Statement for the Record of

Jonathan B. Perlin, MD, PhD, MSHA, FACP
Under Secretary for Health
Department of Veterans Affairs
before the
House Committee on Veterans' Affairs

June 29, 2006
******* ***

Good morning, Mr. Chairman and Members of the Committee. Thank you for allowing me the opportunity to provide an overview of the security and privacy protections that Veterans Health Administration (VHA) has in place to protect the electronic health records and sensitive personal information of our veteran patients.

VHA is committed to providing the best possible health care to each of the 5.3 million patients we treat at our hospitals, clinics and other sites each year. Our nurses, doctors and other health care staff members devote themselves to delivering high-quality, compassionate care to these patients—the men and women who have bravely served our Nation. In VHA, as we carry out our mission, we are dedicated to fully protecting the security and privacy of veterans' medical information. It is one of our fundamental operational pillars.

Today, VA provides some of the best health care in the nation.[1] This is documented in the scientific literature and lay press. Patient satisfaction surveys say the same thing.[2] This outstanding level of patient care is due in large part to VistA – an Information Technology (IT) system that sets the gold standard for electronic health records.[3]

VistA is recognized as one of the best electronic health record systems in use anywhere. It is touted as a model for supporting the President's goal to implement electronic health records throughout the nation. At VA health care facilities around the country, it has helped doctors, nurses and other clinicians save tens of thousands of lives—and provide better, safer and more consistent care.

VHA has succeeded in integrating the electronic health record (including imaging and health-related bar code applications) in the day-to-day workflow of health care delivery processes to a greater degree than any other health care organization in the world.

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

[1] Longman, P. (2005), 'The best care anywhere', *Washington Monthly,* 27 (January/February): 38-48.
[2] Asch, S.M., E.A. McGlynn and M.M. Hogan (2004), 'Comparison of quality of care, for patients in the Veterans Health Administration and patients in a national sample', *Annals of Internal Medicine*, 141: 938-945.
[3] Morgan, Matthew W. (2005), 'The VA Advantage: The Gold Standard in Clinical Informatics', *Healthcare Papers*, volume 5, no. 4, 26-29.

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 statutorily strict 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 Health***e***Vet, a Web-based application that provides veterans, their families and clinicians secure access to trusted health information. My Health***e***Vet 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 VA beneficiaries receive seamless care.

- VHA National Databases - VHA collects healthcare and administrative data in national databases, many of which are located in the secure environment of 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***e***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 (behind the firewall) is not encrypted; when VA data are sent outside the firewall, a Virtual Private Network, or VPN, is used. Data transiting the VPN tunnel are, by definition, encrypted. 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.

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. VHA will comply with any new guidance or directives issued regarding the use of non-VA computer equipment, as set forth by the Department.

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

To illustrate the strength of our security and privacy measures, I would like to call your attention to the Department of Defense/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 was FHIE/BHIE built to the highest standards, it also has received positive assessments from independent reviewers and high scores on National Institute of Standards and Technology criteria. It also is 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.

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, which provides secure, remote access.

FHIE/BHIE is in full compliance with VA, DoD and Federal government information security policies and privacy rules. In December 2005, the system underwent recertification, and received renewal of its authority to operate decision.

VHA Actions In Response to OIG Vulnerabilities

In a recent report, the OIG identified 16 security vulnerabilities. VHA has taken a number of actions to address the nine unresolved security vulnerabilities within VHA's purview; the seven remaining actions are the responsibility of the Department. To verify that VHA has the appropriate safeguards in place for data security and privacy, VHA has taken the following actions: System-wide Ongoing Assessment and Review Strategy site visits, HIPAA/privacy site assessments, and a recent communication from the Deputy Under Secretary for Health for Operations and Management requiring local management to certify compliance with security safeguards consistent with OIG findings. VHA leadership has also been monitoring the completion of all deficiencies identified as a result of the completed certification and accreditation work. Related to the monitoring activities, a recent memo from the Principal Deputy Under Secretary for Health, reiterated the importance of security remediation and directed VHA system owners to complete all remaining actions by June 30, 2006.

