VA Office of Inspector General

OFFICE OF AUDITS & EVALUATIONS

Review of Information Security Issues Impacting VA Teleradiology Contracts

July 20, 2010
10-03122-198

ACRONYMS AND ABBREVIATIONS

CAMRIS	CAMRIS International Inc.
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act
ISO	International Standards Organization
OI&T	Office of Information & Technology
OIG	Office of Inspector General
PACS	Picture Archiving & Communication System
VA	Veterans Affairs
VHA	Veterans Health Administration
VistA	Veterans Health Information Systems and Technology Architecture

Report Highlights: Review of Information Security Issues Impacting Teleradiology Contracts

Why We Did This Review

The Office of Inspector General (OIG) evaluated the merits of a hotline complaint alleging a specific contractor was not appropriately protecting sensitive patient data while performing Teleradiology services for certain Veterans Affairs (VA) medical facilities. We also evaluated whether VA was providing adequate oversight of specific vendor contracts to ensure they met VA's information security requirements.

What We Found

We substantiated the specific allegations of inadequate protections of sensitive patient data and determined comprehensive procedures had not been effectively implemented to mitigate the risk of unauthorized disclosure of sensitive information. Specifically, we substantiated that:

- Patient data is transmitted to the vendor via unencrypted facsimile machines.
- Radiologists and Case Managers could copy, transfer, and store sensitive patient data onto their personal computers.
- VA and the vendor had not maintained a complete listing of all hardware used when evaluating patient data, thereby hindering proper sanitization of equipment.
- Quality assurance procedures had not been implemented to ensure personal computers used by contractor staff provided appropriate security protection.
- VA's oversight of specific vendor contracts did not ensure that contracts contained defined security requirements, thus placing VA sensitive data at risk of inappropriate disclosure or misuse.
- Backup servers were not implemented on the vendor network to provide system fault tolerance in the event of a service disruption.

What We Recommend

We recommend that the Under Secretary for Health and Assistant Secretary for Information and Technology implement procedures to effectively mitigate the risk of unauthorized disclosure of sensitive patient data.

Agency Comments

The Assistant Secretary for Information and Technology and the Under Secretary for Health agreed with our findings and recommendations. The OIG will monitor implementation of the action plans.

(original signed by Sondra F. McCauley, Deputy Assistant Inspector General for Audits and Evaluations for:)

BELINDA J. FINN
Assistant Inspector General for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Objective

We conducted this review to determine the merits of a hotline complaint alleging that a vendor was not appropriately protecting sensitive patient data while performing Teleradiology services for select VA medical facilities.

Complaint

A primary complainant contacted the VA Office of Inspector General on June 4, 2009, followed by a second complainant, who both alleged that CAMRIS International Inc.'s (CAMRIS) processes and security controls do not appropriately protect VA patient data while providing Teleradiology services on behalf of VA. Specifically, the allegation states the contractor is not complying with VA security policies in the following areas:

- Transmission of VA patient data is not encrypted and is sent to unauthorized personnel by CAMRIS employees.
- VA patient data is commingled with other client data or stored on personal computers of CAMRIS International, Inc.
- CAMRIS does not properly destroy or sanitize hardware containing VA patient data.
- CAMRIS did not perform quality assurance checks of Teleradiology systems to ensure compliance with VA security policies.

Additionally, we reviewed the contractor's business processes, system configurations, network and system architectures, and data flows. We identified weak control points and risks that could adversely impact the quality of patient care provided by the contractor and its ability to comply with the terms of VA contracts. Furthermore, we reviewed applicable Teleradiology contracts to determine whether those contracts incorporated consistent and appropriate information security requirements for providing security protections commensurate with the requirements of Federal Information Security Management Act (FISMA). The results of our analysis are included in the following sections of this report.

RESULTS

Finding 1 Encryption and Transmission of Patient Data

Our review showed that some VA patient data such as name, address, date of birth, or social security number is transmitted via unencrypted facsimile machines from VA medical facilities to the contractor as part of initial requests for Teleradiology services. Subsequently, the contractor evaluates the request and prepares a preliminary Teleradiology consultation report, which is faxed back to the facility for entry into the Veterans Health Information Systems and Technology Architecture (VistA).

We also noted that Case Managers and Radiologists remotely access the contractor systems and VistA via encrypted virtual private network connections. Consequently, we partially substantiated the allegation that the electronic transmission of VA patient data with the contractor is unencrypted. Without providing encryption protections during the facsimile transmissions of sensitive VA patient data, VA cannot ensure that patient information is adequately protected from unauthorized disclosure.

Federal Information Processing Standards 140-2, *Security Requirements for Cryptographic Modules,* states that selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security in its computer and telecommunication systems. Additionally, the publication provides a standard for Federal organizations to use when these organizations specify that cryptographic-based security systems will be used to provide protection for sensitive or valuable data.

