VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Audit of VA's Systems Interconnections With Research and University Affiliates

October 23, 2012
11-01823-294

ACRONYMS AND ABBREVIATIONS

CD	Compact Disc
DVD	Digital Video Disc
FISMA	Federal Information Security Management Act
IRB	Institutional Review Board
ISA	Interconnection Security Agreement
MOU	Memorandum of Understanding
NIST	National Institute for Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
PII	Personally Identifiable Information
VAMC	Veterans Affairs Medical Center
VHA	Veterans Health Administration

Report Highlights: Audit of VA's Systems Interconnections With Research and University Affiliates

Why We Did This Review

VA Medical Centers have numerous systems interconnections with external organizations to exchange the data needed to support a range of healthcare services and collaborative research studies. We conducted this audit to determine the effectiveness of VA's management of its systems interconnections and data exchanges with external research and university affiliates.

What We Found

VA has not effectively managed its network interconnections and data exchanges with its external research and university affiliates. Despite Federal requirements, VA could not readily account for the various systems linkages and sharing arrangements. VA also could not provide an accurate inventory of the research data exchanged, where data were hosted, or the sensitivity levels of the data. In numerous instances, we identified unsecured electronic and hardcopy research data at VAMCs and in co-located research facilities.

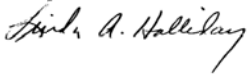
VA's data governance approach has been ineffective to ensure that research data exchanged are adequately controlled and protected throughout the data life cycle. VA and its research partners have not consistently instituted formal agreements requiring that hosting facilities implement controls commensurate with VA standards for protecting the sensitive data. Veterans Health Administration's decentralized approach to research data collection and oversight has not been effective to safeguard the sensitive information. Because of these issues, VA data exchanged with research partners were at risk of unauthorized access, loss, and disclosure.

What We Recommended

We recommended the Assistant Secretary, Office of Information Technology (OIT), in conjunction with the Under Secretary for Health, implement a centralized data governance model to improve VA's oversight of network interconnections and data exchanges with research partners. The Assistant Secretary should ensure that formal agreements are established or updated to require that research partners implement controls commensurate with VA standards for securing the data. We also recommended the Under Secretary for Health support OIT in ensuring research partners protect sensitive data they host in accordance with VA information security requirements.

Agency Comments

The Assistant Secretary for Information and Technology and the Under Secretary for Health generally concurred with our findings and recommendations. They stated that VA will implement agreements, security controls, infrastructure, and standardized data governance and collection to more effectively protect sensitive data. The OIG will monitor implementation of the corrective action plans.



LINDA A. HALLIDAY
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Objective

We conducted this audit to determine the effectiveness of VA's management of network interconnections and sensitive data exchanged with its research and university affiliates. Specifically, we evaluated VA's inventory of interconnections and its efforts to ensure data exchanged were adequately protected at hosting facilities. We also determined whether appropriate security agreements and controls were in place to enforce VA information security requirements at the external data hosting facilities.

Background

Within VHA, the Office of Research and Development (VA Research) takes pride in its history of innovative research and discovery to advance the healthcare of veterans. VA has estimated that during FY 2012, over $1.7 billion and 3,200 full-time personnel will be allocated to support over 2,100 VA research projects. VA Medical Centers (VAMCs) have numerous network interconnections with academic and external organizations to exchange data, such as medical and patient information, needed to help provide a range of healthcare services and perform collaborative research studies. OIT is an essential partner with VA Research through the delivery of available and secure technology services to VAMCs and dissemination of guidance on VA information security requirements Department-wide.

Adequate protection of the protected health information exchanged, including Personally Identifiable Information (PII), is essential to ensure continuing studies and advancements in medical research. VA acknowledges that while patients are willing to participate in research studies, they will do so only if their personal data are not placed at undue risk of loss, theft, or other misuse.

Prior OIG Oversight

Previous VA Office of Inspector General (OIG) Federal Information Security Management Act (FISMA) reviews have identified issues with VA's management of systems interconnections, as well as control deficiencies that could prevent VA from detecting and responding to intrusion attempts in a timely manner. The reviews also disclosed that access and monitoring controls were not always in place to prevent the loss or misuse of VA sensitive information. However, our FISMA work did not fully assess the management and control of sensitive VA data exchanged with and hosted at external organizations.

Appendix A provides a detailed description of our scope and methodology. Appendix B provides additional information on VA Research. Appendixes C and D provide management comments on a draft of this report.

RESULTS AND RECOMMENDATIONS

Finding

Management of Interconnections and Data Exchanged With Research and University Affiliates Needs Improvement

VA has not consistently managed its systems interconnections and data exchanges with its external research and university affiliates. Despite Federal requirements, VA could not readily account for the various systems linkages and sharing arrangements. VA also could not provide an accurate inventory of the research data exchanged, where data were hosted, or the sensitivity levels. In numerous instances, we identified unsecured electronic and hardcopy research data at VA Medical Centers and co-located research facilities.

VA's data governance approach has been ineffective to ensure that research data exchanged are adequately controlled and protected throughout the data life cycle. VA and its research partners have not consistently instituted formal agreements requiring that hosting facilities implement controls commensurate with VA standards for protecting the sensitive data. The responsible VHA program office's decentralized approach to research data collection and oversight at a local level has not been effective to safeguard the sensitive VA information. Because of these issues, VA data exchanged with its research partners were at risk of unauthorized access, loss, and disclosure.

Interconnections and Data Exchanges Not Readily Identified

VA could not provide an accurate inventory of the network interconnections and research data exchanged with external organizations. The National Institute for Standards and Technology (NIST) Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology systems that are owned and operated by different organizations. Implicit in this guidance is the requirement for an agency to accurately identify and inventory the network interconnections and data sharing arrangements in use.

Despite such requirements, VA could not accurately account for all its network interconnections with research partners. VA's Network Security Operations Center initially provided a listing of systems interconnections that we used to identify VAMC systems linkages for our testing. Local VAMCs provided systems interconnection documentation that identified many additional systems connections between VAMCs and research and university affiliates. However, discussions with VAMC Chief Information Officers and Information Security Officers, as well as with affiliate personnel, revealed that they were not fully aware of all systems linkages or sharing arrangements. For example, one university provided teleradiology services without formal documentation establishing the existence of the

network connection, authorizing the types of data exchanged, and defining appropriate information security roles and responsibilities. Another VAMC provided its research partners with commercial Internet access without agreements declaring its existence or authorizing the interconnection.

