

**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 Health<sub>e</sub>Vet, 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 policies, 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.