VA Handbook 6500, *Information Security Program,* states that due care should be taken when "…faxing sensitive information…" and it is authorized as long as secure fax machine procedures are followed. VA Handbook 6500 further advises that personnel should place the following statement on all fax cover sheets:

> *This fax is intended only for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All others are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above.*

VA medical facilities had not implemented a secure fax capability because VA Handbook 6500, *Information Security Program,* does not define a clear policy to encrypt sensitive data traversing public telecommunication circuits. To mitigate risks of unauthorized disclosure of sensitive patient data, VA could implement an encryption solution that would protect sensitive data that is transmitted (via facsimile machines) across open telecommunication circuits. Contractor representatives have stated that they are implementing a Health Level 7 Interface solution[1], which would enable a secure connection from VistA to their call center, thus reducing the need for transmitting VA sensitive information via unsecure fax or in clear text.

[1]Health Level 7 is a messaging standard that enables clinical applications to exchange data while utilizing the seven-layer International Standards Organization (ISO) Communications Model.

Finding 2 Commingling and Storage of Patient Data

The contractor's current business processes introduced risks that VA patient data was not adequately protected to meet VA policy and the contract requirements. In connection with providing Teleradiology services, some Radiologists and Case Managers work from home (using personal computers) and remotely access VA patient X-ray images via encrypted network connections. Although remote access to contractor systems is encrypted, Radiologists and Case Managers have the opportunity to copy, transfer, and store sensitive VA patient data onto their personal computers, while interpreting X-ray images.

Procedures have not been implemented to document and provide assurances that personal computers, used by remote Radiologists and Case Managers, utilize the appropriate security protections such as firewall and antivirus software. Additionally, procedures have not been implemented to ensure that personal computers do not store sensitive patient data in accordance with VA policy and contract requirements. While we did not identify specific instances of inappropriate commingling of VA patient data at the data centers, the current business process introduces the risk that sensitive patient information could be stored on personal computers used by contractor staff.

One VA contract stated that VA sensitive information may not reside on non-VA systems or devices unless specifically designated and approved as appropriate in accordance with the terms of the contract. Additionally, the contractor is responsible for protecting its equipment and system software and preventing malicious code from being transmitted to VA systems. Contractors are responsible for keeping the system's software, configurations, and hardware updated to the latest necessary protection required to guard against malicious code. Finally, contractors are required to document compliance with security requirements prior to connecting equipment to VA's network. In "Finding 6" of this report, we note that VA did not define consistent information security requirements across all active Teleradiology contracts.

VA Handbook 6500 also states that VA sensitive information may not reside on other non-VA owned equipment unless specifically designated and approved in advance by the appropriate VA official. Contractor representatives indicated that they have limited resources to ensure that VA patient data is not stored on personal computers and appropriate computer security protections are applied. Additionally, VA Contracting Officer Technical Representatives have not implemented necessary oversight procedures to ensure that the security requirements of the contracts are enforced, to include the appropriate security of personal computers. While Case Managers and Radiologists connect to the contractor network via an

encrypted connection, their personal computers can be infected with malicious viruses or worms, which can spread to interconnected systems.

One risk mitigation strategy would be to eliminate the use of personal computers on Teleradiology contracts and require that all Case Managers and Radiologists use either VA-owned equipment or contractor-provided equipment. This approach reduces the likelihood that VA sensitive data would be commingled with personal data and would strengthen security controls protecting patient information. According to an official with VA's National Teleradiology Program, the unit cost for computer equipment for Radiologists is approximately $2,000. Consequently, the cost for providing VA-owned or contractor-provided computer equipment for Case Managers and Radiologists nationwide would not be significant in order to substantiality improve the security protections of equipment ultimately connected to VA systems.

The contractor currently provides 14 Radiologists in support of three Teleradiology contracts with VA. Without providing adequate computer equipment and appropriate security protections for all systems used in providing Teleradiology services, VA cannot ensure that sensitive patient information is adequately protected from unauthorized commingling and disclosure of sensitive data.

Finding 3 Destruction of Sensitive Patient Data

VA representatives and the contractor could not provide a complete listing of all hardware and storage devices used while providing Teleradiology services on active and terminated VA contracts. While the contractor maintained a listing of major hardware used to store and process VA sensitive data over the past 5 years, the listing did not include the personal equipment used by the Radiologists performing interpretation services under VA contracts. In addition, VA representatives did not maintain an accurate listing of contractor systems and hardware to ensure that VA sensitive data was properly destroyed in accordance with the contract and VA policies. Finally, procedures had not been developed to validate that VA sensitive data had not been stored or data had been appropriately removed from personal equipment used by Radiologists and Case Managers. Consequently, we partially substantiated the allegation that the contractor does not properly destroy or sanitize hardware containing VA patient data.

VA Handbook 6500.1, *Electronic Media Sanitization*, states that users of non-VA leased or owned equipment (including personally-owned, vendor-owned, or research equipment) are required to protect all VA sensitive information from unauthorized disclosure. One VA contract states that upon termination of the contract, computer equipment or other devices that have stored or processed sensitive data used in performance of contractual obligations will be sanitized according to VA standards and guidelines. Hard drives owned or used by the contractor that store VA patient sensitive data will be either sanitized by a method approved by the VA or turned over to VA for sanitization at the end of the contract. Items turned over to VA for sanitization will not be returned to the contractor.