Historically, VAMCs have relied on dedicated network connections with research partners to facilitate data exchanges supporting healthcare services and cooperative research studies. However, over the past several years, VA has implemented "air-gapped"[1] network connections, when possible, to physically separate VAMC and research partner networks and reduce unauthorized exchanges of sensitive research data. While intended to limit direct system interconnections, the "air-gap" approach has increased the use of portable data storage devices to exchange data with external partners often lacking proper authorization. We saw research data hosted in a highly decentralized manner, located in various network environments, and exchanged using a range of unsecured external media sources, as described below.

- **Internal and external hard drives** – At two facilities, we identified unsecured computer storage drives hosting historical VA Research data. While investigators used external media to store research data, management could not readily provide an explanation of the specific data stored on the media.
- **Compact Discs (CDs), Digital Video Discs (DVDs), and Computer Diskettes** – At several facilities, we identified unsecured storage media used to host historical VA research data. Management could not readily provide an explanation of the specific data stored on the media.
- **Flash drives** – At most facilities we visited, VA Research personnel used unencrypted flash drives to store various types of data. Such devices can be easily used to transfer sensitive VA Research data.

The use of the above removable unencrypted storage devices to store sensitive VA data is prohibited per VA Handbook 6500, *Information Security Program*. This prohibition is reiterated in VA's annual mandatory training, *VA Privacy and Information Security Awareness and Rules of Behavior*. At several VAMCs, research data were also stored and transferred to research partners in hardcopy media, such as computer printouts or consent forms documenting veterans' willingness to participate in VA research studies.

VA and research partners also could not adequately account for all of the research data elements—typically sensitive medical and patient information—collected and exchanged with affiliates. Such electronic and

[1] An "air-gap" is a measure often taken to ensure that secure computers and computer networks are completely physically and electronically isolated from insecure networks, such as the public Internet or an insecure local area network. The only connection between two devices or networks may be via a person switching to different types of media, such as compact discs or flash drives, to transfer data.

hard copy data sometimes contained PII and protected health information that needed to be accounted for and safeguarded. The sensitive information was intended to support various veterans research studies related to traumatic brain and spinal cord injuries, exposure to hazardous agents, post-traumatic stress disorder, mental illness, prosthetics and robotic-assistance, women's health priorities, chronic disease, aging, pain, vision and hearing loss, and homelessness.

NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, states that organizations should identify all of their PII and minimize its use, collection, and retention to what is strictly necessary to accomplish their business purposes and missions. Implicit in this guidance is the need to catalogue sensitive data, periodically review current holdings of PII, and ensure the data are accurate, relevant, timely, and complete.

VAMCs provided us with a listing of active and inactive research studies. However, VAMCs or research partners could not accurately identify all types of data collected to support the research studies, where the data were hosted, how many copies existed, and specific data retention requirements. They also could not define what data elements were collected for which research studies.

Sensitive Data And Media Not Protected at Hosting Facilities

Hosting facilities did not always adequately protect the sensitive data VA shared with them. VA Handbook 6500 establishes VA requirements to protect the confidentiality, integrity, and availability of the information (electronic and hardcopy) created, processed, stored, aggregated, and transmitted. VA employees, as well as the contractors, volunteers, and students supporting them, are required to protect electronic media and hardcopy information by keeping it in locked files or cabinets when not in use. They are also required to dispose of sensitive VA information through shredding or other approved disposal methods.

Despite these data management requirements, we found unsecured electronic research data on computers, and other media and hardcopy research data lying about at eight VAMCs and co-located research facilities we visited. This electronic and hardcopy data sometimes contained unauthorized information and PII such as veteran names, social security numbers, dates of birth, and protected health information that could be linked to individual veterans. Some of the information was old, dating back to the 1980s, and appeared to have been sitting unsecured for a while. Examples of the unsecured research data included the following:

- At two VAMCs, we found portable hard drives containing sensitive VA data stored in unlocked research office desks.

- At one VAMC, within the office space of a researcher no longer on staff, we observed a large assortment of unsecured electronic media and hardcopy data containing sensitive veterans' information.
- In research space that stored old lab equipment and supplies at another VAMC, we discovered hardcopy PII in an open file cabinet and lying on top of a desk covered with dust.
- At several VAMCs, we observed unlabeled hardcopy research data inside unlocked cabinets and desks in co-located research labs and offices.

These security deficiencies were problematic because research areas were shared spaces, used at times by a mix of VAMC staff, research partners, and study participants who could readily access the unsecured data. Additionally, VAMCs and their research partners shared network infrastructures that were not fully separated, with unlabeled VA and affiliate network connections (i.e., wall jacks) right next to each other within VAMC research labs. This could allow someone to physically switch any computer from connecting to one wall jack to another and thereby transfer sensitive VA data onto research partner resources. VAMC janitorial staff and volunteers could potentially access these research spaces as well.

Figures 1 and 2 provide images of electronic and hardcopy veterans research data we found unsecured at VAMC research areas we visited.

Figure 1

Images of Unsecured Veteran Research Data - Electronic Media

Source: VA OIG images taken during VAMC site visits.

The images above depict various types of uncontrolled electronic media that research investigators used to store sensitive VA research data. We found such media stored or lying about in unsecured locations during our site visits to research facilities.

Figure 2

Images of Unsecured Veterans Research Data - Hardcopy

Source: VA OIG images taken at VAMCs during our audit.

These images provide examples of file cabinets used to store sensitive VA research data. The image on the left was taken in unlocked and unattended VA research office space at one VAMC. The image on the right was taken at an unoccupied area within another VAMC. The unlocked and unattended storage cabinets could be accessed by both facility staff and volunteers.

