTS

Chairman Henry E. Brown 1
Prepared statement of Chairman Brown 23
Hon. Michael H. Michaud, Ranking Democratic Member 2
Prepared statement of Congressman Michaud 30

STATEMENT FOR THE RECORD

Hon. Corrine Brown 19
Prepared statement of Congresswoman Brown 32

WITNESSES

Kussman, Brig. Gen. Michael J., M.D., M.S., MACPP (US Army Ret), Principal Deputy Under Secretary for Health, Veterans Health Administration, Department of Veterans Affairs 4
Prepared statement of Dr. Kussman 37
Seliger, Robert, Chief Executive Officer and Co-Founder, Sentillion, Inc., and Chair, Steering Committee for Integration and Interoperability, Healthcare Information and Management Systems Society (HIMSS) 6
Prepared statement of Mr. Seliger 46

POST-HEARING QUESTIONS FOR THE RECORD

Hon. Michael H. Michaud 54
Hon. Corrine Brown 61

HEARING ON SAFEGUARDING VETERANS' MEDICAL INFORMATION WITH THE VETERANS HEALTH ADMINISTRATION

WEDNESDAY, JUNE 21, 2006

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON HEALTH,
COMMITTEE ON VETERANS' AFFAIRS,
Washington, DC.

The subcommittee met, pursuant to call, at 10 a.m., in room 334, Cannon House Office Building, Hon. Henry Brown (chairman of the subcommittee) presiding.

Present: Representatives Brown of South Carolina, Michaud, Turner, Brown of Florida, and Snyder.

Mr. BROWN of South Carolina. Good morning. The Subcommittee will now come to order. We are holding this hearing today to address the vulnerability of VA's electronic medical records system and examine the access and control policies VA employs and the compliance mechanism VA uses to safeguard sensitive, personal veterans' health information from internal and external security threats.

The value of VA's electronic medical records system was evident in VA's response to Hurricane Katrina. During Hurricane Katrina, VA doctors and nurses were able to treat without interruption patients transferred from VA facilities in New Orleans to VA hospitals in Houston. Because of the system's electronic medical records, all patients' records were backed up, securely transported to Houston, and were back on line and available almost immediately.

At the same time, however, there are risks with holding such sensitive and personal information electronically, and the lack of a solid VA information security program greatly troubles me.

The personal and sensitive data of our nation's veterans must be handled with the utmost care. The burglary of the home of a Department of Veterans Affairs employee that included a data file with personal information on millions of veterans is simply unacceptable.

The Department of Veterans Affairs is working with the FBI to thoroughly investigate this matter, and this Committee will be closely monitoring this situation to help ensure that such an occurrence is not repeated.

We must make sure that there are explicit and clear security and confidentiality policies to protect the health information of our nation's veterans. To that end, we are interested today in hearing

from those at the Department that the most sensitive information, individually identifiable health information is currently being protected.

Additionally, in light of the recent theft, I am interested in knowing what the VA anticipates doing to better protect this information in the future and what steps, if any, have already been taken.

Through a series of hearings set up by the Chairman of our full Committee, Chairman Buyer, we have been able to closely examine data integrity and security issues from a number of different perspectives, but today we have the opportunity to specifically focus on health-related information.

In addition to having assembled the cast before us from the VA, we have also taken the opportunity to speak with folks from the private sector. I for one welcome the opportunity to hear what is currently being considered state-of-the-art in the private sector and then benchmarking that standard against VA's current practices. Today we have this opportunity.

I would like to personally thank all of our witnesses for being here today. And with that, I now yield to our Ranking Member, Mr. Michaud, for an opening statement.

[The statement of Henry Brown appears on p. 23]

Mr. MICHAUD. Thank you very much, Chairman Brown, and thank you for holding this very important oversight hearing. VA's electronic patient record system remains the technological force behind VA's state-of-the-art care. It can save lives as well as money.

Last week, the VA Inspector General issued a report on VA's procedure for outsourcing medical record transcriptions. The report showed that the VA had weak controls over the veterans' medical records. In 2005, a subcontractor in India contacted the IG and threatened to expose thousands of patients' records over the internet if the subcontractor was not paid.

This allegation and the IG audit showed the VA was incapable of controlling or detecting where a contractor had medical information transcribed or who had access to it. VA's procedure for acquiring medical transcription services from contractors failed to address basic security requirements.

Of the VA facilities surveyed, 91 percent did not remove personal identifiers such as patients' names and Social Security numbers before transmitting the data to contractors for transcriptions.

I agree with the IG that the VA needs to do this work with VA staff because this is not a practical way to ensure that contractors safeguard patients' protected health information.

As the IG report says, and I quote, "The inability to control confidential information in an era of global outsourcing leaves protected health information unprotected and patients subject to identity theft," end of quote.

Given the clear risk with outsourcing, I cannot understand why this Administration and the Office of Management and Budget identified the jobs in medical information or records as ones that should be studied for outsourcing.

I look forward to hearing from Dr. Kussman about the VA's effort to improve controls on medical transcriptions.

Chairman Brown, I commend you for your leadership in holding this hearing so that we can better understand what the Veterans

Health Administration has done and what they will do to preserve the security and privacy of veterans' medical records.

Also, Mr. Chairman, I would like my full opening statement to be submitted for the record. Thank you.

Mr. BROWN of South Carolina. Okay. Without objection. Thank you, Mr. Michaud.

[The statement of Michael Michaud appears on p. 30]

Mr. BROWN of South Carolina. Mr. Turner, do you have an opening statement?

Mr. TURNER. Mr. Chairman, I want to thank you for holding this hearing. I appreciate your continuing to give information to the Subcommittee members and the members of the full Committee on this important issue, and I would like permission to submit an opening statement for the record.

Mr. BROWN of South Carolina. Without objection.

[No statement was submitted.]

Mr. BROWN of South Carolina. Dr. Snyder.

Mr. SNYDER. No thank you.

Mr. BROWN of South Carolina. Okay. On our first and only panel representing the Department of Veterans Affairs, we are honored to have Brigadier General Michael J. Kussman. Dr. Kussman was appointed Deputy Under Secretary of Health for the Veterans Health Administration on May 29, 2005.

In this capacity, he leads the clinical policy and programs for the nation's largest integrated healthcare system. Among his many accomplishments, Dr. Kussman served as the Army Surgeon Generals chief consultant in internal medicine and governor for the Army Region of the American College of Physicians in 1988.

From March 1993 to August 2005, he commanded Martin Army Community Hospital at Ft. Benning, Georgia and later commanded the Walter Reed healthcare system in Washington, DC, where he was promoted to Brigadier General.

Following his tour at Walter Reed, Dr. Kussman served as commander of the Europe Regional Medical Command and was responsible for healthcare throughout Europe, the Middle East, and Africa.

Dr. Kussman is accompanied by Mr. Craig B. Luigart, VHA Chief Information Officer; Dr. Robert Kolodner, Chief Health Information Officer; Ms. Stephania Putt, VHA Privacy Officer; and Ms. Gail Belles, VHA Technical Security Advisor.

Also I want to welcome Mr. Robert Seliger. He's the CEO and Co-Founder of Sentillion. Mr. Seliger has led the company in creating security solutions that improve information access and work flow for customers in the healthcare information technology industry. He is widely recognized as a visionary at the forefront of converging technical markets and clinical trends in healthcare.

Prior to co-founding Sentillion, Mr. Seliger was a senior R&D manager and chief architect at an International Team responsible for development of Hewlett Packard's medical products group's largest portfolio of clinical information systems products.

Presently he chairs the Healthcare Information and Management Systems Society Steering Committee for Integration and Interoperability. We are very pleased to have him at our hearing today.

Dr. Kussman, before you begin, I gave you all those accolades. I want to chastise you just a bit for the lateness of your prepared remarks to the Committee. We certainly wish you would be a little bit more responsive and a little bit more timely getting the information to us so we will have a better opportunity to review testimony before it is actually presented.

But with that, we will now start with you.

STATEMENTS OF BRIG. GEN. MICHAEL J. KUSSMAN, M.D., PRINCIPAL DEPUTY UNDER SECRETARY OF HEALTH, VETERANS HEALTH ADMINISTRATION, DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY ROBERT KOLODNER, M.D., CHIEF HEALTH INFORMATICS OFFICER, VHA, DEPARTMENT OF VETERANS AFFAIRS; STEPHANIA PUTT, PRIVACY OFFICER, VHA, DEPARTMENT OF VETERANS AFFAIRS; GAIL BELLES, TECHNICAL SECURITY ADVISOR, VHA, DEPARTMENT OF VETERANS AFFAIRS; AND ROBERT SELIGER, CHIEF EXECUTIVE OFFICER AND CO-FOUNDER, SENTILLION, INC., CHAIR, STEERING COMMITTEE FOR INTEGRATION AND INTEROPERABILITY, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY

STATEMENT OF MICHAEL J. KUSSMAN

Dr. KUSSMAN. Good morning, Mr. Chairman, and Ranking Member, other members of the Committee.

First, let me say that I apologize for the lateness of the statement, and I have talked to Counsel and we clearly need to do better and we will.

Mr. BROWN of South Carolina. Well, I know you are under a lot of pressure from a lot of different groups to prepare remarks, but we do need to try to resolve this problem we have. But, anyway, we are grateful to have you here today.

Dr. KUSSMAN. Yes, sir. This is a partnership and we need to do better. So thank you for your comments.

Thank you for allowing me to provide an overview of the data management and security procedures that the Veterans Health Administration employs to ensure the safety and integrity of veterans' electronic health records and to safeguard sensitive personal veteran information from internal and external security threats.

Before I proceed with my review of our security and privacy procedures, I want to assure both you and our nation's veterans that the recent data breach did not include any of the Veterans Health Administration's electronic health records.

VHA views data privacy and security as a fundamental operational pillar. We are committed not only to ensuring that our veterans receive the best healthcare but that we also fully protect the security and privacy of their paper and electronic health records.

VHA is responsible for protecting data on all systems that facilitate the delivery of healthcare benefits to our nation's veterans. Similar protections are provided for the databases that contain the veteran health records exchanged between the Department of Defense and VA. We protect many important health databases and systems that enable us to provide quality care to our veterans.

Our core electronic health records system is VISTA. This widely acclaimed system has saved the lives of thousands of veterans, but it was designed 20 years ago and, as such, it is principally hospital based and is deployed in more than 100 locations. This distributed nature does not lend itself to simple security compliance.

Today network and telecommunications standards and solutions exist to assist in mitigating these risks while creating greater efficiency and effectiveness, and a wide range of security and privacy procedures protect VISTA and other VHA systems.

For years, VHA has required that all employees and contractors complete annual privacy and security training. VA policy is that anyone needing access to our data to perform their duties, whether a provider, a researcher, or veteran service officer, must be granted explicit approval for that access.

This is just the beginning. VHA also develops its own policies and guidance focused on healthcare-specific issues and implements sophisticated technical controls to protect the veterans' health records.

VHA carefully controls access to sensitive data. Only those who have a legitimate and demonstrated need are granted access to sensitive information. Even then, users' access is limited to the information needed to do their jobs.

VHA also employs security measures to protect VA systems and data when VHA employees and contractors perform work outside of VA offices. All external connections into the VA network are protected by a virtual private network, VPN, which provides secure, remote access. VPN access requires management approval and approved users are required to sign and abide by a rules of behavior document that must be in place before access is granted.

Across this nationwide network of systems, VHA applies many other security controls. These include intrusion detection systems that monitor and detect intruders, encryption of sensitive data exchanged with DoD, routine backups of data on our critical systems, and continuity of operations, processes, and procedures.

VHA is committed to continuing to strengthen our security and privacy controls. To this end, VA is investigating the use of encryption solutions appropriate for our information systems and data protection needs that will be adopted for use across VHA.

VHA is reengineering current applications that will broaden auditing capabilities. We are enhancing our current role-based access control capabilities to provide granularity with user-defined roles. And VHA has taken the lead in developing role-based access control enhancements that are being evaluated for national and international endorsement.

To further strengthen security and privacy, VHA has identified a number of specific actions for strengthening data security procedures that are in the planning stages or have been identified as a result of the data security breach as follows:

Provide and mandate centrally deployed security solutions; implement a department-wide encryption solution that encrypts data that is sent across VA networks; increase the use of secure web-based solutions for e-mail, scheduling, and other administrative needs; require that portable media and laptops have the capability to encrypt all sensitive data and that appropriate guidance tools

training are provided to the users to implement these solutions effectively; and update VA and VHA security policies to address changes in technology's current IT environments.

To further emphasize the importance of security, VA is planning a department-wide Security Awareness Week for workforce members from June 26 to 30 June with daily briefings on proper security practices. VHA is taking the lead for coordinating the week.

In addition, to help veterans, VA will set up information booths across the VA so that veterans can get information on identity theft and data protection.

In closing, let me reiterate that we see data privacy and security as a fundamental operational pillar. We are committed to providing the best possible care to our nation's veterans, and we will do everything in our power to fully protect the security and privacy of their health records. For our veterans, for the men and women who have fought so bravely for our country, anything else is unacceptable.

And I might close, if you would not mind, sir, with a personal comment. As a veteran and a retiree, I have received a letter from the Secretary as well. It was not a surprise to me obviously, but I did receive the letter. And I can assure you that myself and others of us who are in that same situation take this very, very seriously both on a personal and professional basis.