The contract also states that if contractor equipment or devices that have stored VA sensitive data are taken out of use, disposed of, or sold as salvage, the contractor will certify that any confidential or private information is rendered totally unrecoverable before disposing of the equipment or components. In "Finding 6" of this report, we noted that VA did not define consistent information security requirements across all active Teleradiology contracts.

VA and the contractor have not developed processes to ensure a full accountability of systems and storage devices supporting Teleradiology services. We also noted that Contracting Officer Technical Representatives were not fully aware of the information security requirements of the VA and the security requirements of the Teleradiology contracts. As discussed earlier, one risk mitigation strategy would be to eliminate the use of personal computers on Teleradiology contracts and require that all Case Managers and Radiologists use either VA-owned or contractor-provided equipment.

This approach would improve accountability for equipment used on Teleradiology contracts and would allow VA or the contractor to sanitize all computers of potential VA sensitive data as needed. Without developing an accurate inventory of Teleradiology hardware, VA cannot provide adequate controls over the destruction of patient data hosted on contractor equipment, to include personal equipment.

Finding 4 Quality Assurance Reviews of Teleradiology Systems

As previously stated, some Radiologists and Case Managers work from home (using personal computers) and remotely access VA patient X-ray images via encrypted network connections. Although remote access to contractor systems is encrypted, Radiologists and Case Managers have the opportunity to copy, transfer, and store sensitive VA patient data onto their personal computers, while interpreting X-ray images. While the contractor performs quality assurance reviews of systems hosted at the contractor data centers, they have not implemented procedures to ensure that personal computers have utilized appropriate security protections in accordance with VA policy and contract requirements. Accordingly, we partially substantiated the allegation that the contractor did not perform quality assurance checks of Teleradiology systems to ensure compliance with VA security policies.

Contractor representatives indicated that they have limited resources to account for employee personal computers, ensure that appropriate security protections are applied, and provide assurance that VA patient data is not stored on personal computers. Although Case Managers and Radiologists connect to contractor networks via encrypted connections, their personal computers can be infected with malicious viruses or worms, which can spread to interconnected systems. One risk mitigation strategy would be to eliminate the use of personal computers on Teleradiology contracts and require all Case Managers and Radiologists to use VA-owned equipment or contractor-provided equipment.

Finding 5 Contract Security Requirements

We reviewed the three active Teleradiology contracts to determine whether those contracts contained language that required contractors to provide information security protections commensurate with the requirements of FISMA. We noted none of these three contracts provided information security clauses consistent with FISMA requirements. In addition, we noted that the contracts did not include consistent information security requirements across all contracts. For example, one Teleradiology contract required VA sensitive data to be retained for 12 months at the contractor data center, while another required VA sensitive data to be purged after 96 hours. The remaining active contract did not provide specific information security requirements.

> FISMA Section 3544 (b) requires that an agency provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

VA is in the process of incorporating FISMA security clauses into all of its service provider contracts but those changes have not been integrated into the current Teleradiology contracts. Additionally, we noted VA Contracting Officer Technical Representatives were not fully aware of the security requirements of FISMA and the need to incorporate those security requirements into the Teleradiology contracts. Without consistent and comprehensive information security compliance contract clauses, VA will continue to lack assurance that sensitive patient information is adequately protected. Furthermore, VA cannot hold third-party contractors accountable for lapses in information system security controls.

Finding 6 Service Availability

During our review of the network architecture, we noted contractor systems consisted of two server functions that are critical for providing Teleradiology services to VA. "Power Reader Server" is used to store VA patients' reports and images and the "Gateway Server" is used to store-and-forward the images from VA's VistA system. While these servers provide core Teleradiology services to VA, the contractor had not implemented backup servers to provide system fault tolerance in the event of a system failure or service disruption.

The three active Teleradiology contracts state that verbal preliminary interpretation reports from Radiologists shall be provided within 30 minutes of exam request and must be followed by written reports. The contracts define several performance objectives relative to Teleradiology services:

- Availability of radiologist—zero tolerance for non-availability
- Maintains patient privacy/confidentiality—zero tolerance for breaches in privacy
- Adheres to all Health Insurance Portability and Accountability Act (HIPAA) Requirements—zero tolerance for breaches in HIPAA requirements

While these contracts require a high availability for Teleradiology services, none of the existing contracts specifically require that the contractor implement fault tolerant systems in meeting these performance requirements.

Contractor representatives indicated that they have limited resources to implement redundant systems supporting the Teleradiology contracts with VA. In 2007, one Teleradiology contract was terminated because of multiple "Notices of Non-Compliance of Contract Requirements", to include service disruption from computer equipment failure.

To mitigate risks of recurring service disruptions, VA should ensure that Teleradiology contracts include requirements that contractor solutions provide fault tolerant systems and architectures. Without implementing hardware redundancy into its system architecture, the contractor cannot ensure that it can meet its service availability requirements in the event of a system failure or service disruption. Ultimately, VA is at risk of not receiving timely diagnoses of X-ray images, which could adversely impact the quality of patient care provided at VA medical facilities.