Causes for Unsecure Data Exchanges and Collections

VA's data governance approach was ineffective in accounting for the systems linkages and data sharing arrangements with research partners, and ensuring that the data collected and exchanged were adequately protected throughout the data life cycle. Specifically,

- VAMCs and their research partners did not always have formal agreements in place to authorize systems interconnections or require information security controls at hosting facilities commensurate with VA requirements. Table 1 summarizes the deficiencies with formal security agreements at the ten VAMCs we visited. VA did not implement adequate oversight to ensure formal security agreements were in place.
- VA Research's decentralized approach to research data oversight and collection also was not effective to safeguard sensitive VA information. This approach did not result in coordinated, consistent measures across VA and research partner organizations to ensure accurate inventory and protection of the research data exchanged.

Inadequate Sharing Agreements

VAMCs and their research partners did not always have formal interconnection agreements in place to authorize systems interconnections or require information security controls commensurate with VA standards at hosting facilities. VAMC Chief Information Officers and Information Security Officers, in coordination with their research partners, approve and implement information systems interconnection agreements. VA Handbook 6500, Appendix D, *Minimum Security Controls for VA Information Systems*, provides the methodology for system owners to use in documenting systems support and interconnectivity agreements in accordance with the previously mentioned NIST Special Publication 800-47.

According to the guidance, Memoranda of Understanding and Interconnection Security Agreements (MOUs/ISAs) are needed to authorize each systems interconnection, and define information security requirements, the network architecture, the types of data exchanged, and the appropriate roles and responsibilities. Systems owners should formally authorize each VA information system connection to external systems and monitor the connections on an ongoing basis. Further, Office of Management and Budget Memorandum M-11-33, *FY 2011 Reporting Instructions for FISMA and Agency Privacy Management*, states Federal agency information security programs apply to all organizations or sources that possess or use Federal information. As such, VA's research partners are required to safeguard the sensitive VA data they collect in accordance with VA standards.

Consistently established MOUs/ISAs provide VA with the means to ensure that hosting facilities institute information security controls commensurate with VA standards. Accordingly, VA MOUs/ISAs should state the terms and conditions for sharing data and information resources, specify the technical and security requirements for each connection, and be formalized prior to any systems interconnections and sensitive data sharing activities. Further, the MOUs/ISAs should detail the rules of behavior that organizations must abide by in using the interconnected systems.

Despite these requirements, we identified two universities providing teleradiology services for which MOUs/ISAs were not in place or documentation did not accurately reflect the network architecture. Teleradiology services involve electronically transmitting radiographic patient images, such as X-rays and patient information, from one location to another for the purposes of interpretation and/or consultation with radiologists. In providing these teleradiology services, unencrypted patient images and sensitive information were transmitted from VA to university systems for clinical and research purposes. In another example, a VAMC provided commercial Internet access for its research partner without an MOU/ISA authorizing the interconnection. As such, neither the VAMC nor the research partner had a means of ensuring the sensitive data hosted would be appropriately protected outside of VA networks.

Where MOUs/ISAs were in place, they did not always provide sufficient details on the specific data sharing agreements or information security requirements commensurate with VA information security standards. Some VAMCs recently developed or updated their MOUs/ISAs in preparation for our site visits, but those documents still included "template" language and did not specify the information security controls that would be implemented to meet VA requirements. At seven of the ten VAMCs reviewed, the MOUs/ISAs also contained general statements that did not provide responsible parties with a clear understanding of the data being exchanged and how the interconnections would be controlled, protected, and maintained. Additionally, some MOUs/ISAs did not clearly define how

VAMC and research partner personnel would perform internal security reviews and monitor research environments for unauthorized access.

Because MOUs/ISAs were lacking specific information security requirements, VA could not hold its research partners accountable for not implementing and enforcing access and monitoring controls commensurate with VA requirements across their facilities. Specifically, research and university partners had not implemented:

- **Local Port Security Controls** – Port security software could prevent the unauthorized use of unencrypted flash drives and CD/DVD writers to transfer research data. Also, disabling the data copying function in using the software could make it difficult to transport sensitive information outside of VAMCs.
- **Network Port Security Controls** – Filtering controls could be used to restrict network connections through port security. Users would not be able to connect unauthorized equipment to the networks or access sensitive information if this control were properly implemented.
- **Network Monitoring Controls** – Monitoring networks for malicious access is critical to detect and respond to intrusion attempts in a timely manner. This control also would allow organizations to identify and react to threats that could undermine the protection of sensitive information.
- **Whole Disk Encryption Controls** – Use of whole disk encryption is critical for protecting sensitive data from unauthorized disclosure due to lost or stolen laptops or mobile devices. When utilizing hardware encryption, research partners should comply with Federal Information Processing Standards, *Security Requirements for Cryptographic Modules*, to protect VA's sensitive information stored on portable computer devices.

Table 1 provides a summary of MOU/ISA deficiencies at the ten VAMCs we visited, demonstrating that VA had not implemented controls to ensure that system interconnections were appropriately authorized and monitored.

Table 1

MOU/ISA Deficiencies at the VAMCs Reviewed by OIG

VAMC	Location	MOUs/ISAs Needed to be Established	MOUs/ISAs Needed to be Updated	Total Deficiencies
Michael E. Debakey	Houston, TX	1	1	**2**
VA Palo Alto Healthcare System	Palo Alto, CA		2	**2**
Portland	Portland, OR	1	1	**2**
North Florida South Georgia Veterans Healthcare System	Gainesville, FL	2		**2**
VA Connecticut Healthcare System	West Haven, CT		1	**1**
Richard L. Roudebush	Indianapolis, IN	1	3	**4**
Louis Stokes Cleveland	Cleveland, OH		2	**2**
Edward Hines Jr.	Hines, IL		1	**1**
VA Pittsburgh Healthcare System	Pittsburgh, PA	1		**1**
James J. Peters	Bronx, NY	1		**1**
Totals		**7**	**11**	**18**

Source: VA OIG analysis of VAMC data.

In March 2012, VA launched the Continuous Readiness in Information Security Program, providing further guidance that external connections, such as those with research and university affiliates, must be approved and documented with MOUs/ISAs. The VA Secretary stated that the program

would provide a three-pronged approach to improve the way the Department looks at information security. First, the program would help ensure that personnel accessing VA systems would have the appropriate levels of access. Second, the program would help establish clear, documented contingency plans for data breaches. These contingency plans would be regularly tested and improved. Lastly, the program would provide accessible, tailored, online information security training for all VA employees, volunteers, contractors, and partners. The program would use an integrated approach to protect sensitive information from inappropriate exposure or loss. VA's senior leadership emphasized that securing information was everyone's responsibility and that this theme would be interwoven into the fabric of normal operations across VA.

