Dr. William Winkenwerder, JR., MD
ASSISTANT SECRETARY OF DEFENSE (HEALTH AFFAIRS)
HEARING ON INFORMATION SECURITY

Introduction

Mr. Chairman, Distinguished Committee Members, I want to thank you for the opportunity to address you, and to report on the Military Health System (MHS) Information Security and the TriWest Computer Information Theft. The protection of beneficiary health care information is of the utmost importance to the MHS. Extreme care and diligence have been taken to put in place the appropriate safeguards to protect this information.

TriWest Computer Information Theft Overview

On Saturday, December 14, 2002, there was a physical break-in of the TriWest Healthcare Alliance Corporate II offices in Phoenix, Arizona. Computer equipment and petty cash were stolen. On Monday, December 16, 2002, the theft was discovered, police and investigative authorities were contacted and the TRICARE Management Activity (TMA) Operations staff was notified. On Tuesday, December 17, 2002, back up tapes were run to restore computer operations (30 hour process). Health Affairs/TMA was notified of beneficiary information theft on Friday, December 20, 2002. The information that was stolen included: beneficiary names, addresses, phone numbers, social security numbers, some claims information with relevant procedure codes, and personal credit card information on 23 individuals. To date, TMA has not received notification of any verified cases of identity theft related to TriWest stolen computer equipment.

Actions Taken in Response to the TriWest Theft

Several steps have been taken to communicate with all affected beneficiaries. During December 21-31, 2002, TriWest mailed 562,797 letters to affected beneficiaries notifying them of the theft and providing information on how to protect against identity theft. TriWest mailed a second letter in early February 2003, with additional information to assist beneficiaries with reporting fraud online to Credit Reporting Agencies and provided the appropriate form for verifying if their SSNs were included on stolen computer equipment. An around-the-clock communication link with beneficiaries was established via Web, toll-free telephone numbers and e-mail. More than 66,000 web queries, 37,500 calls and 10,300 emails have been received. The 23 individuals who may also have had personal credit card information compromised were contacted by phone and informed of the incident and proper actions to be taken in response. I met with beneficiary groups and described the corrective actions being taken.

A number of additional actions were conducted in response to this theft. A government team was dispatched to TriWest, December 22-24, 2002, to make an initial impact assessment. I conducted daily conferences with leaders from the MHS, Defense Criminal Investigative Service (DCIS), and TriWest. Information about the potentially compromised data was provided to the Social Security Administration and Federal Trade Commission. A $100,000 reward for information leading to conviction of individuals responsible was posted by TriWest. A review of security language in current and new TRICARE contracts was initiated to ensure incorporation of strong security requirements.

I requested that all TRICARE contractors perform a physical security assessment of their facilities using a government developed matrix composed of the Defense Information System Agency (DISA) Physical Security checklist and industry best practices. The majority of the physical security assessment results were received by January 1st and the remaining assessments were submitted by January 21st, 2003. On-site validation of the contractors' assessments were conducted by government teams and completed by February 7, 2003. The TRICARE contractors have provided timelines to address the mitigation of deficiencies identified during the assessment process. These actions have further strengthened the TRICARE contractors' overall security posture in terms of protecting our beneficiaries health care data. I requested that the Service Surgeons General also conduct a physical security assessment of all their military treatment facilities using the same matrix. The Services' assessment has been completed and each Service is developing measures and timelines to correct deficiencies.

Additionally, I asked that the Department of Defense (DoD) Inspector General's (IG) office conduct a rapid assessment of the physical information safeguards in place at a sampling of TRICARE contractor sites and DoD medical treatment facilities (MTFs) where patient-sensitive electronic data are stored. The IG is currently conducting assessments at a number of MTFs and TRICARE contractor sites. The report will be available in September 2003.

I formed a Health Information Security Working Group (HISG) comprised of senior representatives for HA/TMA, Service Surgeons General, Command, Control, Communications and Intelligence, Defense Management Data Center, DISA, and TRICARE Contractors. This work group, with support from information systems experts, is currently reviewing security practices and will make recommendations, as needed, for additional requirements for information security. The first meeting occurred on January 14, 2003 to examine commercial and DoD information security best practices, review regulatory requirements and discuss physical security self assessment check lists. On March 28th 2003, TMA conducted a follow up meeting through the HISG, to review and discuss the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), DoD Information Technology Personnel Background Investigation requirements, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulatory requirements, and the DISA Physical Security and industry best practice matrix.