Recommendations

The contractor currently provides Teleradiology services to VA medical facilities under three contracts. As the performance periods for those contracts expire over the next several months, VA will be soliciting additional Teleradiology services. The recommendations below address business processes that will impact future Teleradiology contracts with VA. Recommendation 1 is directed to the Assistant Secretary for the Office of Information and Technology. While recommendations 2 through 6 are directed to the Under Secretary for Health, the Veterans Health Administration (VHA) must work in conjunction with the Office of Information and Technology to ensure that Teleradiology service providers meet VA's information security requirements.

VA must take timely action to implement these recommendations to protect sensitive VA patient information more effectively.

1. We recommend that the Assistant Secretary for Information and Technology develop clear policy and implement controls to protect the confidentiality of sensitive patient information transmitted via unencrypted facsimile devices.

2. We recommend that the Under Secretary for Health require that all personnel providing Teleradiology services use only VA or contractor-owned computers.

3. We recommend that the Under Secretary for Health implement automated mechanisms to ensure that all computers, supporting Teleradiology services, deploy and maintain appropriate security protections, such as firewalls and antivirus solutions, in accordance with VA policy and the terms of the contracts.

4. We recommend that the Under Secretary for Health implement procedures to fully inventory all Teleradiology hardware and sanitize all equipment used by Teleradiology service providers.

5. We recommend that the Under Secretary for Health incorporate consistent and comprehensive information security clauses into current and future Teleradiology contracts, in accordance with FISMA and VA's information security policy.

6. We recommend that the Under Secretary for Health ensure that current and future Teleradiology contracts include clauses requiring that contractor solutions provide fault tolerant systems and architectures.

Appendix A Response from the Assistant Secretary for Information and Technology

The Assistant Secretary for Information and Technology concurred with recommendation 1 and provided a response. The Assistant Secretary stated that the VA Handbook 6500 Information Security Program will be revisited to improve fax handling procedures and control requirements. Additionally, OI&T will update the annual security awareness-training program to address the proper use of fax machines and will continue to review emerging technologies to improve security over the transmission of sensitive patient data.

OI&T identified several factors that may mitigate the risks of using unsecured facsimile machines to transmit sensitive data. We noted that some health organizations utilize "Secure Fax" services to securely store and transmit sensitive health information with external organizations. Moving forward, OI&T should consider whether the use of "Secure Fax" services would improve the protection of sensitive veteran data that is transmitted to external service providers. We consider OI&T's actions plans to be acceptable and will follow up on their implementation. OI&T's entire response to our finding and recommendation follows this summary.

Department of Veterans Affairs

Memorandum

Date: June 2, 2010

From: Assistant Secretary for Information and Technology (005)

Subj: OIG Draft Report, Review of Information Security Issues Impacting Veteran Affairs (VA) Teleradiology Contracts (WebCIMS 455078)

To: Assistant Inspector General for Audits and Evaluations (52)

Thank you for the opportunity to review the subject draft report. The Office of Information and Technology concurs with the report findings and submits the attached response to address recommendation 1. If you have questions, please contact Lou Grippo, Office of Information Protection and Risk Management (005R), at (202) 461-6348.

(Original signed)

Roger W. Baker

Attachment

Attachment

OIG Draft Report, Review of Information Security Issues Impacting Veterans Affairs (VA) Teleradiology Contracts (WebCIMS 455078)

Date of Draft Report: April 9, 2010

Recommendations/ Actions	*Status*	*Completion Date*

Recommendation 1. We recommend that the Assistant Secretary for Information and Technology develop clear policy and implement controls to protect the confidentiality of sensitive patient information transmitted via unencrypted facsimile devices adequately.

Concur

VA has issued policy to address the risks and concerns. VA Handbook 6500, Information Security Program Handbook, Section (8) (Facsimile Machines) outlines proper FAX handling and control requirements, but as with all policy, shall be revisited for improvement in the next planned document revision. Also Section (9) (PBX Voice/Data Telephone Systems) sufficiently outlines proper PBX handling and control requirements, but as with all policy, shall be revisited for improvement in the next planned document revision.

Policy violations and incidents shall be resolved via methods available to the contracting officer with guidance from Information Protection and Risk Management (IPRM) organization.

Although, the use of facsimile (FAX) transmissions should generally be discouraged, their use cannot be eliminated because they still remain a very common and key component of timely information delivery. Technologies reliant upon the Internet do not ensure timely delivery of data in emergency situations. The Internet is far more prone to denial of service and other malicious threats. For example in teleradiology cases, the STAT (Urgent) X-Ray reading requests are provided to the vendor via FAX for immediate review. The reading is delivered over the phone, and then the reading is documented in the system.

In these cases, personally identifiable information (PII) sent unencrypted via analog facsimile transmissions over plain old telephone systems (POTS) and the Federal Telephone System (FTS) is permissible under current security guidelines. Although there is a concern that sensitive information may not be adequately protected during transmission, this is a known and accepted risk.