Decentralized Approach to Data Collection and Oversight

The Office of Research and Development's (VA Research) decentralized approach to research data oversight and collection was not effective in safeguarding sensitive VA information. Within VHA, this office was responsible for not only leading the research and studies to provide medical advancements in veterans healthcare, but also for defining policy to ensure protection of the sensitive VA data collected and shared to accomplish these medical advancements. While VA Research provided high-level oversight of VA research activities, it relied on individual Institutional Review Boards (IRBs) at the local level to review research studies for compliance with Federal regulations on a facility-by-facility basis.

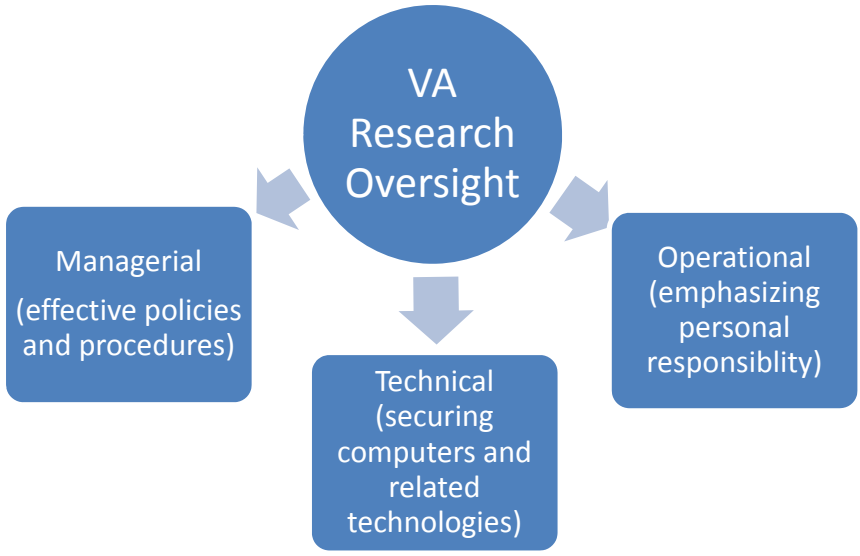
Research Data Oversight

VA Research had implemented a national security oversight program comprised of three elements—managerial, technical, and operational controls. The managerial element included establishing and updating information security policies, directives, and research protocols. The technical element involved upgrading software and equipment to prevent unauthorized access to sensitive data. Finally, the operational element entailed establishing enhanced training programs to educate employees about information security requirements.

Figure 3 provides a depiction of VA Research's oversight process. In this context, VA Research conducted reviews of research protocols to ensure compliance with Federal regulations. More specifically, VA Research periodically evaluated its data collection standards and practices to ensure uniform implementation of security and privacy protections across all research studies. Such reviews were critical to provide assurance that research studies were conducted at the appropriate level of security risk. VA Research also had an Office of Research Oversight, which conducted independent reviews of research studies apart from the process above. These independent reviews were to provide additional assurance that VA facilities were complying with Federal and VA research requirements.

Figure 3

National Security Program for VA Research Oversight



Source: VA OIG-developed based on VHA Office of Research and Development information.

Data Collection

VA Research relied on IRBs at individual VAMCs and academic institutions to oversee inventories of the data collected, and monitor data age and history, where the data were stored, and details on their ultimate destruction. IRBs were formally organized groups designated to review, approve, and conduct oversight of human subject research to ensure compliance with Federal and research regulations. Each IRB was comprised of a board, committee, or other group consisting of VA and/or affiliate research personnel formally designated by the VAMCs conducting research.

IRBs were intended to locally ensure the data collected complied with protocol plans for conducting research investigations, including biomedical, behavioral, social, health service, and educational research, as well clinical trials. IRBs were to review and approve research protocols before a research study could commence. As part of approving research protocols, IRBs had to consider many factors, including minimization of risks, equitable selection of subjects, informed consent, safety monitoring, privacy and confidentiality, information security, vulnerable subjects, conflicts of interest, and research personnel qualifications.

IRBs were specifically charged with ensuring that the data collected met information security requirements, including the following:

- Reviewing and approving creation of research data repositories.

- Reviewing research activities at least once a year to ensure that only appropriate data were collected to meet established needs.
- Maintaining information on research data storage, usage, and security requirements.
- Maintaining information on the mechanisms for copying or transporting data from secure VA servers to other locations.

Concerns with Decentralized Data Governance

We found that this oversight structure, comprised of high-level VA Research oversight and local IRB monitoring, was functioning as intended to carry out the responsibilities outlined above. However, the structure did not promote the coordinated activity needed to adequately safeguard sensitive VA research data at hosting facilities. Specifically, the structure did not ensure that local IRBs, VA Information Security Officers, and research partners worked together as needed to actively monitor VA research areas for the types of data collected, where the data were stored, and whether data security practices complied with information security requirements and research protocols.

For example, only one of ten VAMCs we visited had collaborated with its research partners to conduct joint walkthroughs of research labs and offices. Such walk-throughs are essential oversight mechanisms for identifying unsecured sensitive data and other instances of non-compliance with VA information security requirements. The remaining nine VAMCs typically left it to the local IRBs to conduct such walk-throughs. Consequently, research personnel had to individually determine data management and information security requirements in their local environments, which did not provide for consistent data security protections and practices across the enterprise.

IRB members communicated a number of concerns with this decentralized data management model. A number of the members advocated a more centralized approach. Specifically, IRB members suggested that VA implement the following improvements:

- Create a centralized storage solution that would enable sharing of electronic research data across VAMCs. OIT and VA Research could partner to develop a central database for hosting the research data.
- Provide increased awareness of requirements for physically securing sensitive veterans data in files, cabinets, or desks. OIT and VA Research could partner to develop more comprehensive training programs to clarify applicable information security requirements.