Thank you.

Mr. BROWN of South Carolina. Thank you, Dr. Kussman, for your testimony.

Dr. Kolodner, we will take your testimony next. I am sorry. Mr. Seliger. We will get to you later. Okay.

[The statement of Michael Kussman appears on p. 37]

STATEMENT OF ROBERT SELIGER

Mr. SELIGER. Chairman Brown, Mr. Michaud, distinguished members of the Committee, thank you for the opportunity to testify before you today on a subject of critical importance for our Nation's veterans, but also to every citizen, how to safeguard sensitive personal health and related information from external and internal security threats.

My name is Robert Seliger, and I am Co-Founder and CEO of Sentillion. Sentillion is the industry leading provider of identity and access management solutions to hospitals and healthcare systems. Every day Sentillion helps hundreds of institutions and hundreds of thousands of physicians, nurses, and other caregivers at those institutions employ effective security and privacy practices while also facilitating the care-delivery process.

We are exceedingly proud to say that among these institutions are all 163 medical centers of the Departments of Veterans Affairs.

To further introduce myself, I have 26 years of experience in the field of health information technology. I have served on numerous Standards Committees and have chaired a variety of healthcare industry initiatives.

Recent activities include serving as Chair for the HIMSS Steering Committee for Integration and Interoperability and serving as an advisor on standards uptake for the Pan-Canadian Electronic Health Records Standard Steering Committee.

Today I want to focus on one aspect of the complex challenge of safeguarding patient data in a clinical setting, and that is how can we safeguard patient data without also impeding the care-delivery process? Practicing safe and effective medicine will always take precedence over concerns for security and privacy.

Our nation's nurses and physicians are among the smartest, most highly-trained people in the world. This fact coupled with their deep sense of mission will compel them to avoid, work around, and challenge policies that impede the care-delivery process. This is because the care-delivery process by its very nature requires immediate information access and the constant sharing of information with others.

As a simple example, consider the seemingly trivial tasks of logging onto a computer in order to access patient data and then logging off the computer when done. These actions are almost never performed in the hospital. Instead computer accounts are shared in order to avoid logging in and no one logs off.

The reason is that a caregiver in a busy hospital might need to log on and off 50 to 100 times a day. At a minute or two for each log on and log off, you can quickly see how this seemingly trivial best practice is avoided because it interferes with the pace of providing care.

And so our nation's physicians and nurses practice good healthcare, but leave millions of personal computers across the country open to access or even simple perusal by any passerby from other healthcare workers with no valid reason to view the information to other patients to people visiting patients to anyone else who might be in the hospital.

I would like to assert that the security and privacy challenge that the healthcare industry faces are not just attacks from outside but also transgressions from within. The question is, how do we as a nation change the situation without compromising the care-delivery process?

Data that we have from a study we conducted shows that under circumstances in which log-on and log-off times were reduced to just a few seconds, nurses in one hospital who only logged off 50 percent of the time were now doing so 100 percent of the time. And physicians who were not logging off at all were now doing so 86 percent of the time.

This change in behavior was not due to a new policy or the threat of punitive measures. Rather, we simply made it easier for caregivers to behave as good security and privacy citizens.

The challenge we face is to make sure that the things we do to keep the bad guys out do not effectively prevent letting the good guys in. This is about making sure we engineer security and privacy solutions from a work-flow perspective and not attempt to force upon healthcare organizations mechanisms that make sense for other types of environments but which do not make sense for healthcare.

Delivering effective healthcare is an intense and complicated process. It is also a truly mission-critical process. Our industry must find the right balance between applying security and privacy measures that are known to work and applying measures that could be detrimental to patient care.

We can assert, for example, that every caregiver must have a password for each application that they use, but what, in fact, are we asking our caregivers to do if they need to remember ten different passwords and enter each one in dozens of times a day?

To truly safeguard patient security and privacy requires a broad set of measures. These measures include not only good network security and the appropriate encryption of data but also involves tools and mechanisms that enable good people, well-meaning people to do their jobs without compromising patient health, patient security, or patient privacy.

Mr. Chairman, this concludes my remarks. Thank you for the privilege of speaking before you today. I am happy to answer any questions the Committee may have.

[The statement of Robert Seliger appears on p. 46]

Mr. BROWN of South Carolina. And I thank you very much for your testimony and also Dr. Kussman. Have you all met before?

Mr. SELIGER. I am sorry?

Mr. BROWN of South Carolina. Have you all met before?

Mr. SELIGER. No.

Mr. BROWN of South Carolina. Okay. Well, I think you both bring a great perspective to the process. And, in fact, I will ask you the first question if I might.

Your testimony makes a number of sound points. I wonder if you could expand a bit on the relative importance of auditing electronic access to records. I mean, security protocol and audit capabilities are one thing, but actually doing the audit and understanding who is using the data is quite another.

What security features should a healthcare system like the VA contain?

Mr. SELIGER. Well, the audit process begins with being able to establish the identity of the people using the system. In the example I just gave that people are not logging in, and I am using the same accounts as Dr. Kolodner or Dr. Kussman here, then an audit is irrelevant because you do not really know who is actually using the computer.

So the best audit processes begin with establishing mechanisms that enable caregivers to want to, to easily sign on and sign off the computers, and do so in a secure manner, so each person is uniquely identified. Once we have that, we can then record the access and make appropriate conclusions about whether those accesses were appropriate or not.

Mr. BROWN of South Carolina. Dr. Kussman, do you all have a system similar to this or how do you control and audit the users?

Dr. KUSSMAN. Yes, sir. Thank you for the question.

I believe we do have a process that identifies the people not only that have access to the system but makes sure that the people who have access need to have access.

You know, we talk in the security realm about need to know. That is only part of it. The question is need to have. I mean, a lot of people like to have access to things that they do not necessarily need to have.

From a clinical perspective, obviously, as was mentioned, our primary mission is to provide the state-of-the-art care to our veterans, and the electronic health record is a modality of delivery of care.

For us, it is the same as a stethoscope or an EKG machine or CAT scan, and it has become part of our culture and used daily.

I might ask Dr. Kolodner, who is an expert on this, to maybe illustrate further how that is done.

Dr. KOLODNER. Yes. Thank you very much.

Each of our users has their own account and a two-level password, both of which are private, so the physician or nurse will log on and access the patient.

We also have a third password for the electronic signature. If I am entering data, I have to add that additional password, which means that I cannot come in behind someone else and use the system since I would not know their electronic signature password.

We reinforce the importance of protecting passwords to our providers on a regular basis, and we actually take action for those who violate the log-off, log-on procedures in our facilities.

Dr. KUSSMAN. Sir, I might add just one other thing is that in many ways, the electronic health record has improved the security dramatically and access to information or protection of information because many of us are old enough and dinosaurs before the electronic health record. And when we had hard copy, the records would sit around, if you will. They would be on a nurse's station or on a doctor's desk or in a records room. And in many ways, anybody could come up and pick up that record and read something about the patient. It was very difficult to have physical security on this.

So what Dr. Kolodner has been mentioning is a quantum leap improvement, I think, in security in keeping that information private.

Mr. BROWN of South Carolina. Is it password protected on different segments so the record has different levels of authority and certain controls over parts of the record?

Dr. KOLODNER. Yes. We have a series of access controls in our current system. And based on the work that we have been doing, we have been developing a much more sophisticated system called role-based access that defines what parts of the record a particular individual should be allowed to read from or write to based on the role that they are serving or playing in the facility.

We have taken that schema for the role-based access to the standards development organizations, working in conjunction with our Department of Defense and with Kaiser Permanente colleagues, and it has passed the ballot for an international standard.

So we do already have a process in our current process for controlling that access, and we are devising and planning to implement in our next generation system an even more sophisticated system.

Mr. BROWN of South Carolina. Since the theft of those records, have you done anything different to put in place policies that would further identify in the audit if there has been a breach within your own areas and indicate who might be using this data? Are there other security measures you put in place since the event?

Dr. KUSSMAN. Yes, sir. As you know, that from a healthcare perspective, we always had a very sophisticated and controlled program known as the Health Information Portability and Account-

ability Act, the HIPAA, and that put in place a great deal of standards different than nonhealthcare data.

And that has been inculcated into the culture of all healthcare delivery systems because everyone knows if you breach that, not only are you doing something wrong as far as an ethical, moral thing, but you can really be hurt financially and potentially go to jail for it.

So there is a great deal of sensitivity about controlling healthcare information. So that was already the foundation. Because of this breach of information, and as we have said, thank goodness it was not involved with healthcare data, but it certainly has sensitized us immensely to that.

And I might ask Ms. Putt, who is our privacy manager, and Gail, our security people, to comment on what are some of the newer things that we have looked at in respect to the breach.

Ms. BELLES. Actually, we have taken a number of steps to address issues. One thing that we have done is to issue a data access inventory to all of our VA personnel. We are identifying the access to sensitive data for every individual in our workforce, employees, contractors, students, residents, et cetera. That is a major undertaking for us. We are planning to get the results back from that access inventory at the end of June.

The Security Awareness Week, we talked about. We are going out to the entire workforce to give briefings on the importance of security and privacy and the things that need to be done to protect patient data so that it is not compromised at any time.

There has been policies that have been updated, rewritten to address remote access to our systems and data. We have actions to bring groups together to look at encryption methodologies for laptops and portable media so that we can address that area which we know is vulnerability.

So a number of good steps as a result of this.

Mr. BROWN of South Carolina. Let me just follow-up on that statement. The access inventory—you will not get a response until the end of June. How often would you get a report if somebody accessed a file that should not be there? If somebody accessed a file, they would have to have access to some password. But what does the access inventory do for you?

Ms. BELLES. What that does is provides us with a list of the entire workforce and the systems, the sensitive data that they have, and how they access it. So if they access it remotely or if they access it from an office or they access it in paper form, we can identify that and we can also look very closely at the appropriateness of those accesses.

As far as individuals accessing medical records, we have audit trails that are logged on a continuous basis and are reviewed by the facility information security officers on a regular basis to ensure that with managers that the individuals accessing these records or accessing these options have the need to know.

Mr. BROWN of South Carolina. And how timely is that review?

Ms. BELLES. I am sorry?

Mr. BROWN of South Carolina. How timely is that review?

Ms. BELLES. It is a real-time recording of the audit.

Mr. BROWN of South Carolina. Right.

Ms. BELLES. I think it's probably a 30-day review by the ISOs.

Dr. KUSSMAN. Sir, if I might add to that. With our inventory review, we are going out and looking at not only who have laptops but who have access to that virtual network that I talked about, the VPN, because over a period of time, organizations, there may be more people who have access than we think we really knew need to have.

Many people may be using it just for e-mail and they do not need the laptop for that. We have Blackberries and other ways of doing that. So we are doing a very close scrub on who has laptops and what are they doing with them, and then also educating people very closely on what their responsibility is if they have a laptop.

I mean, you can have it and need VPN access both when you are going some place. You have a responsibility to protect that laptop in a hotel or a restaurant or even in your car. And on top of that, you should not carry as much as possible any information that if indeed the laptop was stolen for some—I mean, obviously we cannot prevent somebody from holding somebody up on the street and taking their laptop, but we certainly would not want any information on there or as little information on there that would be incriminating or sensitive in any way.

Mr. BROWN of South Carolina. That leads me to my next question, and this will be my last question. I notice that your written testimony referenced the Department's interest in starting to encrypt the data that is sent between VA sites. Is there some specific reason why that has never been seen as appropriate before?

Dr. KUSSMAN. Yes, sir. Let me just make a comment that our VPN network is already encrypted. And so there is a significant amount of encryption that goes forward. And if everybody stayed within the firewall, if you will, using the encryption, then indeed we have much less of a potential problem.

The question is that in data that even flows within the system or somebody downloaded something to their hard drive, can that bypass the VPN encrypted nature? And so we are looking at that. But that really is not only a VHA responsibility, it's a VA-wide responsibility to look at encryption, and we would want to coordinate that with the VA CIO so we have one system of encryption.

Would either one of you like to add to that?

Ms. BELLES. I will just add that several years ago, we transformed from what we had in place for our network was IDCU, which is a private network, and we have gone to a more open network.

So at the time we had the IDCU, we did not require any encryption between the facilities. But now that we are in this environment where we have a more open network, we need to look at encryption between the facilities.

Mr. BROWN of South Carolina. Thank you very much for your testimony.

And, Mr. Michaud.

Mr. MICHAUD. Thank you, Mr. Chairman.

Dr. Kussman, I just want to reiterate what Chairman Brown had mentioned in his opening as far as questioning. I, too, was concerned about the lateness of your testimony, and have not had a chance to go through it.

And I know next week, we have a hearing on Tuesday and VA's testimony is supposed to be in tomorrow. So hopefully we will be able to, you know, have your testimony tomorrow for next week's hearing.

Dr. Kussman, in your testimony, you state that VA contracts forbid the transfer of veterans' protected health information outside the jurisdiction of the United States. A couple of questions.

How will you monitor compliance with that provision? Can you give us total and complete assurance that absolutely no VA contractor will use an overseas subcontractor to transcribe veterans' medical information?

Dr. KUSSMAN. Yes.

Mr. MICHAUD. How will you monitor the provision?

Dr. KUSSMAN. Sir, that is written into the contract and the contractors have to abide by the same security issues that we have in-house that is part of the contract.