VA's Office of Information and Technology (OI&T) has identified the following factors that mitigate the risk:

- Small amounts of PII are sent via individual facsimile sessions for STAT readings (typically one patient).

- For transmissions using Voice over Internet Protocol (VoIP) to the Private Branch Exchange (PBX) confined to the local VA facility prior to transmission of FTS/POTS, VoIP use for facsimile delivery is contained to the local facility and is relayed through the facility PBX to the FTS/POTS network.

- VA facilities and their wiring are currently accepted as secured by adequate physical security, and, therefore, there is no encryption requirement at the facility.

- The FTS/POTS networks delivered by the various carriers are considered reasonably secure in that the switching centers would need to be compromised or the wires would need to be tapped on United States soil and in plain sight along the path between endpoints. VA OI&T, at present, is not prepared to declare this medium as insecure because the process in securing sensitive facsimile and voice transmissions would be cost prohibitive and generally impracticable. If threat vectors and incidents are determined to warrant reevaluation of this determination, VA would follow guidance issued by the National Institute of Standards and Technology and the Office of Management and Budget.

An observation was made that the contractor in question may have alluded to the use of the Health Level 7 (HL7) protocol between VA and vendor systems being a solution by providing needed security. VA OI&T would like to clarify that business-to-business (B2B) connections between systems using the HL7 protocol does not, on its own, provide any additional security. Encryption must be added such as with Transport Layer Security (TLS) that leverages a Federal Information Processing Standards (FIPS) 140-2 validated cryptographic module in FIPS mode (FIPS suite of algorithms only in use).

VA OI&T will seek to improve the required annual security awareness training by emphasizing policy and best practices relevant to FAX transmissions. VA OI&T will also continue to review emerging technologies that can better secure the required business processes.

The action that VA OI&T will be taking is increasing information in the Annual Security Awareness Training Module for all users on security measures for faxing information. The additional information has been provided to Training Education and Professionalism (TEAP), and the additional faxing information will be in the Security Awareness Training module released on October 2010.

Status: In process October 2010

Appendix B Initial Response from the Under Secretary for Health

The Under Secretary for Health concurred with recommendations 2 through 6 and provided corrective action plans for each recommendation. To improve the security over VA sensitive data, the Under Secretary for Health agreed that Teleradiology service providers should use only VA or contractor-owned computers. Additionally, the Under Secretary for Health agreed to review all service provider contracts to ensure they contain appropriate information security clauses.

The Under Secretary for Health plans to add language to contracts requiring that contractors provide fault tolerant systems and architectures. At the request of the OIG, the Under Secretary for Health provided additional information regarding their corrective action plans for recommendations 3 and 4. With the exception of the initial responses for recommendations 3 and 4, we consider VHA's corrective actions plans to be acceptable and will follow up on their implementation. The Under Secretary for Health's revised corrective action plans are included in Appendix C of this report.

Department of Veterans Affairs

Memorandum

Date: May 19, 2010

From: Under Secretary for Health (10)

Subj: OIG Draft Report, Review of Information Security Issues Impacting the Department of Veterans Affairs' (VA) Teleradiology Contracts, (WebCIMS 455078)

To: Assistant Inspector General for Audits and Evaluations (52)

1. Thank you for the opportunity to review the draft report. I concur with the report findings and recommendations 2-6. A response to recommendation one will be provided under separate cover by the Assistant Secretary for Information and Technology (005).

2. A complete action plan to address the report recommendations is attached. If you have any questions, please contact Linda H. Lutes, Director, Management Review Service (10B5) at (202) 461-7014.

(Original signed)

Robert A. Petzel, M.D.

Attachment

VETERANS HEALTH ADMINISTRATION (VHA)

Action Plan

OIG Draft Report, Review of Information Security Issues Impacting the Department of Veterans Affairs' (VA) Teleradiology Contracts, (WebCIMS 455078)

Date of Draft Report: April 9, 2010

Recommendations/ Actions	Status	Completion Date

Recommendation 2. We recommend that the Under Secretary for Health require that all personnel providing Teleradiology services use only VA or contractor-owned computers.

VHA Comments

Concur

The requirement that all personnel providing teleradiology services use only VA or contractor-owned computers will be placed in future contract language as they are awarded. However, it should be noted that some teleradiology vendors might withdraw because of this requirement.

Status: In process New contract requirement will begin May 2010

Recommendation 3. We recommend that the Under Secretary for Health implement automated mechanisms to ensure that all computers, supporting Teleradiology services, deploy and maintain appropriate security protections, such a firewalls and antivirus solutions, in accordance with VA policy and the terms of the contract.

VHA Comments

Concur

Automated mechanisms already exist for single users connected to VA using the Other Equipment - Remote Enterprise Security Compliance Update Environment (OE-RESCUE) and Government Furnished Equipment- Remote Enterprise Security Compliance Update Environment (GFE-RESCUE). These mechanisms currently provide an automated method of checking for appropriate anti-virus and firewall applications. All VA-issued GFE must be returned to VA at the end of the contract. The hard drive does not need to be surrendered because the GFE image enforces Full Disk Encryption (FDE). The encrypted information is non-sensitive once the access is revoked because it cannot be recovered.