The concerns shared and the unsecured electronic and hardcopy research data we observed both underscored VA's need to implement a centralized data governance model to effectively manage and protect sensitive research data throughout their life cycle.

Benefits of Centralized Data Governance

Leading Federal and industry sources also have proposed a more centralized model for governing sensitive data throughout the data life cycle. Specifically, a VA and National Institutes of Health collaborative report, *Working Group on Information Technology Security and Privacy in VA and National Institutes of Health-Sponsored Research,* November 2010, discusses elements of effective data governance. National Science Foundation representatives similarly believe that a centralized data management model is an integral component of research data governance and that such a model should describe how the data will be authored, managed, and made accessible throughout the data life cycle.

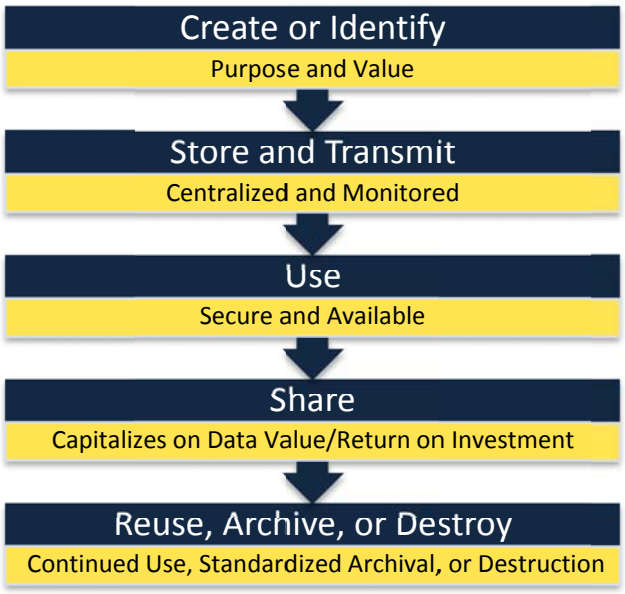
Federal and industry sources emphasize that effective data governance should provide centralized policies, procedures, and resources to effectively identify important data and securely manage them, from creation through retention or destruction, across an organization. As part of the data life cycle, data should be accounted for upon creation by identifying their purpose and value. Data should then be stored, monitored, and transmitted in a centralized manner that fully accounts for their disposition at each phase of existence. Further, data must be available, and their use and sharing safeguarded, depending upon the intended purpose, value of the information, and organizational information security policies.

The benefits of centralized data governance can be seen in an organization's improved ability to share data across the enterprise and with trusted research partners. Centralized data governance is particularly important for safeguarding unique human data that cannot be easily reproduced, but can allow researchers to readily translate research results into knowledge, products, and procedures for improved healthcare. At the end of their life cycle, data may be re-used, archived for future use, or destroyed as appropriate.

Figure 4 depicts the life cycle for centralized management of research data. Implementing a centralized data governance and storage model at VA would facilitate the sharing of research data across the organization and with trusted research partners to enhance mission accomplishment. OIT and VHA could partner to define appropriate data storage requirements and develop a centralized storage model that would alleviate the need to store sensitive research data on locally hosted computer systems, portable hard drives, CDs, DVDs, flash drives, and other uncontrolled media. Without centralized data governance, VA Research personnel will continue to use unsecure methods to collect and store research data.

Figure 4

Common Data Life Cycle Attributes as Part of Data Governance



Source: VA OIG-developed based on VA, National Institutes of Health, and National Science Foundation reports.

Effects of Information Security Deficiencies

VA's decentralized method of sharing sensitive veterans' data with research and university partners has left such data vulnerable to potential unauthorized access, loss, or disclosure. Without inventories of the network interconnections and the data exchanged, the data may be proliferated and shared with unintended recipients, without awareness to VA or the study participants. Controls over the data may be lost and PII or protected health information could be compromised. Where VAMCs and their research partners share network infrastructures that are not fully separated within VAMC research labs, someone could physically switch computer connections from one network port to another and easily transfer sensitive VA data onto research partner resources.

Further, the unsecure practice of transferring, collecting, or storing sensitive research data on locally hosted computer systems, portable hard drives, CDs, DVDs, flash drives, and other uncontrolled media has made the data highly portable and easy to divert to unknown recipients. Electronic media and hard copy data left unsecured at affiliate locations may be left open to compromise, theft, misplacement, or transfer by individuals such as research staff, volunteers, participants, or janitorial staff without authorization.

The opportunities for fraudulent use of the unsecured sensitive data in such an environment may pose high risks. For example, recent media reports have noted increases in data breaches and related to identity theft at hospitals that have not kept pace with new technologies and have not provided

adequate security for mobile communication devices. Within the VAMCs, research data, including PII, could be obtained from various sources and used to perpetrate various types of fraud, including tax fraud. To illustrate, the Treasury Inspector General for Tax Administration informed Congress in April 2012 that fraudulent returns involving identity theft totaled $6.5 billion in 2011.[2]

The ultimate consequence of inadequately managed data may be loss of trust by veterans and other study participants who may no longer want to take part in VA research studies for fear of becoming victims of identity theft. VA acknowledges that while patients are willing to participate in research studies, they may do so only do so with assurances that their sensitive personal or medical data will be duly safeguarded. Reduced volunteer participation in research studies because of inadequate data security could hinder or potentially slow advancements in medical science intended to save or extend lives, improve health, and enhance the quality of life for patients.

VA leadership recognizes it must improve its data security to maintain the trust of its veterans. Two previous VA Secretaries testified before Congress regarding their commitment to make the Department the "Gold Standard" in data security within the Federal government. They asserted that VA must be the best in the Federal government in protecting personal and health information, training and educating employees to achieve that goal, and providing a culture that puts the custody of veterans' personal information first. Similarly, in announcing VA's Continuous Readiness in Information Security Program in March 2012, the VA Secretary stated that the trust veterans have in the Department depends on VA's ability to constantly and consistently protect its information from exposure and ever-increasing cyber threats. The Secretary stated that veterans have suffered the consequences of careless information security practices in the past, including unintended loss of PII, and VA can, and must, do better.