The issue that you are describing, I am well aware of, that took place. We did not realize, quite frankly, that the contractor had subcontracted. When we found out, we stopped that and we have prohibited that from occurring again.

Mr. MICHAUD. Okay. Thank you.

And are you confident that the VA can control veterans' private and personal medical information while it is outsourced for medical transcriptions here in the United States?

Dr. KUSSMAN. Yes, sir. As you are well aware of, we are a large organization. We talked about the need to balance the delivery of healthcare with safety. They are not mutually exclusive. I mean, they are together.

We with our contractors will leave no stone unturned, no process unlooked at to protect the privacy and security of all our veterans. And if indeed there is a mishap, we will have in place processes that will aggressively and quickly address those issues and be sure that we inform the veterans.

As you know, we have a very elaborate safety program that we do. We have briefed you and others on similar types of issues related to safety. We have an open environment. There are no secrets. We try to make sure that both you and other supervising entities as well as the patients know what we are doing.

So I believe we have in place and we will aggressively enforce all the security needs to protect our patients.

Having said that, as you know, the gold standard in this country is the airline industry and FAA, as I mentioned to you earlier, and we all feel fairly secure when we get on an airplane. Unfortunately, even with everything, airplanes do not work the way that they are supposed to and there are accidents.

We will put in and aggressively put in all the processes that would minimize and mitigate any situations that we can anticipate. But to tell you a hundred percent that it will never happen again, you know as well as I that that would be difficult to do.

Mr. MICHAUD. Thank you.

Also in your testimony, you state that the VA conducts an annual system-wide ongoing assessment and review strategy called SOARS.

What did SOARS identify to be the most significant privacy and security threat to VA's medical health data system both internal and external?

Ms. PUTT. Mr. Congressman, I do not have that information at this time on the finding of the SOARS assessment specifically. I do have information on other assessments.

Mr. MICHAUD. Would you be able to provide the Committee with the SOARS assessment?

Ms. PUTT. I think we can.

Dr. KUSSMAN. Yes, sir. The SOARS has been a very successful program for us. It has been a self-induced, self-initiated program that looks at a whole gamut of things much like a mini joint commission assessment would volunteer. And it was originally volunteers. The facilities were not required to do this. But it has been successful, everybody asks for it. So effectively it is a guaranteed program.

One of the things that we have always looked at but will look at more closely is the issue of data security. I am not aware that that has been a major problem for us that has come up in the SOARS, but we will look back at that. And with your indulgence, we will report back to you for the record on that.

Mr. MICHAUD. Thank you.

VA researchers can have access to databases with Social Security numbers identifying veterans. I understand that researchers must go through an approval process to get access codes to this database.

What does VA do after a researcher has access to ensure that such data is not downloaded, put on a laptop or extended hard drive or otherwise put at risk of being lost or stolen and how do you enforce this policy?

Dr. KUSSMAN. Yes, sir. Thank you for the question.

We are aware of that situation. We monitor it very closely. As you alluded to, that anybody who does research has to apply for that. There are standards that have to be met. It is part and parcel of the approval in the Institutional Review Boards at the facilities that approve the human research and protect the patients, and it is not only protection for their clinical things, but it is also protection of their information and their rules and regulations on what the researcher can do and what they can transport.

But I will ask Gail or Stephania to elaborate on that.

Ms. PUTT. Thank you.

As stated, researchers/investigators do have to follow the privacy and security of protecting their research information as outlined in their research protocol that is approved by the Institutional Review Board.

The data that they use and collect cannot be used for any other purpose without going back to the Institutional Review Board for approval. They must also follow policies regarding the protection of human subjects and their data for research to ensure that the information is not shared with affiliates or colleagues who are not VA employees or do not have legal authority to see the information, and they have to safeguard it in accordance with policies if it is placed on any laptops or other devices.

Mr. MICHAUD. But the question was, what does the VA do after they do all the research? What does the VA do after the researcher

has access to all this information? How do you know that they do not download it or make copies on another CD?

Ms. PUTT. VA researchers should follow policies that prohibit them keeping the data after the research study has concluded. Once the study has concluded and they have maybe published their results, they are supposed to destroy the data or return the data. They are not to keep it to use for future research projects.

Mr. MICHAUD. On that same line of questioning, how does the VA enforce a policy for researchers from taking the stuff home?

Ms. PUTT. There is a Research Compliance Office that is responsible for reviewing researchers' activities in terms of their research protocols and what they are doing in terms of their studies, along the same lines with the protection and security of their information.

I do not have any more information on the processes of the Research Compliance Office, but facilities do actually have Research Compliance Officers at some of the facilities who are responsible for reviewing the researchers' activities.

Mr. MICHAUD. Not being a computer whiz, how confident are you that the researchers do not take this information home? Is there any way that you can find out? I mean, just how confident are you?

Dr. KUSSMAN. I guess I got the look to answer the question.

Sir, through the Office of Research Oversight, they do random samples. They look at that. They look at a process under which people adhere to the processes. We set that up—it used to be called ORCA. It is now the ORO, the Office of Research Oversight—to really look at this.

Part of the reason was to look at this issue because the researchers do research. And sometimes, just like anybody else, you could get a little lax about what you are doing. And so we needed to have a process under which we looked at that.

Does every protocol need to be looked at? No. We believe that the process is valid. Because of this, we will relook at our thing to see if it needs further strengthening. But to some degree, we have to trust the people who signed the pieces of paper who say that they are following what we have told them to do.

We believe that the process that we have in place works pretty well because I am not aware of a significant or any episodes where things have been lost or sensitive data has been compromised. It is not to say that it could not have happened.

Mr. MICHAUD. My last question for you, Dr. Kussman, not knowing whether it can be done or not, can you prevent any information, any of the data that you have from being downloaded? Is the technology available to do that and, if so, are you doing that?

Dr. KUSSMAN. Whether it is research or otherwise?

Mr. MICHAUD. That is correct.

Dr. KUSSMAN. Using the VPN network, and I might ask Dr. Kolodner to comment on it, my understanding—and I am a dinosaur when it comes to this stuff too. I can just use e-mail and that is about—or a little WordPerfect and that is it. But it is not easy to download using the VPN process, and it is encrypted.

The issue of downloading, as we said, that at the place of work, people can download things into their computer. We are aggressively looking at an encryption process that would protect that as

well. So whatever was downloaded and making the presumption that the person had need to have this information, it was not done for any other spurious reason, that it would be encrypted and very difficult to get access to if the computer was compromised in any way, shape, or form.

So we are clearly getting better and learning as we move along. Rob, would you like to comment?

Dr. KOLODNER. The downloading that might occur would take place mostly inside the firewalls at the office, and there are some business reasons why one might need to do that.

As part of this access review, we are examining who has access to bulk data, confirming if they need access, and, what constraints we have on that access.

To reiterate, there are business reasons why sometimes someone needs to download such data. We just need to know about that and to know that the proper controls are in place, the proper agreements have been signed, and a periodic review is done.

Mr. MICHAUD. So if there is a business reason why they have to download information, would they have to get approval first?

Dr. KOLODNER. Yes. They would have to have requested approval, had their supervisor present that request to their information security officer, and then been given approval based on that justification.

Mr. MICHAUD. Great. Thank you.

My last question which will go to Mr. Seliger, again not being familiar with technology, I have seen situations, and as you described in your testimony, when going through a hospital, you see someone's medical record up there on the screen, people can see it.

And I can understand where it would be cumbersome to log off, log on quite frequently, which will take time, but I have also seen technology, particularly actually in Maine, with Bangor Mental Health, where when the employees punch in to go to work, they use their finger which identifies the employee.

Is the technology available so if someone wants to access quickly a medical record that you can use your thumbprint to open up the system and then a certain time frame, it automatically goes off? Is that something that your organization has looked at and might be available?

Mr. SELIGER. The answer is yes. We have a number of hospitals and healthcare organizations in the private sector using technology exactly as you described. For the record, I would like to point out it is not your thumbprint but any of the other three fingers that one tends to use for technical reasons.

But having said that, we have caregivers who are using interesting combinations of devices. So fingerprint, as you said, for authentication, but also devices that are called active proximity devices, not much bigger than my card holder here, and they detect your arrival or departure from a workstation. And the operative word here is departure. When you leave the vicinity of a computer, it locks it up. Okay?

So having to remember—and this is the kind of technologies I was alluding to in my testimony, being able to accommodate the caregiver work flow. Imagine yourself in an emergency room com-

ing and going, patients coming and going, computers all over the place. Even if it was fast, you still have to remember to do it.

And by equipping caregivers with devices to make the log-on process fast and easy, to make the log-off process implicit by just leaving, we can achieve the kind of safeguards I alluded to and actually facilitate the care-delivery process. People are actually going to use the computers rather than paper as Dr. Kussman referred to, which is still the primary source of information data in most healthcare organizations in a general sense.

Now, the VA itself has made a number of steps to be, I guess the better way of putting it, quite pioneering in a number of regards relative to information security in the caregiver workplace.

And as recently as this summer, we are proud to be working with the VA at its Hines Facility on a project that has been code named Medical Sign-On which is about taking this process, these work flows with good security to a whole other level. We will pilot at Hines, work out the kinks, make sure it works properly, and then hopefully have a basis to roll this out to the other VA medical centers.

Dr. KUSSMAN. Sir, we also have instituted a program where the computers would automatically log off in five minutes is what we are doing. It drives me crazy in my office because I will have logged on, I will answer the phone, and then I have got to log back in and things. But it certainly works, I can assure you, because it logs off and then I have to log back in.

That would be the same thing around the system, whether it is a nurse's station or anything else, that if a nurse walks away or a physician walks away, if they do not get back on and they are not sitting there within five minutes, it automatically logs off. It is an irritant to people, but it is a protection.

Mr. MICHAUD. If I might, Mr. Chairman.

Is the VA looking at the same technology that was just talked about as far as using your——

Dr. KUSSMAN. We are looking at that and I think it will be looked at as an agency issue with the CIO of whether we are going to embark on that technology or not. I do not have enough information. I do not think any of us know how much that would cost or whatever.

Would you like to comment on that?

Ms. BELLES. We are working on a Medical Sign-On pilot with Sentillion at Hines as Mr. Seliger said. We are looking at all kinds of technologies that can improve that interface for clinicians and nurses so that we do not have a situation where people just get up and walk away because they are called out for an emergency or other things.

You know, we have been in the position where the clinicians come to us and say you have got to make this process better for us. And Sentillion is partnering with us to find out the right methods to do that.

Mr. MICHAUD. Thank you very much.

Thank you, Mr. Chairman.

Mr. BROWN of South Carolina. Okay. Thank you, Mr. Michaud.

Dr. Snyder, do you have a question?

Mr. SNYDER. I do. Thank you, Mr. Chairman.

Dr. Kussman, it is good to see you again and your colleagues there.

You got me curious, Dr. Kussman, with what I thought was a bit of a cryptic response when you were gently chastised for your tardy statement here, which I know you try to get them here, when you made some mention of lawyers or legal opinions or something.

And I always remember the old Art Linkletter show, Kids Say The Darnedest Things, and his best question always was, is there anything your mother did not want you to talk about to tell us on the show today.

And so now I am curious. Did your statement get overly scrubbed by OMB and you had to redo it or were there things that you had included in your original statement that caused you to make that reference to lawyers or legal folks?

Dr. KUSSMAN. I am sorry. I do not remember what I said.

Mr. SNYDER. But was there some delay in the process? The Congress has lots of problems with folks that want to do opening statements and tell us things, and the statements, anything written goes through OMB and gets scrubbed, and we do not get the information we want.

And I was just curious if there were some things that you had intended to tell us that got removed in the process of your statement being approved for delivery to the Congress.

Dr. KUSSMAN. Not that I am aware of. So I am not even sure I can give you a thorough explanation of why, other than people being busy as the Chairman mentioned and lots of hearings. And all I can say is they apologize for the delay and we will do everything we can to prevent that from happening.

Mr. SNYDER. You had mentioned the days of written records which a lot of medical facilities still rely on. And I remember, and I do not know how long ago, it was 15 years ago or so when I was still practicing medicine. I had seen this young boy. I can still see him in the exam room. He was about eight. And his grandmother asked me about some behavioral things that he was doing.

And sometimes medicine is like doing a crossword puzzle. You know, a week later, you think, oh, that is what that answer was. Well, I knew right away that the kid had Tourette's and I just did not—it did not come to my mind when I was talking to the grandmother.

Well, we had an all-handwritten medical section. I could not remember anything. We could not figure out who the boy was. So I had one staff member who over several Saturdays, because we were slow, it was a slower day, went through every medical record, opened up and tried to find the chart.

Now, if we had had a computerized system, we could put in an approximate age range. I think I even remember what the diagnosis was I actually saw him for. We could have pulled up those charts. We never did find the chart.

I always felt bad about that because I can still see that little boy sitting there probably being chastised by his grandmother for some of his behavioral stuff. I suspect that he had Tourette's.

So my point is, while we had those written records, there was a built-in protection which is it is a pain in the butt to go through those written records trying to find something compared to having

access to a CD that holds, you know, 500,000 Social Security numbers of veterans or something, which is the issue that we are dealing with.

I want to pick up on what Mr. Michaud said, was asking about the research aspect of this and the ability of people to take information off.