It should be noted that in 1967, a decision was made to use the SSN as the universal identifier for the Department of Defense (DoD). The decision was made to avoid the use of separate personal identifiers within the Medical, Financial, and Personnel communities of DoD. Additionally, the SSN is the one number that connects DoD to other Federal Agencies such as Department of Health and Human Services and the Social Security Administration. To move to a separate identifier would negatively impact the services provided to TRICARE beneficiaries.

Military Health System Information Security

The Military Health System (MHS) Information Security (IS) Program vigilantly protects patient information of Service members, military retirees, and beneficiaries in accordance with Federal and Department of Defense (DoD) policies and guidance. The MHS IS Program does this by enhancing the integrity, availability, confidentiality, non-repudiation, and authentication of MHS Automated Information Systems (AISs) and networks that support military medical readiness and peacetime health care.

This program monitors IS operations to ensure critical health care information is available throughout DoD's Global Information Grid. It also ensures critical health care information is managed consistently with defense in depth methodology and evolving DoD IS Strategic Goals of protecting information, defending systems and networks, providing IS situational awareness and IS command and control, improving and integrating IS transformation processes, and creating an IS empowered workforce.

The MHS IS Program accomplishes its missions by utilizing a variety of government and industry security assessment resources and tools to continuously strengthen the MHS security program and plans. The program performs comprehensive risk assessments which test security controls. Third party assessments of MHS Security Program are frequently conducted to validate that policies and practices align with government and industry best practices such as the Information Assurance Vulnerability Management program, security practices from National Institute of Standards and Technology, Computer Security Institute, Carnegie Mellon, General Accounting Office, Defense Information Systems Agency, etc.

This program maintains an IS empowered workforce through an aggressive training program which includes initial user security training and yearly refresher training via an automated Web-based IS security and awareness module for all users. Advanced training is also available through IS training media, including those provided by DISA, either through Web-based training and/or CD ROMs for individuals with significant security responsibilities. Formal classroom training and professional seminars are coordinated to promote and expand IS knowledge (e.g., coursework from The National Defense University such as Information Security Common Body of Knowledge; Critical Information Systems Technologies; Managing Information Security in a Network Environment; and Assuring the Information Infrastructure.)

The MHS information security program aligns with DoD security regulations and guidelines to include the DoD Information Technology Security Certification and Accreditation Process and DoD Information Technology Personnel Background Investigation requirements. The MHS also provides strong representation on DoD IS workgroups. These DoD workgroups provide the direction for emerging DoD security requirements and assist in the preparation of DoD security requirements. The MHS IS workgroup, comprised of TMA, Army, Navy, Air Force, Defense Information Systems Agency and Joint Staff representatives, develops a single Tri-Service strategy for incorporating DoD information security requirements into the MHS. Coordination through the MHS IS workgroup has resulted in a cohesive medical process for addressing dynamic DoD information security requirements.

The MHS has been a leading partner in the development of health information security and privacy standards at the national level. Under the Health Insurance Portability and Accountability Act (HIPAA), representatives from the MHS have participated with federal agencies to include the Department of Health and Human Services, Department of Veterans Affairs, Food and Drug Administration, Centers for Disease Control, Social Security Administration, and Centers for Medicare and Medicaid Services, in crafting the regulations that define health information privacy and security protections. Over the last two years, the MHS has diligently worked to meet the HIPAA Privacy regulation by the April 14, 2003, implementation date. With the recent publication of the HIPAA security rule on February 20, 2003, and the directed implementation deadline of April 15, 2005, the MHS will execute a comprehensive analysis of the regulation and finalize a plan for implementing HIPAA security throughout the MHS.

Conclusion

Mr. Chairman, we take seriously our responsibility to protect the privacy and confidentiality of the patient information for our Service members and our broader military family.

Extensive efforts to further enhance physical security are ongoing. Based on outcomes of ongoing assessments, DoD will determine if additional resources and support are required to plan, program and implement new requirements.

Thank you for the opportunity to testify before your Committee on this important issue.