Conclusion

Beyond its fundamental mission of providing benefits and services, VA has the opportunity to further serve veterans by supplying the patient and medical data needed to achieve advancements in medical research and healthcare services. However, providing such sensitive data through electronic or hard copy means without effective information security controls and oversight has left the data susceptible to unauthorized access, loss, or disclosure. Leaving hosting facilities responsible for data governance at the local level without coordinated involvement of all stakeholders has proven ineffective and improvements are needed.

Consistently establishing MOUs/ISAs is one means of documenting data sharing agreements and ensuring that hosting facilities institute information

[2] "Problems at the Internal Revenue Service: Closing the Tax Gap and Preventing Identity Theft," Testimony of the Honorable J. Russell George, Treasury Inspector General for Tax Administration before the Committee on Oversight and Government Reform, Subcommittee on Government Organization, Efficiency, and Financial Management, U.S. House of Representatives, April 19, 2012.

security controls commensurate with VA standards. Further, as industry leaders suggest, a centralized data governance and storage approach would ensure researchers effectively control and securely manage sensitive VA research information over the data life cycle. Such measures are key to protect veterans' PII and personal health information and promote continued advancements in medical research now and for the future.

Recommendations

1. We recommend the Assistant Secretary for Information and Technology establish or update all Memoranda of Understanding and Interconnection Security Agreements needed to accurately reflect operational environments and require that research partners implement information security controls commensurate with VA's information security standards.

2. We recommend the Assistant Secretary for Information and Technology support the Under Secretary for Health by providing the information technology infrastructure needed to implement a centralized data governance and storage model to securely manage research information over the data life cycle.

3. We recommend the Assistant Secretary for Information and Technology direct Information Security Officers to partner with the Veterans Health Administration's Institutional Review Boards, research personnel, and research partners to routinely conduct joint oversight and monitoring of research labs to ensure security of sensitive veterans' data, compliance of data collections with research protocols, and fulfillment of the Department's information security requirements.

4. We recommend the Under Secretary for Health develop and implement a centralized data governance and storage model that ensures accurate inventory of all research data collected, data collection compliance with research protocols, and secure management of research information over the data life cycle.

5. We recommend the Under Secretary for Health require the Office of Research and Development to partner with Information Security Officers to routinely conduct joint oversight and monitoring of research labs to ensure security of sensitive veterans' data, compliance of data collections with research protocols, and fulfillment of the Department's information security requirements.

Management Comments

The Assistant Secretary for Information and Technology generally concurred with our findings and recommendations. The Assistant Secretary stated interconnections and data exchange agreements between VA and research partners would be updated and implemented along with related guidance. OIT will evaluate and continuously monitor these agreements and data

exchanges as part of their Continuous Readiness in Information Security Program. The Assistant Secretary also stated OIT would support VHA by providing the information technology infrastructure needed to implement a centralized data governance and storage model, but noted VHA's concerns with this centralized approach. Finally, OIT will participate with local VHA Institutional Review Boards and research staff on providing oversight of VA Research labs.

The Under Secretary for Health generally concurred with our findings and recommendations. VHA had concerns about the feasibility of implementing a centralized data governance and storage model to securely manage research information over the data life cycle. Accordingly, VHA proposed as an alternative solution forming a workgroup with OIT to standardize processes and procedures for data collection and security between VA Medical Centers and affiliated academic partners. The Under Secretary also stated that it is extremely important for OIT to support VHA and develop an action plan for providing joint oversight of VA Research labs that meets the needs of each organization and ensures the protection of sensitive information. Finally, VHA's Office of Research Oversight will collaborate with OIT on inspections of VA Research labs to identify information security deficiencies.

OIG Response Management's comments and corrective action plans are responsive to the recommendations. We believe VHA's proposed solution of working with OIT to standardize processes on data collection and security will result in corrective actions that will satisfy the intent of our recommendation. Accordingly, such actions could ensure an accurate inventory of all research data collected, data collection compliance with research protocols, and secure management of research information over the data life cycle. We will follow up as required on all actions.

Appendix A Scope and Methodology

Scope

We conducted our audit work from April 2011 through August 2012. To accomplish our audit objectives, we conducted field work at selected VAMCs that had active partnerships and systems interconnections with research and university partners. At the VAMCs, we evaluated VA oversight of the systems interconnections and assessed whether appropriate agreements were in place to define and enforce applicable information security procedures and practices. We did not evaluate network connections that exchanged financial and patient-related data within VA networks. When judgmentally selecting VAMCs for testing, we considered the geographic region, size, complexity, and number of systems interconnections with external organizations. We evaluated systems interconnection controls at the following locations:

Table 2

OIG Site Visits		
VA Medical Facility	**Location**	**Research Partners**
Michael E. Debakey	Houston, TX	Baylor College of Medicine
VA Palo Alto Healthcare System	Palo Alto, CA	Stanford School of Medicine
Portland	Portland, OR	Oregon Health and Science University
North Florida South Georgia Veterans Healthcare System	Gainesville, FL	University of Florida College of Medicine
VA Connecticut Healthcare System	West Haven, CT	Yale University, Yale-New Haven Hospital
Richard L. Roudebush	Indianapolis, IN	Indiana University School of Medicine
Louis Stokes Cleveland	Cleveland, OH	University Hospitals Cleveland, Case Western Reserve University School of Medicine
Edward Hines Jr.	Hines, IL	Loyola University Health System
VA Pittsburgh Healthcare System	Pittsburgh, PA	University of Pittsburgh, University of Pittsburgh Medical Center
James J. Peters	Bronx, NY	Mount Sinai School of Medicine

Source: VA OIG-developed based on VAMC data.

Methodology

To accomplish the audit, we examined the nature, type, and volume of research information collected. We interviewed OIT and VHA staff to gain an understanding of the types of sensitive data collected and the controls for protecting such data. In addition, we observed research labs at all VAMCs visited to evaluate security controls governing electronic and hardcopy data exchanges with external organizations.

We researched applicable VA directives, handbooks, and Federal information security requirements, and identified relevant business practices and information security controls. Federal agencies are governed by the *Federal Information Security Management Act* (FISMA), Public Law 107-347. FISMA requires each Federal agency to develop and implement an agency-wide security program that will ensure security controls adequately protect information resources. FISMA applies to all organizations or sources that possess or use Federal information. Further, the *Health Insurance Portability and Accountability Act of 1996* identifies security and privacy requirements for protecting electronic health information, with a focus on data and the information technology environment. This Act specifically directs that healthcare information be protected at all times, regardless of whether the data are transmitted to or stored at a hosting facility.