My first question is, why does the VA—and this is years and decades before you got there, Dr. Kussman—why does the VA have to use Social Security numbers? Why do your researchers have to use Social Security? Why do they even have to have that? Why do the researchers even have to have the name? Why can you not develop a program for the researchers that would delete name, birth date, Social Security number throughout the medical record, pretty much throughout the medical record?

There might be a reference in a note that, well, he was born in the same year as his, you know, twin sister. But they do not have to have the name or Social Security number or birth date. All they need is an identifying, this is subject number one whose age is 23.

Have you all considered that as part of your security, of getting away from using Social Security numbers and what information those researchers have to have?

Dr. KUSSMAN. Thank you for that question.

As you probably know, it was not so long ago when we did not use Social Security numbers. The military had a military ID number that transposed to the VA when the person left——

Mr. SNYDER. Though we all still remember, right?

Dr. KUSSMAN. Yes, I remember. I had a military ID. I am old enough to have one of those, just like I would not say you are old, sir, but——

Mr. SNYDER. No. And I also got a letter by the way.

Dr. KUSSMAN. And I think it was 1970 or 1971, and somebody correct me, where the military decided to go to Social Security numbers, and we went along with that. I do not think anybody anticipated the second, third, fourth level effects of the Social Security number and it became so valuable.

It was not so long ago that when you tried to cash a check in the military PX or something, you had to write your Social Security number on the check to get it. They have stopped doing that because people rose up in righteous indignation. But the Social Security number became the key to almost everything, and we kind of went along.

I think there are a lot of people looking at this now to determine whether or not we ought to just get away from the Social Security number for one thing and go back to some other type of identification number, and that would have to be done in conjunction with a government-wide thing, I think, particularly with DoD for us.

The other part of the question was do we need to have that information in research things or any sensitive information, and the answer is I do not think we need it in each case.

And another thing that we are looking at is what information is needed for people to do their job, whether it is research or administrative things. Do they need to have dates of birth, Social Security numbers, and things like that?

And I might ask Ms. Belles to add to that.

Ms. BELLES. I do not think I have much to add to that. As Dr. Kussman said, there are a lot of groups that are looking at the issue of SSNs as identifiers.

I know that in our environment, we use the SSN for patient safety reasons, to ensure that we have got the right veteran when we are providing care. But outside of that, it is an issue. I know it has been an issue for a number of years, talked about across government agencies.

And at this point, I do not think we have come to a resolution. But certainly with everything that is going on around us related to identity theft and the importance of protecting SSNs, we need to address it.

Dr. KUSSMAN. I think, Doctor, you hit the nail on the head. The good thing about the electronic health record and other electronic process is you do not have to carry big things. I mean, nobody is going to go out of the office with two tons of records to get anything or it limited what you did.

So electrifying the records is a good thing. The bad thing is now we are confronted with the challenge of protecting that information because people in a small thumb thing can walk out with lots of records. So it is a balance and we are learning how to handle that.

Mr. SNYDER. I notice the clock. The only comment I would make is I think the reality is we are not going to be able to protect that information. We are all going to try and try and try.

The reality is, I think we are going to have to get to the point where financial institutions will not accept some handwritten things scrawled out by the new person who moves into the house that I lived in ten years ago and some mass mailing got there ten years too late and they will accept that.

I think we are going to have to go to—I mean, I would think banks would want to go where we have to walk in and have a picture made and three fingerprints just to get a card because there is no way we are going to protect this information.

Thank you, Mr. Chairman.

Mr. BROWN of South Carolina. Thank you, Dr. Snyder.

Ms. Brown, do you have a question?

Ms. BROWN of Florida. Yes, sir. Thank you, Mr. Chairman and Ranking Member, for hosting this hearing on this subject.

And I got to tell you it is very disturbing to me, 26 and a half million veterans' information compromised. And I know someone close to me had this happen to them in this area and it took them 18 months to get it cleared up. They went to co-sign for someone and they said you need a co-signer.

So my question to you—and I do not feel that this is an isolated incident. I mean, it may be an incident that we found out about it, members of Congress and the public. But I do not think it is just isolated. If this has happened, it has happened before.

And what I want to know is, what have you done to ensure the safety of the data since the loss of this data and how can you assure us that this is just a one-time major incident?

Dr. KUSSMAN. As we mentioned earlier, ma'am, the——

Ms. BROWN of Florida. And that is okay. You can tell us over and over again because I am not convinced that you all get it.

Dr. KUSSMAN. The issue that came up was not data that was related to the Veterans Health Administration or health records. We have programs in place that we believe significantly protect our patients from loss of data both from a security and privacy perspective.

We operate under the principles of the Health Information Portability and Accountability Act that puts very stringent requirements in and holds people accountable both from an ethical, moral perspective, but as well as a legal and financial perspective. So we believe we have in place situations that will protect our patients from loss of information and protection or privacy.

Ms. BROWN of Florida. So you are saying that none of the veterans', in the healthcare system, information have been compromised in the past and you can assure us it is not going to be compromised in the future?

Dr. KUSSMAN. No. I think as I mentioned to Mr. Michaud earlier, it is a very large organization with lots of people. Just like the FAA and its gold standard in the airline industry of protecting patients and making flyers and making people assured, but even in spite of that, there are airplane accidents.

Our process and our goal is to put in place processes that would minimize or mitigate as much as conceivable the loss of information. But could I promise you that there would never be or that there has never been a loss of information? No. That would be impossible to do.

Ms. BROWN of Florida. Yes. But with FAA, we put in certain safeguards. And so I guess I am asking you what additional safeguards have you all put in place since this incident occurred?

Ms. BELLES. We talked about this earlier as well. We have done a number of things as a result of the data breach. A couple of things that we have done is we have instituted a Security Awareness week to raise the awareness with our entire workforce about the importance of data security, data protections.

We have got a technical group that is being convened to look at encryption. One of the areas that we recognize is a vulnerability as a result of this is that the data, we do not have guards at the door. We are not stopping people from walking out the door with this because we do not check these people as they walk out the door.

But what we can do is put technical controls in place to protect that data. We can put encryption on laptops and we can require encryption of files so that if that data is on a laptop, that if anyone accesses it, if it is stolen, then the data is protected, that people cannot use it or cannot see it.

Ms. BROWN of Florida. A lot of people work from home. What kind of safeguards do you have there? I am not a technical person, but the amount of information that they can pull down, how does that work?

Ms. BELLES. We do have what is called a virtual private network in place, and everyone who is an approved telework status is able to dial into our networks via that VPN connection. That is an encrypted connection between the individual's laptop and the computer systems.

We also allow on a very limited basis some of our contractors and business partners to access that VPN as well, and they are held to

specific systems based on IP address so that they can only go to that system. The same with myself and everybody around the table. I have a VPN connection. I can only go to those systems that I would access if I were sitting at my desk at work.

Ms. BROWN of Florida. Do you have extra safeguards for those private contractors that you all contract with?

Ms. BELLES. We have business associate agreements that discuss the date use, the protection of that data. We have contracts in place that have the security language in them that requires background investigations at the same level as VA workforce members. We have requirements for them to take security and privacy training just like our workforce members.

Ms. BROWN of Florida. Thank you, Mr. Chairman.

I guess the only other follow-up question I would have was what kind of penalties if someone breached the agreement.

Mr. BROWN of South Carolina. I assume that the person that was involved before, Dr. Kussman, lost his job. Is that kind of the penalty?

Dr. KUSSMAN. I have not been directly involved in that as you probably know. But, yeah, that is my understanding.

But to answer the question that was asked, there is a whole human resource protocol for actions that are inconsistent with our policies and programs all the way from letters of admonition to firing and fines and things. So that process would be used in this instance if somebody violated our procedures and policies as well.

Mr. BROWN of South Carolina. Thank you, Ms. Brown.

Mr. Michaud, you have a question?

Mr. MICHAUD. Just two quick questions, Dr. Kussman. You had mentioned that we can have all the policies we want and it is not a hundred percent. There is one area where when you look at medical transcription when you contract that out, which actually you can help, is by going to, I believe it is called voice recorders versus contracting out. I think that will definitely be more secure.

Are you seriously looking at doing that sort of thing versus contracting out? Yes or no?

Dr. KUSSMAN. Yes.

Mr. MICHAUD. The second one is, the VA and when you look at Department of Defense for our active military, when they deal with medical records, are you working closely with the DoD particularly when you look at medical records?

Dr. KUSSMAN. Yes, sir. The transfer of information for the FHIE and the BHIE, the forward flow and the backward flow of information, the working together of the two agencies, as you know, is unprecedented with the partnering that is going on.

All that information, and it is my understanding, and I will ask Dr. Kolodner to confirm, is that all that information is encrypted.

Dr. KOLODNER. The systems have not only met VA's standards and government standards, but also DoD standards for security, and all the data moving back and forth is encrypted as we move it between the Departments.

Mr. BROWN of South Carolina. Thank you very much, Mr. Michaud.

I remind all members they have five legislative days to submit questions.

And, panel, thank you very much for coming. I hope that we were able to gather some information from you that the VA might be able to use. I know you are working already with them, and look forward to a continued dialogue on this. Dr. Kussman, keep us abreast of what you come up with in order to prevent a breach similar to what we have just experienced.

Dr. KUSSMAN. Yes, sir. Thank you very much for inviting us.

Mr. BROWN of South Carolina. I also might remind members they have five legislative days to submit opening statements.

And with that, the meeting stands adjourned.

APPENDIX

OPENING STATEMENT
HONORABLE HENRY E. BROWN, JR.
CHAIRMAN, SUBCOMMITTEE ON HEALTH
COMMITTEE ON VETERANS' AFFAIRS

Subcommittee on Health Oversight Hearing on Safeguarding Veterans' Medical Information within the Veterans Health Administration (VHA).

June 21, 2006

The Subcommittee will come to order.

We are holding this hearing today to address the vulnerability of VA's electronic medical records system and examine the access and control policies VA employs and the compliance mechanisms VA uses to safeguard sensitive personal veteran health information from internal and external security threats.

The value of VA's electronic medical record system was evident in VA's response to Hurricane Katrina. During Hurricane Katrina, VA doctors and nurses were able to treat without interruption patients transferred from VA facilities in New Orleans to VA hospitals in Houston

because of the system's electronic medical records. All patient records were backed-up, secured, transported to Houston and were back on-line and available almost immediately.

At the same time, however, there are risks with holding such sensitive and personal information electronically and the lack of a solid VA information security program greatly troubles me.

The personal and sensitive data of our nation's veterans must be handled with the utmost of care. The burglary at the home of a Department of Veterans' Affairs employee that included a data file with personal information on millions of veterans is simply unacceptable.

The Department of Veterans' Affairs is working with the FBI to thoroughly investigate this matter and this

Committee will be closely monitoring this situation to help ensure that such an occurrence is not repeated.

We must make sure that there are explicit and clear security and confidentiality policies to protect the health information of our Nation's veterans.

To that end, we are interested, today, in hearing from those at the department, how the MOST sensitive information—individually identifiable health information—is currently being protected.

Additionally, in light of the recent theft I am interested in knowing what the VA anticipates doing to BETTER protect this information in the future and what steps, if any, have already been taken.

Through a series of hearings set up by the Chairman of our full Committee, Chairman Buyer, we have been able to closely examine data integrity and security issues from a

number of different perspectives. But today, we have the opportunity to specifically focus on health-related information.

In addition to having assembled the cast before us from the VA, we have also taken the opportunity to speak with folks from the private sector. I, for one, welcome the opportunity to hear what is currently being considered "state of the art" in the private sector and then benchmarking that standard against VA's current practices. Today, we'll have that opportunity.

I'd like to personally thank all of our witnesses for being here and with that....

I now yield to our ranking Member, Mr. Michaud for an opening statement.

Thank you, Mr. Michaud.

On our First and only Panel, representing the Department of Veterans Affairs, we are honored to have Brig. Gen. Michael J. Kussman. Dr. Kussman was appointed Deputy Under Secretary for Health for the Veterans Health Administration on May 29, 2005. In this capacity, he leads the clinical policy and programs for the nation's largest integrated health care system.

Among his many accomplishments, Dr. Kussman served as the Army Surgeon General's chief consultant in Internal Medicine and governor for the Army Region of the American College of Physicians in 1988.

From March 1993 to August 2005 he commanded Martin Army Community Hospital at Ft. Benning, Ga., and later commanded the Walter Reed Health Care System in Washington, D.C., where he was promoted to brigadier general.

Following his tour at Walter Reed, Dr. Kussman served as commander of the Europe Regional Medical Command and was responsible for Army health care throughout Europe, the Middle East and Africa.

Dr. Kussman is accompanied by: Mr. Craig B. Luigart [loo-gart], VHA Chief Information Officer; Dr. Robert Kolodner, Chief Health Informatics Officer, Ms. Stephania Putt, VHA Privacy Officer; and Ms. Gail Belles, VHA Technical Security Advisor.

I also want to welcome Mr. Robert Seliger [sell-a-gher]. He is the CEO and co-founder of Sentillion [cen-til-E-in], Inc.. Mr. Seliger [sell-a-gher] has led the company in creating security solutions that improve information access and workflows for customers in the healthcare information technology industry.