For Site-to-Site (S2S) Virtual Private Network (VPN) connections to the Internet gateways and Business Partner Gateways (BPG) that connect directly to the facilities for high-bandwidth connections, there are no automated systems in place to ensure the compliance of attaching vendor networks. While VA enforces the connection encryption requirements, the security posture of the vendor is agreed to in the Memorandum of Understanding/Interconnection Security Agreement (MOU/ISA) that is signed by the vendor and the VA System Owner and approved by the Enterprise Security Configuration Control Board (ESCCB). Contracts going forward will stipulate that:

- Vendors are responsible for information security of the data on their systems;
- Penalties for improper disclosure of PII are covered under Health Insurance Portability and Accountability Act (HIPAA); and
- Damages and expenses are incurred by VA.

VA's OI&T will also continue to review emerging technologies that can better secure VA's required business processes.

Status: Completed

Recommendation 4. We recommend that the Under Secretary for Health implement procedures to fully account for all Teleradiology hardware and sanitize all equipment used by Teleradiology service providers.

VHA Comments

Concur

VA Handbook 6500.6, Contract Security already requires full accounting for all teleradiology hardware and sanitization for all equipment used by teleradiology service providers.

It is common practice for large teleradiology firms to receive images from multiple client hospitals. These images are routed to one server and distributed to a pool of radiologists. If the teleradiology firm co-mingles VA's images with other hospital images, the contract should specify how the disk drives and personal computers (PCs) will be ultimately disposed of in accordance with VA's destruction and media sanitization procedures, as specified in VHA Handbook 6500.6, appendix C, section 3.b and section 5.h.(4). Further, the vendor must have in place a Business Associate Agreement. The contract should stipulate that vendors are responsible for information security of the data on their systems and that penalties for improper disclosure of PII are covered under HIPAA.

Status: Completed

Recommendation 5. We recommend that the Under Secretary for Health incorporate consistent and comprehensive information security clauses into

current and future Teleradiology contracts, in accordance with FISMA and VA's information security policy.

VHA Comments

Concur

VHA currently requires consistent and comprehensive information security clauses under VA Acquisition Regulations (VAAR) 852.273-75, Security Requirements for Unclassified Information Technology Resources (Interim - October 2008). Other applicable security clauses will be included in all future contracts, and current contracts that do not already contain this clause will be modified accordingly. The Chief Procurement and Logistics Office will transmit a reminder to contracting officers to incorporate consistent and comprehensive information security clauses into future teleradiology contracts.

Status: In process May 30, 2010

Recommendation 6. We recommend that the Under Secretary for Health ensure that current and future Teleradiology contracts include language requiring that contractor solutions provide fault tolerant systems and architectures.

VHA Comments

Concur

When assessing the suitability of the contractor's architecture, the contract needs to note that VA retains the patient's images and does not rely upon the contractor to do so. Also, the contract needs to stipulate reports generated by the contractor are ordinarily transmitted to VA within 48 hours. The contractor does not provide long-term storage of these documents except for quality assurance and consultation purposes.

The continuity of operations plan should be specified in the contract. If the contractor's server fails or network connection is lost, the fall back plan may be that the contractor comes on-site to perform the work rather than requiring a specific fail-over server architecture.

Language requiring that contractor solutions provide fault-tolerant systems and architectures will be included in all future contracts. The Chief Procurement and Logistics Office will notify contracting officers when such language has been finalized and current contracts will be modified accordingly.

Status: In process May 30, 2010

Veterans Health Administration

May 2010

Appendix C Revised Response from the Under Secretary for Health

While VHA's initial response concurred with our findings and recommendation, we requested the Under Secretary for Health provide additional information regarding planned actions for recommendations 3 and 4. In the revised response, the Under Secretary for Health stated that VHA has begun coordinating the resources and approach for conducting service provider site assessments to evaluate compliance with VA's contract security requirements and Business Associate agreements.

We consider VHA's revised actions plans to be acceptable and will follow up on their implementation. The Under Secretary for Health's revised action plans are included in the following section of this report.

Department of Veterans Affairs

Memorandum

Date: June 24, 2010

From: Under Secretary for Health (10)

Subj: OIG Draft Report, Review of Information Security Issues Impacting the Department of Veterans Affairs' (VA) Teleradiology Contracts, (WebCIMS 455078)

To: Assistant Inspector General for Audits and Evaluations (52)

1. Attached is a revised action plan for recommendations 3 and 4 of the draft report. The revised plan not only outlines the Veterans Health Administration's (VHA) policy concerning privacy compliance assurance and monitoring, but also includes details on:

2. The Office of Information Technology Oversight and Compliance (ITOC) reviews of contracts that receive or store information on VA clients to assess compliance to security requirements;

3. VHA site assessment of business associates for compliance with VA contract security requirements; and

4. VHA continued collaboration with the Department's Office of Information and Technology to ensure contracts and agreements with business associates contain the required security language, and assess business associates operations for compliance with VA's security requirements.