Data Reliability

We used computer-processed data, such as systems interconnection reports provided by VA's Network Security Operations Center to identify VAMCs for testing. To test for reliability, we compared this data with VA Web site information and discussed the data accuracy with VA personnel. As we noted in this report, VA did not accurately identify all network interconnections at VAMCs. Thus, we report the lack of complete information as a finding in this report.

Government Audit Standards

Our assessment of internal controls focused on those controls relating to our audit objectives. We conducted this performance audit in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B Background

Additional Information on VA Research

The Secretary has stated that VA's forward-looking contributions to medical research will continue to bring life-improving treatment to our veterans and our Nation. The Secretary is committed to VA research playing an integral part in transforming the Department into a 21st century organization. With one of the country's largest integrated healthcare systems and a vast patient population, VA is uniquely positioned to conduct pioneering research. VA believes its research is a valuable investment with remarkable and lasting returns.

Historically, VA, the National Institutes of Health, and academic institutions have collaboratively conducted research studies to improve the lives of many Americans. VA has also partnered with nonprofit organizations and other agencies to leverage resources and expand the potential effectiveness of Federal research. Within VHA, VA Research has contributed to numerous advancements in healthcare currently in use today. For example, VA Research studies have led to advancements in implantable cardiac pacemakers, computerized tomography scans, high-performance artificial limbs, nicotine patches, and liver transplants. A recent Association of American Medical Colleges report states that VA's collaborative research with other organizations has reduced deaths due to stroke and heart disease caused by hypertension. These research organizations have also developed laboratory diagnostics used in nearly every medical laboratory in the Nation, improved cancer treatment, and improved care for individuals afflicted with hundreds of medical conditions.

With access to electronic medical data and a large research population, VA Research is renowned for conducting large-scale clinical trials and comparative effectiveness research studies. VA Research's focus areas include healthcare concerns for veterans returning from Operation Enduring Freedom and Operation Iraqi Freedom. VA Research studies traumatic brain and spinal cord injuries, prosthetics, pain, vision and hearing loss, and post-traumatic stress disorder—issues typically faced by recently returning veterans.

Sharing of PII and personal health information is instrumental to ensuring success of continued studies and further advancements in medical research. As such, effective information security practices are critical for protecting this research data, particularly among VA and its research partners. If not controlled, the numerous system interconnections and data exchanges supporting VA Research partnerships may place sensitive VA data, including PII, at risk of unauthorized use and disclosure.

Appendix C Assistant Secretary for Information and Technology Comments

Department of Veterans Affairs

Memorandum

Date: September 28, 2012

From: Assistant Secretary for Information and Technology (005)

Subj: OIG Draft Report: Audit of VA's Systems Interconnections With Research and University Affiliates

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

Thank you for the opportunity to review the subject draft OIG report. The Office of Information Technology submits the attached written comments for each recommendation. We appreciate your time and attention to our information security program. If you have any questions, contact my office.

Attachment

Office of Information Technology
Comments to Draft OIG Report,
"Audit of VA's Systems Interconnections With Research and University Affiliates"

Recommendation 1: We recommend the Assistant Secretary for Information and Technology establish or update all Memoranda of Understanding and Interconnection Security Agreements needed to accurately reflect operational environments and require that research partners implement information security controls commensurate with VA's information security standards.

OIT Response: Concur. The Office of Information Technology (OIT) has updated its Memoranda of Understanding (MOU)/Interconnection Security Agreement (ISA) templates which are used to document system interconnections. MOU/ISAs for seven external connections have already been updated and OIT, in conjunction with the Veterans Health Administration (VHA), will ensure that all known connections have current MOU/ISAs which reflect the operational environment. In addition, VA has identified three air gapped connections. Field guidance is to be published by OIT on documenting air-gapped connections with an MOU only. Once this guidance is published, OIT will document all known air-gapped connections. OIT will work with VHA to ensure the documentation of all known connections is completed and issue field guidance related to the documentation of air-gapped networks by October 15, 2012. OIT will document all air-gapped connections by October 31, 2012.

VA Handbook 6500, Information Security Program, paragraphs 2a and 2b, already require the following:

2. Scope:

a. The security policies, procedures, and controls in this handbook apply to all VA employees, contractors, researchers, students, volunteers, representatives of Federal, State, local, or Tribal agencies, and all others authorized access to VA facilities, information systems, or information in order to perform an authorized activity.

b. The requirements in this handbook and appendices apply to all VA or contractor operated services and information resources located and operated at contractor facilities, at other government agencies that support VA mission requirements, or other third party utilizing VA information in order to perform an authorized VA activity.

However, when an Informed Consent Document and Health Insurance Portability and Accountability Act (HIPAA) authorization has been signed, the above mentioned levels of control does not apply to the information that is transferred and disclosed to another party. This authorization states that the protection of this data is now the responsibility of another entity and would fall under those entities' policies.

VA's Enterprise Security Change Control Board (ESCCB) has established external (university) connections through the Trusted Internet Connection (TIC). Enforcement becomes the responsibility of the facility Chief Information Officer with oversight by the cognizant information security officer and VA's Network Security Operations Center. The connection is required to be documented in an ISA/MOU and is included as part of the system security plan

for the supporting Local Area Network (LAN). The security implications of the connection are evaluated by OIT prior to granting authority for the LAN to operate on the VA network. This evaluation is conducted as part of the Assessment and Authorization (A&A) for the LAN. Authorities for VA systems to operate are granted consistent with VA's continuous monitoring capability.

As part of its Continuous Readiness in Information Security (CRISP) Program, VA emphasized its commitment to protect its system and data from unauthorized access and use which included the requirement to document, evaluate, and approve external connections to the VA network.

Recommendation 2: We recommend the Assistant Secretary for Information and Technology support the Under Secretary for Health by providing the information technology infrastructure needed to implement a centralized data governance and storage model to securely manage research information over the data life cycle.