He is widely recognized as a visionary at the forefront of converging technical, market, and clinical trends in healthcare. Prior to co-founding Sentillion [cen-til-E-in], Mr. Seliger [sell-a-gher] was a senior R&D manager, and chief architect of an international team responsible for the development of Hewlett-Packard Medical Product Group's largest portfolio of clinical information system products.

Presently, he chairs the Healthcare Information and Management Systems Society Steering Committee for Integration and Interoperability. We are very pleased to have him at our hearing today.

Dr. Kussman, you may begin

Thank you both for your participation and attendance today.

With nothing further, the hearing stands adjourned.

Opening Statement of Congressman Michael Michaud
Ranking Member of the House Veterans Affairs Health Subcommittee
June 21, 2006

Chairman Brown, thank you for holding this important oversight hearing.

VA's electronic patient record system remains the technological force behind VA's state of the art care. It can save lives and money. But could the wireless laptops VA providers use to access veterans' lab results and do other medical work also jeopardize the security of that veteran's personal health information?

As we have seen, there may be a dark side to huge electronic databases. The recent data breach exposing the personal data of up to 26.5 million veterans and some spouses, including the names, birth dates and social security numbers of 1.1 million active-duty military personnel, 430,000 National Guard members and 645,000 Reserves, should be a jarring wake up call for all VA offices and the rest of the federal government.

The loss of personal and private information was not due to a breach in security of the Veterans' Health Administration data systems. The data breach had nothing to do with the VA's electronic medical records. But that does not mean we should think that the VHA data systems, including the electronic medical record system, are not vulnerable to internal and external security threats.

Last week, the VA's Inspector General issued a report on VA's procedures for outsourcing medical record transcription. That report showed that VA had weak controls over veterans' medical records. In 2005, a subcontractor in India contacted the IG and threatened to expose thousands of patient records over the Internet if the subcontractor was not paid. This allegation and the IG's audit show that VA was incapable of controlling or detecting where a contractor had medical information transcribed or who had access to it.

VA's procedures for acquiring medical transcription services from contractors failed to address basic security requirements. Of the VA facilities surveyed, 91% did not remove personal identifiers, such as patient

names and social security numbers, before transmitting the data to a contractor for transcription.

I agree with the IG that VA needs to do this work with VA staff, because there is no practical way to ensure that contractors safeguard patients' protected health information. As the IG report says, "The inability to control confidential information in a era of global outsourcing leaves protected health information unprotected and patients subject to identity theft." Given the clear risks with outsourcing, I cannot understand why this Administration's Office of Management and Budget identified the jobs in medical information and records as ones that should be studied for outsourcing. I look forward to hearing from Dr. Kussman about VA's efforts to improve controls on medical transcription.

Other threats to the privacy and security of veterans' medical information remain. Data hackers are a threat to VA's security. A nurse who accidentally leaves on a computer screen while rushing off to help a patient is also a threat to patient privacy and information security. It would be irresponsible for us to believe that the risk to information security has been limited to one VA Central Office data analyst who used his home laptop to work on a report.

Last week, at the full committee hearing, we heard from the VA Inspector General and from the Government Accountability Office. They both testified to report after report warning the Veterans Health Administration of significant concerns about weaknesses in the security of VA's data and information systems. I am concerned that holes and weak spots in the VHA data systems may still exist. I look forward to hearing from Dr. Kussman about what steps VHA has put in place to conduct regular risk assessments and to monitor for unauthorized access to medical information.

Chairman Brown, I commend you for your leadership in holding this hearing so that we can better understand what the Veterans Health Administration has done and will to do to preserve the security and privacy of veterans' medical information. I know that you and I are united in our desire to make sure that Congress, veterans and their families, can have confidence that VA is vigilant in keeping veterans' medical information safe, secure and private. I look forward to working with you on this issue and to hearing from our witnesses.

Statement of Rep. Corrine Brown
Committee on Veterans' Affairs Subcommittee on Health
Safeguarding Medical Information
June 21, 2006

Thank you, Mr. Chairman and Mr. Michaud for holding this hearing.

To say that I am disturbed by the loss of data would be understating the feelings I have. However, the dribs and drabs of information that is coming out from the Department of Veterans' Affairs concern me greatly.

I am glad we are holding these hearings both in this subcommittee and the full

committee, because otherwise we would not know anything.

The administration still seems not to take this breach seriously. The letter sent to veterans does not take any responsibility for its action or lack thereof.

"Out of an abundance of caution, however, VA is taking all possible steps to
protect and inform our veterans." This is directly from the letter. There is a culture, an arrogance that seems to

pervade how the VA is responding to this crisis.

This response is inadequate.

Every time there is a hearing more information is added to what might have been on that computer. At first, names addresses, phone numbers, social security numbers and possibly the disability ratings.

Of veterans.

Then, some widows might have their information included.

Then active duty National Guard and Reserves information was probably on that computer.

So not only do the servicepeople in Iraq and Afghanistan have to worry about getting killed, but their families might be at risk for identity theft while they are overseas.

So forgive me if I do not believe the first words out of the Secretary's mouth that the health information is not compromised.

Statement for the Record of Brig Gen. Michael J. Kussman, M.D.
Principal Deputy Under Secretary of Health
Veterans Health Administration
Department of Veterans Affairs

Before the House Committee on Veterans' Affairs Subcommittee on Health
June 21, 2006
***

Good morning, Chairman Brown, Ranking Member Michaud and Members of the Subcommittee.

Thank you for allowing me the opportunity to provide an overview of the Veterans Health Administration (VHA) data management and security procedures in place to ensure the safety and integrity of veterans' electronic health records, and to safeguard sensitive personal veteran information from internal and external security threats.

Before I proceed with my review of our security and privacy procedures, I want to assure both you and our nation's veterans that the recent data breach did not include any of VHA's electronic health records.

VHA has always viewed data privacy and security as one of its fundamental operational pillars. While safeguards have to be balanced against our ability to provide critical and timely healthcare, VHA is committed to providing our veterans with the best possible healthcare while protecting their privacy and the privacy and security of their medical information.

VHA is responsible for protecting data on all systems that facilitate the delivery of healthcare benefits to our nation's veterans. Similar protections are provided for the databases that contain the veteran health records exchanged between the Department of Defense (DoD) and VA. We protect many important health databases and systems that enable us to provide quality care to our veterans.

VHA systems contain considerable amounts of sensitive data that is used in the delivery of health care benefits to our veterans and their dependents. Sensitive data typically handled in VHA include, but are not limited to, medical/health and benefit data, personnel and employment data, individually identifiable data for veterans and employees, and financial data. VHA also handles various forms of storage media in support of systems operations.

Since VHA is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), VHA complies with the provisions of HIPAA through a comprehensive Privacy Program that provides oversight and guidance throughout VHA to ensure privacy of veterans' information is maintained. While the other VA Administrations and Staff Offices are not covered entities under HIPAA, they do comply with other Federal privacy laws, such as the Privacy Act of 1974.

VHA databases include:

- Veterans Health Information Systems and Technology Architecture (VISTA), the automated environment that gives VA clinicians near-real-time, secure access to the electronic health information available in the Computerized Patient Record System, or CPRS, and VistA Imaging.

  VistA is our core electronic health record system. This widely acclaimed system has saved the lives of thousands of veterans. But it was designed twenty years ago. As such, it is principally "hospital" based, and is deployed in more than 100 locations. This distributed nature does NOT lend itself to simple security compliance. Today, network and telecommunications standards and solutions exist to assist in mitigating these risks while creating greater efficiency and effectiveness. Later in my testimony, I will discuss the solutions we are developing to address these risks.

- My HealtheVet, a Web-based application that provides veterans, their families and clinicians secure access to trusted health information. My HealtheVet links to Federal and VA benefits and resources, the veteran's Personal Health Journal, and online VA prescription refill capability.

- The Federal Health Information Exchange/Bidirectional Health Information Exchange (FHIE/BHIE), a federal healthcare initiative that facilitates the secure, electronic exchange of patient medical information between government health organizations. FHIE/BHIE provides both VHA and DoD physicians access to health data at locations where patients receive care from both systems.

- The Health Data Repository (HDR), a repository of selected clinical data for every veteran who has received care in a VA hospital. Data from the HDR is used to create an historical, longitudinal picture of the veteran's health record, and is available to every clinician within the VA who provides care to a veteran. While the HDR database is not complete, we have populated it with clinical data in the areas of allergies, laboratory and out-patient pharmacy. We are continuing to add additional clinical data to the HDR database.

- The Clinical and Health Data Repository (CHDR) initiative, which seeks to ensure the interoperability of the DoD Clinical Data Repository with VA's HDR. CHDR permits the exchange of clinical data so that DoD Tricare and HealtheVet beneficiaries receive seamless care.

- VHA National Databases - VHA collects healthcare and administrative data in national databases, many of which are located at the VA Austin Automation Center. These data provide the foundation for understanding and improving the quality of VA healthcare, allocating resources across the organization, and managing operations.

All VHA systems in the VA's Federal Information Security Management Act (FISMA) inventory were certified and accredited and received authority to operate in 2005. A program to continuously monitor the effectiveness of the security controls in these systems, and to re-certify systems in accordance with VA policy is in place. All transmissions of data to and from My HealtheVet, CHDR, and FHIE/BHIE are encrypted to current Federal standards. VHA complies with all VA policies and develops additional health care-specific privacy and security policy and guidance.

The Rules of Behavior advise users that misuse of government systems, mishandling of veteran data, or unauthorized disclosure of sensitive information could result in disciplinary action up to and including termination of employment.

To protect VHA systems and data from unauthorized access, a number of security controls have been implemented. Let me address specific security procedures in place to control access, ensure continuity of operations and protect data.

Access
VHA carefully manages access to information system resources through a combination of technical and administrative controls. User access and verify codes are required to gain access to information system resources. Sensitive data can be accessed only by those with a legitimate and demonstrated need. Even then, users can access only the information needed to do their jobs. Granting access to users requires management approval, which is routed through the appropriate Information Security Officer (ISO). User access privileges are reviewed to ensure legitimate and continued need for access.

Storage
All VHA systems are backed up at least weekly in accordance with VA and VHA policy, or more often depending on the nature of the data. Several generations of backups are retained, and the restore process is tested regularly to ensure that data can be restored to its original state. The backups are stored at off-site locations, and appropriate physical and environmental controls are in place to protect the backups. Media used to record and store sensitive software or data are secured when not in use, or they are sanitized or destroyed in accordance with VA policy. Contingency plans are in place, and plans are "tested" as a consequence of system outages. VHA is focusing efforts on improving compliance with the requirement to document these tests.

Allow me to provide an example of how our backup procedures were employed after the New Orleans VA Medical Center was shut down and evacuated following Hurricane Katrina. Because telecommunications lines were down, back-up tapes of our electronic health records from the New Orleans facility were flown to Houston Veterans Affairs Medical Center and loaded onto systems. The VistA systems were back up and running in less than two days with no loss of data. This was a well-documented test that demonstrated effective backup procedures.

Security of Data in Transit
Data transmitted among VA systems are monitored 7 days a week, 24 hours a day, 365 days of the year, primarily for the purposes of system performance and availability. Data traffic moving inside the VA network is not encrypted; when VA data are sent outside the firewall, a Virtual

Private Network, or VPN, is used. In addition, intrusion detection systems have been deployed; the VA Security Operations Center monitors these systems for the presence of unwanted intruders or attacks on VA networks. Data are encrypted in accordance with VA and VHA Directives 6210.

VPN Access

The VPN is a centralized service that provides secure, remote access to VA's employees and contractors. The OneVA-VPN grants remote access for individuals such as doctors, nurses and other clinicians who need access to data or information to perform their functions (e.g., patient care). Typically, these employees are logging into the system at home or during travel. Some off-site contractors also use VPN to access information essential to the performance of their tasks. Users must read, comprehend, sign, and abide by the Rules of Behavior form that requires signature before access is granted. Contractor access through the VPN is restricted to the locations appropriate to each contractor through Internet Protocol (IP) addresses. User access is authorized and controlled in accordance with VA remote access guidelines, and requires supervisory approval and confirmation with the supervisor by the appropriate ISO.

Contractor access must be approved by both the Contracting Officer Technical Representative and the ISO. Contractor accounts are established with VHA's business partners who support remote maintenance for medical devices, provide medical transcription services or perform diagnostic radiology services.

A recent OIG audit identified the need to mitigate risk associated with its transcription contract. VHA is taking several steps to alleviate this risk. VHA has inserted language into the VHA business associate agreement (BAA) template that forbids the transfer of veterans' protected health information outside the jurisdiction of the United States. We are also developing recommendations for a uniform approach to transcription and speech recognition to be used throughout VHA. VA is now gathering information on current contracts and experience with speech recognition technologies. The VHA Prosthetics and Clinical Logistics Office (P&CLO) will coordinate an interdisciplinary workgroup to review this data. The group also will prepare a report to include recommendations on the feasibility of a national contract for transcription services, a national roll-out of speech recognition technologies, or a combination of the two in VHA, along with cost information. The report and recommendations are due by October 1, 2006, with implementation to follow.

Telework

The Department issues VPN user accounts and equipment for use by teleworkers at management's discretion. VPN user accounts, as described above, provide secure, remote access to VA systems and data. Telework agreements are signed by the employee and supervisor and describe the responsibilities and procedures for telework.