5. If you have any questions, please contact Linda H. Lutes, Director, Management Review Service (10B5) at (202) 461-7014.

(Original signed)

Robert A. Petzel, M.D.

Attachment

VETERANS HEALTH ADMINISTRATION (VHA)

Action Plan

OIG Draft Report, Review of Information Security Issues Impacting the Department of Veterans Affairs' (VA) Teleradiology Contracts, (WebCIMS 455078)

Date of Draft Report: April 9, 2010

Recommendations/ Actions	Status	Completion Date

Recommendation 3. We recommend that the Under Secretary for Health implement automated mechanisms to ensure that all computers, supporting Teleradiology services, deploy and maintain appropriate security protections, such a firewalls and antivirus solutions, in accordance with VA policy and the terms of the contract.

VHA Comments

Concur

VA has implemented automated mechanisms to ensure that all systems that connect to the VA network are checked for appropriate anti-virus, firewall and other applications before the computer can connect to the VA network. The Remote Enterprise Security Compliance Update Environment (RESCUE) functionality also prevents users connected to the VA network from downloading VA data. VA/VHA does not have the capability; however, to validate the presence of security protections on business associates' systems that do not connect to the VA network. The security protections that business associates must implement and penalties for non-compliance are required to be written into contracts in accordance with VA Directive and Handbook 6500.6 and associated guidance. VA/VHA relies on the contractor to comply with the contract and Business Associate Agreement terms when doing business with VA.

In a May 21, 2010 memorandum, the Assistant Secretary for Information and Technology informed the Administrations that the Office of IT Oversight and Compliance (ITOC) would review all contracts that receive or store information on VA clients. The reviews are criteria-based (i.e., ten (10) largest dollar amount contracts, and twenty (20) randomly selected contracts). Additionally, ITOC will randomly select 2-3 vendors to physically assess their compliance to security requirements, such as encrypting computers when PII/PHI is contained.

Prior to the recent incidents involving improper disclosure of PII by business associates, VHA had begun putting the necessary infrastructure in place to begin conducting site assessments to ascertain compliance with VA's contract security requirements and Business Associate Agreements. Several site assessments have been conducted to

date, an assessment tool is being refined, and a comprehensive annual schedule is being established to conduct on-site reviews on an ongoing basis; assignment of priorities for conducting on-site assessments vs. self-assessments to be submitted by the business associate will be made based on pre-established criteria (i.e., corporate size of the business associate, volume of VHA data accessed by business associate; number of VHA facilities serviced by business associate; type of services provided by business associate; complexity of services provided by business associate; location of business associate; and previous data breaches, complaints or incidents involving business associate).

The schedule of these assessments includes a concentrated effort in the first quarter of fiscal year 2011 with additional assessments being conducted throughout the year, being normalized into the regular schedule as a part of ongoing evaluations conducted by the VHA Privacy Compliance Assurance Office. In fiscal year 2011, it is expected that approximately 5% of the national business associates will be assessed with an on-site assessment and the remaining 95% will be required to complete a self-assessment survey to determine their compliance level. Additional details regarding the on-site assessments such as the business associate name and location are being worked out. VHA compliance monitoring teams consisting of personnel from privacy and security components of VHA Office of Health Information will be trained on the business associate assessment process during a training session scheduled for the first week of August 2010.

In addition to the assessment activities, VHA released VHA Handbook 1605.03 in fiscal year 2009 that requires local facility privacy officers to develop a compliance monitoring process for evaluating the ability of local business associates to meet the terms of the business associate with the VHA facility. Also, this policy requires VHA Privacy Compliance Assurance (PCA) to evaluate the privacy officer's compliance with this Handbook and the business associate monitoring requirement. PCA is currently developing tools to be used by facility privacy officers to conduct these local business associate reviews.

VHA will continue collaborations with VA's OI&T to identify and implement emerging technologies, ensure contracts and agreements with business associates contain the required security language, and assess business associate operations for compliance with VA's security requirements.

Status: In process January 2010 with completion of first set of assessments.

Recommendation 4. We recommend that the Under Secretary for Health implement procedures to fully account for all Teleradiology hardware and sanitize all equipment used by Teleradiology service providers.

VHA Comments

Concur

As noted in response to Recommendation 3, VHA is putting the necessary infrastructure in place to begin conducting site assessments to ascertain compliance with VA's contract security requirements and Business Associate Agreements, and VHA will incorporate checks for an equipment inventory and media sanitization in the assessment tool. The planned schedule for on-site assessments of Business Associates will begin in the first quarter of FY2011.

Veterans Health Administration

June 2010

Appendix D Scope and Methodology

To determine whether the contractor's processes and security controls adequately protect the confidentiality, integrity, and availability VA patient data, we:

- Interviewed VA and contractor officials directly supporting VA's Teleradiology contracts,
- Reviewed relevant information security controls,
- Reviewed the contractor's current and terminated Teleradiology contracts with VA, and
- Reviewed applicable VA Directives and Federal requirements.