The Deputy Under Secretary for Health for Operations and Management also issued a memorandum in May 2006 requiring all facilities to submit an inventory of external business partner gateways through their Veterans Integrated Services Network (VISN) offices; all VISNs have complied with this request. In addition, the facilities are required to prepare and submit the necessary paperwork for the gateways to the VA Enterprise Security Change Control Board for formal review and approval. VHA policy requires all older operating systems installed on medical equipment to be connected to facility networks using the VA's Isolation Architecture as published in April 2004. This architecture provides increased security controls through a well-defined structure of isolation from the facility's main information network.

VHA's change control procedures are in the process of being addressed through several actions, which involves the strengthening of the current software development governance process. VHA is instituting a rigorous Capability Maturity Model Integration approach with assistance from Carnegie Mellon's Software Engineering Institute. The outcome of the approach is a fully integrated and effective configuration management and change control process implemented across the organization.

VHA has implemented security controls to address wireless security vulnerabilities, but recognizes that there are a number of policies, procedures and tools that need to be implemented to improve VHA's ability to protect IT systems and data in the wireless environment. A workgroup has been formed to address wireless requirements from an organizational perspective to comply with OIG vulnerability assessments and recommendations. The workgroup is charged with developing a wireless security controls test plan for facilities, identifying standard tools to improve management and control of the wireless environment, and developing associated policy templates and assessment checklists.

Privacy/Security Issue
Since the unfortunate theft occurred of veteran data, while it did not include VHA health care data, VHA has used this as an opportunity to validate its ongoing security and privacy practices, has re-educated its employees and contractors about privacy and security, and has begun making bold changes where necessary. These decisive actions are in addition to the many other measures VHA takes on an ongoing basis to ensure the security and privacy of our veterans' medical information.

A privacy and security issue was brought to light in 2005 when a sub-contractor in India threatened to expose medical records of veterans due to non-payment by their contractor. [4] VA had originally provided the medical information to a transcription company, and was alarmed to learn that VA-contracted medical transcription services had been subcontracted to an offshore company without our knowledge. Various offices within VA, including the OIG, the Office of the General Counsel, and VHA were involved in the review, investigation and resolution of this matter. Though VHA determined that no privacy disclosure violation had occurred in this incident under the Privacy Act of 1974 or Health Insurance Portability and Accountability Act (HIPAA), action was taken to ensure that no VHA programs were contracting for non-domestic transcription services. A settlement agreement reached in this matter included an agreement to destroy all records that the vendor had in its possession. A certification was subsequently received from the vendor stating that it had permanently destroyed all hard copies of records and deleted all electronic files containing VA medical records.

In response to the concerns raised by this incident and concerns regarding contractors using offshore or non-domestic subcontractors, VHA issued a moratorium on contracting for non-domestic telehealth services in May 2005. In addition, the Business Associate Agreement (BAA) template was revised to include language requiring contractors to only use subcontractors or agents who are physically located within a jurisdiction subject to the laws of the United States. The Under Secretary for Health further strengthened VHA's position to prohibit offshore work in a memorandum issued in June 2006 that permanently requires contractors to transcribe in the United States or its territories, and requires all facilities to have BAAs in place. Transcription vendors contracted by VHA must also sign BAAs in addition to following Privacy Act requirements.

We also are 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 Clinical Logistics Office will coordinate an interdisciplinary workgroup to review this data and prepare a report with recommendations on the feasibility of a national contract for

[4] OIG Draft Report, Audit of the Veterans Health Administration's Acquisition of Medical Transcription Services, Project Number 2004-00018-R3-0195

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 in October, 2006, with implementation to follow.

Actions to Further Strengthen Security and Privacy

At VHA, the security and privacy of veteran information is of paramount concern, and 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 to broaden auditing capabilities, and continue to implement enhancements to its existing role-based access mechanisms to ensure that access to information is based on defined roles.

The next generation of VistA, which is being developed now, will have enhanced security controls built into the system. This widely acclaimed system has saved the lives of tens 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. In the next generation of VistA, 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.

VHA already has strong security procedures in place, yet these procedures can be strengthened. We can do this by enhancing privacy and security guidance, through strong directives with enforceable actions, by conducting regular privacy and security-awareness training led by senior VHA leadership, and by emphasizing privacy and security education.

The recent theft of data that occurred has emphasized the need for extra vigilance in the use of the data that enables us to carryout our mission. The Secretary is developing a plan for VA to become the Gold Standard in the areas of security and privacy. VHA actively supports this direction.