Telework is not open to everyone, nor to every type of work. The VA policy requires managers to determine whether it is appropriate for an employee to telework and whether it is appropriate for the work to be performed via a telework arrangement. If an authorized teleworker will be accessing sensitive documents, that person has received management approval and must agree to

protect Government/VA records from unauthorized disclosure or damage in accordance with the requirements of the Privacy Act and all applicable Federal laws and regulations, VA Directive and Handbook 6210, and other applicable VA policies.

Security of Equipment Brought in to VA
All employees and contractors must follow VA policy when they bring in any non-VA computer equipment that is connected to the VA network. Before this equipment may be connected to the network, it must be scanned to ensure that it is in compliance with the latest operating system patches and virus updates.

Training Requirements
VHA follows VA policy regarding security and privacy training requirements. Employees and contractors must undergo initial security orientation before they can access VA systems. In addition, employees and contractors are mandated to complete annual security awareness training, which must be documented. Users must sign Rules of Behavior documents. Annual privacy training also is mandated. Privacy training must be completed within 30 days of an employee's or contractor's start date and before access to sensitive data can be granted. Both privacy and security training modules continue to be developed to target specific job responsibilities.

Enforcement of Procedures
Given the complexity of information technology systems, vulnerabilities will be discovered periodically. Therefore, on an ongoing basis, VHA performs internal risk assessments to identify our weaknesses. When our assessments identify vulnerabilities, we remediate the problems in the appropriate manner, including issuing new policy and making technical changes to the system.

Security and privacy policy compliance is monitored internally by annual FISMA security surveys, site security program reviews conducted by the VA Office of Cyber and Information Security and during VHA System-wide Ongoing Assessment and Review Strategy (SOARS) site visits. SOARS visits are designed to review facility compliance with internal and external oversight groups {e.g., Office of Inspector General Combined Assessment Program (CAP) Reviews, Joint Commission on Accreditation of Healthcare Organizations (JCAHO)} standards prior to visits from these oversight groups. On an ongoing basis, the VHA Privacy Office conducts site assessments to ensure compliance with privacy policies and laws, and to provide direction on how to remediate problems. Additionally, VA's Office of Cyber and Information Security is currently letting a contract for independent validation and verification of VA's certification and accreditation documentation, testing, and approval-to-operate processes to ensure that VA certification and accreditation procedures comply with FISMA requirements.

VHA also has health-specific privacy programs enforced by Privacy Officers at each facility. Information security responsibilities are delineated in senior executives' performance plans. The effectiveness of the required security controls/policies are tested through the certification and accreditation process. Security and privacy violations are reported to a central entity, appropriately researched and resolved. Privacy violations are reported by the Privacy Officers to

the Privacy Violation Tracking System, and security incidents are reported by the ISO to the VA Security Operations Center.

There are also external mechanisms promoting VHA compliance. Compliance with the Health Insurance Portability and Accountability Act (HIPAA), including the Privacy and Security Rules, is determined by the Department of Health and Human Services through its conduct of investigations in response to complaints or compliance reviews as appropriate. The Department of Justice monitors VHA Freedom of Information (FOIA) and Privacy Act compliance. The OIG monitors our compliance with all privacy and security requirements through CAP Reviews. Also, agencies such as JCAHO actively assess VA compliance with privacy and security requirements. Reviews of JCAHO findings in information management indicate that VA is doing well in this area.

Security and Privacy of DoD/VA Clinical Data Sharing
Using a specific database cited near the beginning of my testimony as an example, please allow me to present the following overview of the current state of security and privacy of the DoD/VA electronic health data sharing program.

The Department of Veterans Affairs is the lead agent for FHIE/BHIE, the award-winning DoD/VA program that enables the two agencies to share the patient records of U.S. service members and veterans. Not only is FHIE/BHIE in full compliance with VA, DoD and Federal government information security policies and privacy rules, it also has received positive assessments from independent reviewers and high scores on National Institute of Standards and Technology criteria. In December 2005, the system underwent recertification, and received renewal of its authority to operate decision.

In Full Compliance: FHIE/BHIE is in full compliance with VA cyber-security policies and DoD Information Assurance polices, as well as Federal privacy policies such as the Privacy Act and HIPAA.

Built to Highest Standards: DoD and VA have agreed that the FHIE/BHIE joint infrastructure must meet or exceed DoD's Information Assurance policies, which are more complex than VA's policies. During the design-and-build phase, VA and DoD used standards published by the National Security Agency (NSA) to "harden" the security of this interagency system. In 2002, FHIE was the first VHA system to be granted an authority to operate by meeting the VA FISMA requirements.

Highest Level of Protection Provided to Exchange of Data: To ensure the highest level of protection for the DoD and VA clinical data as it is sent across the Internet, the information is double-encrypted using DoD-approved software, effectively securing the transmission of all sensitive data from unauthorized access. The data also traverses both Departments' firewalls via a hardware VPN.

FHIE/BHIE Earns High Marks: During the project's required triennial review in the first quarter of Fiscal Year 2006, independent reviewers, who also consult with the NSA, provided positive comments on the FHIE/BHIE project's joint infrastructure and gave it

high scores on NIST criteria. As stated previously, this resulted in a renewal of the authority to operate in December 2005. The interagency review was accepted by DoD Information Assurance managers as well. It is also noteworthy to add that FHIE/BHIE was one of five winners of the prestigious Excellence.Gov award from the American Council for Technology for demonstrating best practices in information sharing for federally led IT program implementations.

Solid Governance Structure: VA is the lead agent for FHIE/BHIE. To manage this project, VA and DoD have appointed a single manager who sustains FHIE/BHIE operations, maintains project artifacts and documentation, and ensures internal controls for handling the DoD monies transferred to VA to support this joint program. In addition, DoD provides a full-time deputy project manager to the project. The manager and deputy are ultimately accountable to both the DoD Military Health System and VHA Chief Information Officers.

Strengthening Security

I want to assure you that security and privacy of veteran information is of paramount concern. In addition, our electronic health records offer protections that are not possible with paper records.

VA and VHA are committed to continuing to strengthen our security and privacy controls. To this end, VA is investigating the use of encryption solutions appropriate for our information systems and data protection needs. VHA is also re-engineering current applications that will broaden auditing capabilities, and implementing role-based access to limit access based on defined roles.

The next generation of VistA, which is being developed now, will have enhanced security controls built into the system. For example, role-based access control permissions will be much more granular than the access controls in VistA today, enabling tighter management of user permissions across all applications as well as the ability to set system operations (e.g., create, read, update, delete, execute) for data and software applications. These enhanced processes will be employed to address need to know, least privilege, and separation of duty principles. Many other technical and procedural security controls are also being identified in VHA's security requirements repository for implementation across the system development life cycle for the next generation of VistA.

In addition, VHA has identified a number of specific actions for strengthening data security procedures that are in the planning stages or have been identified as a result of the data security breach. These are separated into two categories, as follows:

Planned actions:

- Provide and mandate centrally deployed security solutions. VHA implements security solutions identified by the Department to improve security protections in our health care environment. The Department should mandate the approved solutions to ensure consistency and compatibility across the Administrations and Staff Offices.

- Implement a Department-wide encryption solution that encrypts data that is sent across VA networks. A workgroup that includes Department-wide representation has been established to identify solutions that meet business needs, and are transparent to the end user so that encryption capabilities are provided as a component of VA's network and telecommunications infrastructure.
- Increase monitoring and ongoing compliance reviews of security and privacy programs. VHA has been conducting limited compliance reviews via SOARS and HIPAA privacy assessments; however, results of OIG and GAO audits make it necessary to increase monitoring and compliance activities within VHA to ensure that facilities and program offices are in compliance with VA and VHA security and privacy policies and incorporate the policies and procedures into daily operations.
- Increase the use of secure, web-based solutions for e-mail, scheduling and other administrative needs. VHA has been given approval to move from pilot to implementation of Outlook Web Access (OWA) across VA facilities to provide access to VA administrative resources rather than require secure connections for these activities. This will enable VA to reduce the number of VPN users, reserving the VPN user accounts to those individuals who require the added security controls.

Additional measures to strengthen data security:

- Require that portable media and laptops have the capability to encrypt all sensitive data, and that appropriate guidance, tools and training are provided to the users to implement these solutions effectively.
- Update VA and VHA security policies to address changes in technologies/current IT environments. This is an ongoing activity that can fit into either category; however, there has been an increased focus on the review and update of all policies to ensure they are comprehensive, and are enforceable in our current IT environment.

To emphasize the importance of security, VA is planning a Department-wide Security Awareness Week, which will be held June 26-30, 2006, and annually thereafter. VHA has been identified as the lead VA Administration to coordinate the Security Awareness Week. During the week, briefings will be provided daily to members of the VA workforce to address the proper and secure use of equipment at home, reminders of the impact of data security failures, proper handling and disposal of sensitive data in electronic and paper forms, and the implications to individuals in regard to data breaches (e.g., identity theft). In addition, to help veterans, VA will set up information booths across VA so that veterans can get information on identity theft and fact sheets on data protection. Patient advocates will be available to answer questions related to the data security incident and provide guidance for monitoring financial statements and transactions to detect any misuse. Members of the VA workforce will sign a Statement of Commitment and re-certify their understanding of the Rules of Behavior for access to VA systems and data.

Closing

In closing, VHA already has strong security procedures in place, yet these procedures can be strengthened further. We can do this by enhancing privacy and security guidance, through strong directives with enforceable actions, by conducting annual or as-required privacy and security-

awareness training led by senior VHA leadership, and by emphasizing privacy and security education.

We are committed to providing the best possible care to our nation's veterans. We are also fully committed to ensuring that the VHA workforce is vigilant in protecting the privacy and security of veterans' health records, whether electronic or paper. We also employ and will continue to enhance tools that help us to safeguard sensitive information from internal and external security threats. For our veterans, for the men and women who have fought so bravely for our country, anything less is unacceptable.

Thank you for your attention, and I am ready to answer your questions.

Testimony of
Robert Seliger
Chief Executive Officer
Sentillion, Inc.

For

The U.S. House of Representatives
Committee on Veterans Affairs
Subcommittee on Health

June 21, 2006

Chairman Brown, Mr. Michaud, distinguished members of the Committee, thank you for the opportunity to testify before you today on a subject of critical importance for our nation's veterans, but also to every citizen—how to safeguard sensitive personal health and related information from external and internal security threats. My name is Robert Seliger and I am co-Founder and CEO of Sentillion. Sentillion is the industry leading provider of Identity and Access Management solutions to hospitals and healthcare systems. Everyday, Sentillion helps hundreds of institutions and hundreds of thousands of physicians, nurses, and other caregivers at those institutions employ effective security and privacy practices while also assisting the care delivery process. We are exceedingly proud to say that among these institutions are all 163 medical centers of the Department of Veterans Affairs.

I have twenty six years of experience in the field of healthcare information technology including eighteen years at the former Hewlett Packard Medical Products Group where I served as a senior R&D manager and distinguished scientist and eight years at Sentillion, a company founded to serve the healthcare industry. I have served on numerous healthcare standards committees and have chaired a variety of healthcare industry initiatives. Recent activities include serving as the chair for the Healthcare Information Management and Systems Society (HIMSS) steering committee for Integration and Interoperability, and serving as an advisor on standards uptake for the Pan-Canadian Electronic Health Record Standards Steering Committee. My degrees are in electrical engineering from Cornell University and Computer Science from MIT.

Over the past several weeks, this Committee has spent many hours examining why personal information of Veterans was lost and what can be done to effectively safeguard the privacy and security of this data in the future. You have focused a great deal of attention on what management policies and technical solutions need to be implemented at the enterprise-level to prevent another breach. It is a hugely complex challenge as you have found, but your oversight role and your responsibility to our nation's veterans demands nothing less.

Today I want to focus on one aspect of that complex challenge that is particularly critical in the clinical setting. That is, how we can we safeguard patient data without also impeding the clinical work flow?

The terms security and privacy are often used in conjunction so as to imply that they mean the same thing. Actually, they do not. Security means that people who do not have the proper permissions are not allowed to see information, or access systems, even if they try to do so. Privacy means that people who do have access do not intentionally or even inadvertently share sensitive information with others. Breaking into a hospital's computerized medication order entry system in order to maliciously change the dose of a medication with the intent to do harm is an example of a security breach. Talking by name with a medical colleague about a patient's diagnosis in an elevator occupied by other random people who are in earshot is an example of violating the patient's privacy. Protecting patient security and privacy are key concerns for healthcare organizations, but different measures are required.

One of the key reasons that different measures are required is the fact that in healthcare, the foremost mission of caregivers is to care for patients. By definition, practicing safe and effective medicine will always take precedence over concerns for security and privacy. Our nation's nurses and physicians are among the smartest, most highly trained people in the world. This fact, coupled with their deep sense of mission, will compel them to avoid, work around, and challenge policies that impede the care delivery process. This is because the care delivery process, by its very nature, requires immediate information access and the constant sharing of information with others.

As a simple example, the seemingly trivial task of logging off of a computer after a physician or nurse is finished reviewing a patient's record is almost never done in the hospital. Logging off takes too long to do, is often forgotten when more pressing activities occupy the caregiver's attention, and is often viewed as discourteous because it will require that the next caregiver who wants to use the computer in order to access patient information would need to take the time to log on. A caregiver in a busy hospital might need to log on and off fifty to one hundred times a day. At a minute or two for each log on and log off, you can quickly see how this seemingly trivial best practice is avoided because it interferes with the pace of providing care. And so our nation's physicians and nurses practice good healthcare but leave millions of personal computers across the country open to access or even simple perusal by any passerby – from other healthcare workers who have no valid reason to view the information, to other patients to people visiting patients, to anyone else who might be in the hospital.