In addition, we interviewed the primary and secondary complainants to develop a better understanding of the nature of the allegations. To evaluate the effectiveness of system security controls supporting Teleradiology services, we:

- Reviewed the contractor's business processes, system configurations, network and system architectures, and data flows to identify relevant information security controls,
- Conducted system and business process walkthroughs with Case Managers and Radiologists, and
- Reviewed the contractor's business continuity, disaster recovery, and sanitization procedures supporting the Teleradiology services provided to VA.

We reviewed eight of the contractor's Teleradiology contracts with VA. Five of the contracts have been subsequently terminated for various reasons. We conducted our fieldwork at VA offices and the contractor's corporate office from July – October 2009.

Reliability of Computer-Processed Data

We did not request computer-processed data for this review. We evaluated information provided in connection with the Teleradiology contracts, workflow processes, and system security controls for sufficiency and accuracy during our review procedures.

Compliance with PCIE Standards

We conducted our review in accordance with *Quality Standards for Reviews* published by the President's Council on Integrity and Efficiency.

Appendix E Background

Teleradiology Services Provided

CAMRIS of Rockville, Maryland provides Teleradiology services for several VA medical facilities. Teleradiology services involve electronically transmitting radiographic patient images (such as X-rays) and consultative text from one location to another for the purpose of interpretation and/or consultation with Radiologists. Teleradiology improves patient care by allowing Radiologists to provide timely services without actually having to be at the location of the patient. Teleradiology specialists interpret patient images when VA Radiologists are not available.

Although VA has a large staff of medical doctors and Radiologists, a significant need still exists for radiology services during weekends, holidays, and certain shifts. Specialists such as Neuroradiologists or Musculoskeletal Radiologists generally work only during daytime hours, thus the additional radiology services are vital to patient services.

The contractor provides Teleradiology services to VA medical facilities under the following active contracts:

- Murfreesboro VA Medical Center
- Veteran Integrated Service Network 15
- Veteran Integrated Service Network 12

The contractor provides a staff of Radiologists to interpret X-ray images after normal business hours as needed. In fiscal year 2010, VA plans to solicit additional Teleradiology services as the performance periods for the above contracts are due to expire. In accordance with the requirements of the above contracts, VA will send two types of Teleradiology cases to the contractor for interpretation:

- **Routine Cases** are created by VA and X-ray images are routed to the contractor operations center (Nashville, TN) where they are stored on the application server. The Case Manager logs onto VistA to perform this routing function. The Case Manager contacts a Radiologist and routes the X-ray image to the Radiologist for interpretation. The Radiologist evaluates the image, creates a Routine Interpretation Report of the findings, and electronically signs the report. The Case Manager logs onto VistA system and transmits the final report to VA.
- **STAT Cases** are created by VA staff who immediately contacts the contractor's operations center. VA staff then routes X-ray images to the contractor's application server and transmit a requisition to the Case

Manager via facsimile device. The Case Manager contacts the Radiologists and has them access the images. Once the images are interpreted, Radiologists deliver the STAT report verbally and follow up with a written report. The Case Manager logs onto VistA system and transmits the final report to VA.

Data Flows

VHA developed VistA Imaging with Picture Archiving & Communication System (PACS) to integrate image-based information, such as pathology slides and scanned documents, into the VistA electronic medical records system. Within VHA, examinations are archived within the PACS system.

The contractor's applications consist of several servers that are hosted at the data center located in Nashville, TN. Critical application servers supporting Teleradiology services include the "Power Reader Server" used to store all of the VA's patient reports and images and the "Gateway Server" used to forward the images from VA's VistA PACS system. Case Managers and Radiologists remotely access the Power Reader and VistA PACS via virtual private network encrypted connections.

The contractor utilizes firewalls, compliant with Federal Information Processing Standards 140-2, to provide access control protection over critical applications. The contractor is implementing Health Level 7 interfaces for all VA medical facilities it supports. Health Level 7 is a messaging standard that enables clinical applications to exchange data while utilizing the seven layer ISO Communications Model.

Currently more than 90 percent of healthcare facilities in the United States use Health Level 7 interfaces enabling disparate medical systems and applications to communicate using common data formats and protocols. With the full implementation of the Health Level 7 interfaces, the contractor expects to process a greater number of cases per month. From September 2009 through December 2009, the contractor interpreted approximately 3,700 cases per month.

In fiscal year 2010, the contractor has made significant investments in improving its level of service to VA. For instance, a new web-based scheduling and case management system has been implemented to increase productivity and security of VA data. Additionally, the contractor has updated its Security Information Handbook and is developing procedures to improve the security and services provided to VA.

Appendix F OIG Contact and Staff Acknowledgments

OIG Contact	Michael Bowman, 202-461-4676
Acknowledgments	Carol Buzolich Elijah Chapman Katherine Gers Felita Traynham

Appendix G Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Assistant Secretaries
Office of General Counsel

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

This report will be available in the near future on the OIG's Web site at http://www.va.gov/oig/publications/reports-list.asp. This report will remain on the OIG Web site for at least 2 fiscal years after it is issued.