My younger brother fell ill several years ago and wound up in the intensive care unit of a Massachusetts hospital. Fortunately he is now fine. I arrived soon after he was admitted. There was not much to do but worry and wait while my brother lay in front of me, intubated and unconscious. That's when I noticed the elegant flat panel display next to his bed. What then caught my eye was that on the display was an application that I spent many years of my life developing when I worked for Hewlett Packard. The application was unlocked and the data on the display could be easily seen by anyone, including me, my brother's wife, and his boss who came to visit later that day. Even though I was curious about the application and wondered if I could remember how to use it, I did not look at the display, because that would have been an invasion of my brother's privacy.

More recently, while visiting one of our customer hospitals with a colleague, we got lost in a labyrinth of corridors and asked a nurse who was walking towards us for directions. She pointed us to a hallway that led through a women's clinic. Outside of every patient's room was a computer on a mobile cart. No one was using these computers, but they were unlocked and each display presented personal health information about one of the patients. My colleague and I averted our eyes and simply found our way out of the building. This is another example of disrespect for patient privacy.

In both of these cases, as best I could tell there were no hackers or criminals in sight. My guess is that the networks upon which these computers were connected were also reasonably secure and protected from unwanted external access. Nevertheless, in two

state of the art healthcare facilities, during normal working hours, in broad daylight, many doors (so to speak) to sensitive patient information were left wide open.

I would like to assert that the real security and privacy challenge that the healthcare industry faces are not attacks from outside, but rather transgressions from within. The question is, "How do we as a nation change this situation without compromising the care delivery process?" How do we improve the security and privacy of patient information without impeding access to the caregivers who need immediate access to the information to care for patients?

The answer is that security and privacy practices that we ask our caregivers to follow must fit with their workflows. Better yet, these practices should enhance the workflows. Let me give a example. What if we could reduce the time it took for a caregiver to log on or log off from minutes to just a few seconds? Data that we have from a study we conducted shows that under such circumstances, nurses in one hospital who only logged off fifty percent of the time were now doing so one hundred percent of the time. And physicians, who were not logging off at all, were now doing so eighty-six percent of the time. I have attached as an Appendix a more detailed description of this issue.

This change in behavior was not due to a new policy or the threat of punitive measures. Rather, we simply made it easier for caregivers to be good security and privacy citizens. By the way, they were also more likely to access the information they needed to make timely and informed decisions from a computer than by looking at paper records, asking a colleague, re-performing expensive tests, or making decisions without information that is available but not used because electronic access is too slow or cumbersome. In other words, security and privacy solutions that are thoughtful and that support the caregiver's workflow can also result in safer, more effective, and less costly healthcare.

I make bold claims and you might be wondering if what I am saying is too good to be true. The basis for these claims is not a specific magic technology or product, but rather the assertion that in healthcare, people want to do the right thing. This is about making sure that things we do to keep the bad guys out do not effectively prevent letting the good guys in. This is about making sure that we engineer healthcare information technology solutions from a systems perspective and not attempt to force upon healthcare organizations mechanisms that make sense for office or other types of business environments, but which do not make sense for healthcare.

People often ask me why I have committed my career to the healthcare industry. I am a businessman, and certainly part of my answer is that it is how I make my living. However, I do have an idealistic streak, and part of my motivation is that I also want to make a difference. One of the fascinating things about working in healthcare is that virtually everyone I meet has the same personal commitment. This is particularly noticeable at the VA, where I have had the privilege to work with physicians, nurses, and IT staff for many years. I realize that the VA has had its challenges, but I have never once thought that these challenges were due to a lack of commitment or caring.

Delivering effective healthcare is an intense and complicated process. It is also a truly mission critical process. Our industry must find the right balance between applying security and privacy measures that are known to work and applying measures that could be detrimental to patient care. We can assert, for example, that every caregiver must have a password for each application that they use, but what in fact are we asking of our caregivers if they need to remember ten different passwords and enter each one in dozens of times a day? To truly safeguard patient security and privacy requires a broad set of measures. These measures include not only good network security and the appropriate encryption of data, but also involves tools and mechanisms that enable good people, well meaning caregivers, to do their jobs without compromising patient health, patient security, or patient privacy.

Mr. Chairman, this concludes my remarks. Thank you for the privilege of speaking before you today. I am happy to answer any questions the Committee may have.

*****

Appendix: Additional Testimony

Barriers to Effective Security and Privacy Practices in Hospitals

The following steps illustrate what is required today for a typical physician to actually practice proper security and privacy within the four walls of a hospital. In this scenario the physician is attempting to review a patient's test result from a computer located in an intensive care unit:

Step	Description	Cumulative Time (estimated)
1	Log onto the computer by entering network username and password.	00:04
2	Wait for computer logon to be completed.	00:34
3	Launch a results reporting application to review patient's test results.	00:35
4	Wait for results reporting application to present its logon screen.	00:40
5	Look up username and password on index card carried in shirt pocket. (Note: this is not the same username or password as that for logging onto the network.)	00:45
6	Enter username and password for the results reporting application.	00:49
7	Wait for the logon to the results reporting application to be completed.	00:55
8	Using the results reporting application, select the patient of interest from the list of available patients.	00:59
9	Select the data of interest (e.g., the latest lab test results) and wait for the data to be displayed.	01:03
10	Based upon the test results, decide which medication dose to adjust.	01:13
11	Launch the medication order entry application.	01:14
12	Wait for order entry application to present its logon screen.	01:19
13	Look up the necessary username and password on index card carried in shirt pocket. (Note: this is not the same username or password as used for logging onto the network or for logging onto the results reporting application, but is the same index card.)	01:24
14	Enter username and password for the order entry application.	01:28
15	Wait for the logon to the order entry application to be completed.	01:32
16	Using the order entry application, select the patient of interest from the list of available patients.	01:36
17	Select the data of interest (e.g., the current set of	01:40

	medications) and wait for the data to be displayed.	
18	Select the medication of interest and adjust the dose.	01:50
19	Log off of the order entry application.	01:53
20	Log off of the results reporting application.	01:56
21	Log off of the computer (ALT-CONTROL-DELETE, then select Log Off).	02:00

In this example, 20 seconds of productive work required 1 minute 40 seconds of additional tasks pertaining to signing on, selecting the patient of interest, and signing off. A typical physician might need to access a computer thirty to fifty times a day, meaning that between a half hour and an hour is spent on the minutiae of logging in, selecting the patient, and logging out. In addition, while the physician is trying to focus on clinical decisions for the care of patients, she has to keep focusing on remembering which usernames and passwords are used for which applications.

In the absence of a more productive solution, the vast majority of physicians will not perform these tasks. The same situation generally plays out as illustrated in the following scenario:

Step	Description	Cumulative Time (estimated)
1	Walk up to an unlocked computer.	00:00
2	Using the results reporting application, which is already running under another person's log on, select the patient of interest from the list of available patients.	00:04
3	Select the data of interest (e.g., the latest lab test results) and wait for the data to be displayed.	00:08
4	Based upon the test results, decide which medication dose to adjust.	00:18
5	Handwrite the new medication order on a paper form and hand it to a nurse.	00:28
6	Leave. The computer and the results reporting application (which is still displaying the patient's data) is now visible and available for anyone to use.	00:28

The same 20 seconds of productive work is encumbered by only 8 seconds of additional tasks. This overhead represents between four minutes and six minutes of overhead each day and require few interruptions to the physician's thought process about patient care. Clearly the cost of complying with security and privacy best practices is too great for most physicians to tolerate.

Possible Solutions

The technology now exists to enable caregivers to be productive while also performing proper security and privacy practices:

- Single Sign On enables a caregiver to enter their username and password (or other credential, such as a fingerprint or smart card) only once per logon, and as they open applications they are automatically signed on. This obviates the need to remember usernames and passwords, to have to carry them on "cheat sheets", or to even type them in.

- Single Patient Selection enables caregivers to select a patient of interest once, in any application, and in so doing automatically tune all of the other applications in use to the selected patient's records. If an application is newly launched then it automatically tunes to the selected patient's records.

- Single Sign Off enables caregivers to sign off of all of the applications that they have logged on to, and to sign off of the computer, all in one easy button click.

- Fast User Switching enables caregivers to share the same computers so that the time it takes to sign on to the computer and the underlying applications is dramatically reduced. Some techniques employ the capability to keep applications running "hot" and ready to go as soon as a valid user logs on to the computer. The applications are not visible until the computer is unlocked by a valid user.

Solutions that support these behaviors are in use throughout the United States. The VA presently employs Single Patient Selection, has the capability to deploy some elements of Single Sign On, and is evaluating the addition of Fast User Switching and Single Sign Off.

Questions For the Record
The Honorable Michael H. Michaud
Ranking Democratic Member
Subcommittee on Health
House Committee on Veterans' Affairs

June 21, 2006

Hearing on Safeguarding Veterans' Medical Information with the Veterans Health Administration (VHA)

Question 1: Last week the VA Inspector General issued a report on VA's outsourcing of medical record transcription. I agree with the Inspector General that outsourcing this function creates a risk to veterans' privacy and identity that VA cannot control. This weakness in VA's medical record system was spotlighted last year when an offshore subcontractor in India threatened to expose personal and private information of about 30,000 VA patients over the Internet.

In your testimony you stated that VA contracts now forbid the transfer of veterans' protected health information outside the jurisdiction of the United States

a) Will you conduct audits to ensure contractor compliance with the provision prohibiting the transfer of veterans' protected health information outside the jurisdiction of the United States?

Response: Yes, the contracting officer's technical representative (COTR) is required to meet routinely with the contractor. In addition, the Veterans Health Administration (VHA) is requesting that reviews be added to the system-wide ongoing assessment and review strategy (SOARS) and the Office of Inspector General's (OIG) combined assessment program (CAP) audits that are accomplished every 3 years. VHA has requested that OIG and the SOARs program office include a review of the contract file demonstrating that the COTR and contracting officer have documented their meetings with the vendor showing all data that indicates the work accomplished by the vendor and if any of the work is subcontracted.

b) Please describe in detail how VA will monitor contractor compliance with that specific contract provision.

Response: On June 20, 2006, a memorandum from the Deputy Undersecretary for Health for Operations and Management was sent to all VHA chief logistics officers. The first requirement in the memorandum calls for contracts to specify limitations on the access to VHA data at contractor facilities and ensure the following within 30 days of the date of the memorandum: (1) contracts contain security requirements for transcribers working at home; (2) contract staff working at VHA facilities undergo background investigations and sign "Rules of Behavior" defining acceptable practices concerning the use of the VHA information systems; (3) contracts specify when and how

contractors are to purge VHA data from contractors' computer systems; and (4) require contractors to transcribe in the United States or its territories. The second recommendation is that all facilities complete the required business associate agreements with their transcription contractors. With these two recommendations in place at all sites that contract for transcription services, a process for follow-up and continued assurance of compliance will be instituted such as routine meetings between the COTR, contracting officer and vendor, covering work accomplished to date, listing of all employees and subcontractors and their employees validating and certifying that no work is accomplished outside of the United States.

c) Can you give us a total and complete assurance that absolutely no VA contractor will use an overseas subcontractor to transcribe veterans' medical information?

Response: Subsequent to this hearing, VHA learned that a 2003 contract with a previous business associate agreement (BAA) was in place between VA and a company named InfoPro. The previous BAA template did not, on its face, preclude offshore contracting or subcontracting. InfoPro subcontracted to Global Data Source, LLC, for transcription services. These services were being conducted offshore. As of August 11, 2006, these contracts were re-negotiated to reflect new regulations.

A template for a BAA, required by regulation under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, was produced in October 2005 and distributed to VHA HIPAA representatives. The template includes a clause specifically addressing the safeguard of Protected Health Information (PHI) with regard to offshore transcription services. Processes are being put in place to assure that in all future contracts, the appropriate BAA will be used and no VA contractor will be allowed to use an overseas subcontractor to transcribe veterans' medical information. These security requirements, coupled with our continued vigilance, will help ensure compliance in safeguarding the privacy of our veterans' health information.

Question 2: In your testimony you stated that audit trails are monitored continuously and reviewed every month by VA IT security officials. Please give specific examples of what actions VA has taken in response to these audit trails.

Response: Audits of user activities on Veterans health information systems and technology architecture (VistA) systems are available for review by information security officers (ISOs) at any time. In addition to providing audit report capabilities, VistA also generates a bulletin to the ISO for all user accesses to records flagged as "sensitive." The sensitive flag is used to mark employee records, and records of public figures to provide an extra layer of access protection. The bulletins are sent to the ISO, who validates the access with the user's supervisor. If it is determined that the user's access to the records was not authorized in the performance of official duties, appropriate disciplinary action is taken.

As a result of the ongoing review of audit bulletins and reports, VHA identified an issue with the employees' understanding of "authorized access" to records. Additional

training and information was provided to employees on their responsibilities regarding the appropriate and authorized use of VA records and systems to address this issue.

Question 3: In your testimony you stated that contractor access is tightly controlled. Are you highly confident that VA terminates access codes and passwords for contractors in a timely manner?

Response: While VHA's testimony focused on contractor access that is strictly controlled through the virtual private network (VPN) via Internet Protocol (IP) addresses, the termination of access of employees, volunteers, and contractors has been identified as an area that requires VHA attention both in OIG CAP reviews and in SOARS assessments. Facility directors have been encouraged to bring together the appropriate entities in the facilities to meet and resolve the access termination issues. In addition, VHA is working with the Department to implement an automated solution to terminate VPN user accounts based on inactivity.

Question 4: In your testimony you stated that VA conducts an annual System-wide Ongoing Assessment and Review Strategy or SOARS. What did SOARS identify to be the most significant privacy and security threats to VA's medical health data systems, both internal and external? Please describe the changes in technology, policies or practices that VHA has implemented in response to these and other assessments.

Response: SOARS has identified two significant areas that require immediate attention across VHA facilities; this information was communicated to the facility directors on a June 23, 2006 national conference call. The first is promptly terminating the access of employees, volunteers, and contractors when they leave their assignments. This should occur either before or on the day they leave to ensure that there is not a possibility of continued access to VA databases. SOARS teams generally find facilities in at least partial compliance for employees departing their facility through the normal clearance process, but often find considerable delays for others. Directors were encouraged to bring together the appropriate entities in the facilities to meet and resolve the access termination issues.

The second common area of findings has to do with identifying and inventorying all computer equipment on at least an annual basis. Because many or most laptops and desktop computers fall under the $5,000 threshold required for inclusion on Equipment Inventory Lists, these types of equipment are not always well monitored. Even though they are considered "sensitive equipment," many facilities don't always identify them as such, and don't complete inventories or continually update locations where they are assigned as those locations change. VHA considers this a risk area and has directed facilities to properly account for and monitor this equipment closely.

The SOARS teams will be heightening their review of these areas as well as other areas identified in OIG CAP reports effective immediately.

Question 5: What are the most significant internal threats to unauthorized review of veterans' medical information? Please describe in detail your plans to address these threats.

Response: The most significant internal threat of unauthorized access of medical information for any health care provider is its employees. VHA is no exception. However, VHA does everything possible to ensure that employees are educated and trained on their responsibilities for appropriately accessing and protecting veteran medical information and are aware of the penalties and disciplinary actions for unauthorized access to veteran medical information. Furthermore, VHA audits employees' access to medical information for those individuals flagged sensitive in the system, and users are prohibited from accessing their own electronic health records to ensure that proper release of information procedures are followed.

Through the HealtheVet-VistA re-engineering effort, VHA is implementing role-based access control (RBAC) to address management of user permissions across all applications. RBAC grants user access to information based on "need to know," "least privilege," and "separation of duty" principles. Further granularity of user permissions is provided within RBAC, to enable setting of system operations (e.g., create, read, update, delete, execute) for data and software applications.

VHA led the effort in defining the standard access control permissions that can be used to make access control decisions within Department of Veterans Affairs (VA), between VA/Department of Defense (DoD) and other business partners, and among members of the international healthcare community. In May 2004, these definitions were adopted by Health Level Seven (HL7), Inc., the non-profit organization that is accredited by the American National Standards Institute (ANSI), for creating the standard healthcare permissions vocabulary worldwide, and were successfully balloted in January 2006. The Draft Standard for Trial User for worldwide role-based access control permission definitions represents a major milestone for VHA-led standardization efforts, as well as for collaborating partners including DoD, and Kaiser Permanente.

Question 6: Does VA conduct joint IT security and threat assessments with DoD to strengthen and improve the safe and secure exchange of medical information between the two agencies?

Response: VA co-leads with DoD the Federal Health Information Exchange (FHIE) and the Bi-directional Health Information Exchange (BHIE) initiatives, the award-winning DoD/VA programs that enables the two agencies to share the patient records of U.S. service members and veterans. FHIE and BHIE are in full compliance with VA, DoD and Federal government information security policies and privacy rules, and have received positive assessments from independent reviewers and high scores on National Institute of Standards and Technology criteria. In December 2005, the system underwent recertification, and received renewal of its authority to operate decision. FHIE and BHIE are in full compliance with VA cyber-security policies and DoD

information assurance polices, as well as Federal privacy policies such as the Privacy Act and HIPAA.

DoD and VA have agreed that the FHIE and BHIE joint infrastructure must meet or exceed DoD's information assurance policies. During the design-and-build phase, VA and DoD used standards published by the National Security Agency (NSA) to "harden" the security of this interagency system. In 2002, FHIE was the first VHA system to be granted an authority to operate by meeting the VA's Federal Information Security Management Act (FISMA) requirements. To ensure the highest level of protection for the DoD and VA clinical data as it is sent across the Internet, the information is double-encrypted using DoD-approved software, effectively securing the transmission of all sensitive data from unauthorized access. The data also traverses both Departments' firewalls via a hardware virtual private network.

Question 7: I remain concerned that VA's research program, which I support, is VHA's Achille's heel when it comes to protecting veteran's health care and personal information. VA researchers can have access to databases with Social Security numbers identifying veterans. I understand that researchers must go through an approval process to get an access code to this database. Please describe in detail the steps VHA plans to take to ensure that after a researcher has access to data it is not downloaded, put on a laptop or external hard drive or otherwise put at risk of being lost or stolen. Please describe in detail VHA's plan to monitor, audit and enforce compliance with the policies and practices VHA proposes will prohibit breaches in security due to researchers' use of data.

Response: Policy. VHA Office of Research and Development (ORD) researchers must currently comply with all relevant VA and VHA policies related to storage and security of data and information (see Attachments A and B).

VHA ORD, in collaboration with the VHA Office of Research Oversight (ORO), VA Office of General Counsel (OGC), and other appropriate offices, is developing a handbook on use of databases for research purposes to include existing, updated and expanded policy. Processing has been expedited. Issues to be addressed include security of servers used to store data; parameters for use of desktop computers, laptop computers, "thumb" drives, memory sticks or other portable storage media or computer; encryption; removal or duplication of data from secure servers; transmitting or transporting data; use of identifiable identifiers; and availability of data to non-VA investigators.

The handbook also is to include specific instructions to Institutional Review Boards (IRBs) who review and establish protocols at the local level. The goal is to assure that all data security and privacy requirements are met before the start of a research project.

VHA already has significant protections for Medicare data in place (see Attachment C) and is committed to strengthening the protection of veterans' data. For example, ORD will implement a new requirement that all VA and Medicare research datasets reside

within the VA firewall. In addition to developing sound policy about researchers' use of data, VHA ORD is also committed to develop policy and assure enforcement, in collaboration with ORO, to confirm that data is appropriately managed and destroyed after a researcher has finished with the data.

To emphasize compliance, VHA ORD is increasing its effort to educate researchers about these policies to emphasize the importance of compliance. These actions include additional field conference calls, memorandums to the research community about specific topics, a separate section on the ORD website related to privacy and data security, newsletter articles to address specific issues, and individual contacts as concerns are identified.

Also, ORD is establishing a Privacy and Data Security Group using VA Central Office and field personnel to assure that policy is effective and appropriate to meet national requirements as well as individual situations in the field. This group will discuss issues such as education and training, policy, and effectiveness of implementation. Including a mix of Central Office and field perspectives assures that policy is strong and implementation is practical to assure research continues with the strongest safeguards available to protect veteran's data.

Audit and Enforcement. VHA Office of Research Oversight (ORO) reports directly to the Under Secretary for Health and is the primary office in VHA for overseeing the responsible conduct of research and investigations of allegations of research misconduct. Accordingly, ORO will be responsible for monitoring, auditing, and enforcing compliance with the policies and practices related to privacy and data security.

ORO Central Office carries out its assurance and compliance activities through a network of regional offices. VHA Office of Research and Development (ORD) and ORO are currently discussing changes that are needed to establish strong monitors and audit processes to assure enforcement and compliance with current and upgraded policy and required procedures.

Question 8: Please describe the security weakness in the VistA system. Please describe how VA plans to strengthen the identified weaknesses.

Response: During the security controls assessment testing component of VHA's certification and accreditation initiative completed in fiscal year 2005, VHA found the following issues specific to VistA Legacy, which have been determined to be national in scope. Each is identified by its control title, per National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-53. All of these issues are currently being addressed.

Account Management – Currently, access codes are created for a new user and the verify code is left blank. When the new user logs on to the system for the first time, they are prompted to create a verify code. To meet NIST requirements all accounts must

have a User ID and password (access code and verify code) assigned. Currently, VHA's Office of Information (OI) is developing a patch to the VistA Legacy software that forces creation of a verify code at the time a new user account is created.

Access Enforcement – Identified as a vulnerability across VHA sites, this issue centers on the fact that many users have high-level access privileges at some sites. A high number of users with administrative-level or other administrator-like access privileges were identified during security controls assessment testing. This must be remediated at the local level by a thorough review of user access and determination of continued need. This review is currently under way across the Department.

Separation of Duties -- System administrators have the ability to review audit logs. While VHA believes this is not an issue because these positions are held to a high standard of security and require high-risk background investigations, it is not in compliance with current NIST requirements. NIST requires some elements of the control to be organizationally defined, which is a Departmental responsibility. Further guidance will be issued to the sites to address this vulnerability in VistA Legacy systems as soon as the control elements have been defined.

Remote Maintenance -- A high number of sites were found to have desktop computers containing modems that are connected to the VA network. Sites have been directed to review desktop computers and remove all resident modems unless they are specifically justified and a waiver has been granted. In addition, system security plans must reference or contain risk mitigation strategies for computers containing modems that are connected to the VA network.

At the time the security controls assessment testing was completed in FY 05, VHA identified more than 4,126 vulnerabilities across all VistA legacy systems installed and operational at VHA facilities. Of these, 613 are ongoing and 211 are considered to be national in scope. This is not 211 specific issues but 19 issues identified at multiple locations. VHA continues to address these issues at the facility and national levels and has finalized a plan to remediate all remaining issues identified through this specific phase of security controls assessment testing by December 2006.

Question 9: Please describe how the VHA CIO office coordinates with the VA CIO office to identify and address security weaknesses in VistA software and other VHA database software.

Response: This is accomplished through the certification and accreditation requirements as described above. Results of the security controls assessment testing component are used to populate the Department's POA&M database so that remediation actions can be monitored and tracked through completion.

The Honorable Corrine Brown

Question 1: What kind of protection is the health data under?

Response: Within the Veterans Health Administration (VHA), health data is protected under the HIPAA Privacy Rule, Privacy Act of 1974, and Title 38 United States Code Section 5701 and 7332.

Question 2: Providers are required to have in place reasonable safeguards to protect the privacy of patient information and, in general, must limit the information used or disclosed to the minimum amount necessary to accomplish the intended purpose of the use or disclosure.

Response: Correct. VA health care providers are required to limit their access to only the minimum amount of information necessary to perform their duties as outlined in VHA Handbook 1605.2, Minimum Necessary Standard for Protected Health Information.

Question 3: Are you compliant with HIPAA?

Response: The response that follows interprets the question to refer to the HIPAA Privacy and Security Final Rules under Title II of HIPAA. VHA has completed specific actions to comply with both HIPAA Privacy and Security requirements and acknowledges that ensuring ongoing compliance must, by definition, be a continuing goal that is achieved through ongoing monitoring and improvement activities.

HIPAA Privacy Rule Compliance: VHA has broadened its VHA Privacy Program to include the HIPAA requirements and updated its privacy policies and practices that comply with the requirements set forth in the HIPAA Privacy Rule as well as requirements of the Privacy Act, and title 38 privacy statutes. Compliance with these Federal privacy requirements and VHA privacy policies is monitored by the VHA Privacy Office on an ongoing basis through reviews of privacy practices throughout VHA and assessments of VHA health care facilities and Program Offices that are conducted in conjunction with the VHA HIPAA Program Management Office (PMO). A complaint investigation and remediation process, involving both the VHA Privacy Office and VHA HIPAA PMO, is in place and active.

HIPAA Security Rule Compliance: While VHA is the Covered Entity under HIPAA, VA is the business owner of the information security infrastructure; thus VHA is dependent on VA's security program in ensuring compliance. On May 23, 2005, the VA Office of Cyber and Information Security (OCIS) submitted a report detailing VHA's compliance with the HIPAA Security Rule which cites VA's overarching security program as ensuring VHA HIPAA Security Rule compliance. This report relied heavily on FISMA compliance as the foundation for HIPAA Security Rule compliance.

To enhance security compliance, VHA and OCIS Field Operations developed Security Policy and Procedures templates that were distributed by OCIS for use by VHA field

facilities in support of HIPAA Security compliance; the effect of these templates will be strengthened when the 1997 (pre-HIPAA Security Rule) VA Departmental policy is updated. The VHA HIPAA PMO also developed and distributed a HIPAA Security Rule Assessment Tool to enable VHA facilities to conduct self-assessments of their compliance level so they could develop and implement road maps to compliance. In addition, the VHA HIPAA PMO conducts ongoing Security assessment of health care facilities and Program Offices in conjunction with VA OCIS.

While we have made substantial progress in many HIPAA related areas, including a national banking industry award for a HIPAA Electronic Transaction initiative, we recognize that in the Security realm vulnerabilities exist. We will continue to work with VA OCIS to mitigate them and ensure an ongoing effort to continually monitor and improve capabilities in this area.