OIT Response: Concur. OIT agrees to support the Under Secretary for Health by providing the information technology infrastructure needed to implement a centralized data governance and storage model to securely management research information over the data life cycle subject to the budget prioritization process of the Information Technology Leadership Board (ITLB). However, VHA has indicated that they will need to determine whether the use of a centralized data governance and research data storage model is feasible and whether the benefit to be gained by such a system is appropriate to the level of resourcing required to develop, implement, and manage it over time. See comments in the VHA response to Recommendation 4 for more detail.

Recommendation 3: We recommend the Assistant Secretary for Information and Technology direct Information Security Officers to partner with the Veterans Health Administration's Institutional Review Boards, research personnel, and research partners to routinely conduct joint oversight and monitoring of research labs to ensure security of sensitive veterans data, compliance of data collections with research protocols, and fulfillment of the Department's information security requirements.

OIT Response: Information Security Officers (ISOs) will be directed to participate, rather than partner, with local VHA Institutional Review Boards and research staff on periodic reviews of research labs to ensure that VA information security requirements are met. However, these reviews will be performed subject to ISO availability. Target date(s) for performance of these reviews are to be determined.

VHA has concerns about ISOs partnering with VHA Institutional Review Boards (IRB) in the context of the intent of the Federal Policy for the Protection of Human Subjects (usually referenced as the Common Rule). Currently, ISOs participate as non-voting members of IRBs to assist IRBs in their oversight responsibilities.

These reviews will be led by the local VHA Research Compliance Officer with support from the cognizant ISO and VHA Privacy Officer. Also, the VHA Office of Research Oversight (ORO) was established by statute to ensure that VA research meets regulatory requirements. In that context ORO and OIT officials have in the past collaborated on inspections of VA research space to identify information security deficiencies. This will continue. The local RCO and ORO have the authority to enforce compliance.

The Assistant Secretary for Information and Technology and the Under Secretary for Health will collaborate to develop an action plan that meets the needs of both OIT and the VHA including the need for Veterans Integrated Service Network and VA Medical Center leadership and officials to retain their abilities to exercise appropriate local authorities and responsibilities.

VHA and OIT will collaborate about establishing guidelines for participation of ISOs in IRB activities in accordance with the Common Rule. Target date for establishment of these guidelines is to be determined.

Recommendation 4: We recommend the Under Secretary for Health develop and implement a centralized data governance and storage model that ensures accurate inventory of all research data collected, data collection compliance with research protocols, and secure management of research information over the data life cycle.

OIT Response: Defer to VHA.

Recommendation 5: We recommend the Under Secretary for Health require the Office of Research and Development to partner with Information Security Officers to routinely conduct joint oversight and monitoring of research labs to ensure security of sensitive veterans data, compliance of data collections with research protocols, and fulfillment of the Department's information security requirements.

OIT Response: Defer to VHA.

Appendix D Under Secretary for Health Comments

Department of Veterans Affairs

Memorandum

Date: October 3, 2012

From: Under Secretary for Health (10)

Subj: OIG Draft Report, Department of Veterans Affairs: Audit of VA's Systems Interconnections With Research and University Affiliates

To: Director, Information Technology Security Audits (52CT)

1. Veterans Health Administration (VHA) officials have reviewed the draft report and collaborated with officials from the Office of the Assistant Secretary of the Department of Veterans Affairs (VA) Office of Information Technology (OIT) in the examination and analysis of the findings and recommendations.

2. I have also reviewed the report and have comments regarding recommendations made directly to VHA as well as findings and recommendations addressed to VA OIT.

3. VHA agrees with the recommendation that Memoranda of Understanding and Interconnection Security Agreements be updated. VHA also agrees with the recommendation that research partners implement security controls that achieve levels of security appropriate for this information with the caveat that VHA only has authority to require security standards for data that is still owned or controlled by VHA. It is important to note that the VHA understanding is that VA will lack authority to require these levels of control if information has been transferred and disclosed to another party, including an academic affiliate, pursuant to an Informed Consent Document and Health Insurance Portability and Accountability Act (HIPAA) authorization purposely and correctly drafted to achieve that result. In these cases, VHA understands that information security controls would then be managed by the entity that receives the data. When VHA discloses its data pursuant to legal authorities other than an authorization signed by the subject of the data, VHA may enter into data use agreements (DUA) or other agreements that define security controls and confidentiality expectations that must be followed by the affiliate. In these instances VHA would expect that the affiliate meet the specific terms of the DUA or other agreement regarding security controls and privacy requirements.

4. While I agree that it is important to ensure an accurate inventory of all research data collected, data collection compliance with research protocols, and secure management of research information over the data life cycle, I do not agree with the specific recommendations to implement a centralized data governance and storage model to securely manage research information over the data life cycle. It is not yet

clear whether the use of a centralized data governance and research data storage model is feasible or appropriate; such a governance and management model would take considerable human and monetary resources, and a cost-benefit analysis has yet to be performed to determine whether the benefit to be gained by such a system is appropriate to the level of resourcing required to develop, implement, and manage it over time. The responses to Recommendation 2 and 4 provide an alternative solution.

This proposal is designed to codify standardized processes and procedures that individual VA Medical Centers (VAMC) and affiliated academic partners can use to conduct research and safeguard the security of VA data at VAMCs and affiliates. This process would involve internal discussions within VA as well as facilitate the interactions between VA and its academic affiliates about how data can be appropriately inventoried and managed throughout its life cycle. The attached action plan provides more detail about concerns with Recommendations 2 and 4.

5. I agree that it is extremely important that facility information security officers (ISO) with research expertise be readily available to support the research community in ensuring the protection of sensitive information. This will require VA OIT and VHA to develop an action plan that meets the needs of both the VA OIT and VHA, including the need for Veterans Integrated Service Network and VAMC leadership and officials to retain their abilities to exercise appropriate local authorities and responsibilities.

6. VHA has concerns about the part of Recommendation 3 that recommends ISOs partner with VHA Institutional Review Boards (IRB). In summary, ISOs currently participate as non-voting members of IRBs to assist IRBs with their oversight responsibilities. A more formalized partnership relationship is inadvisable because it would tend to undermine the independence of the IRB which is the primary responsibility of an IRB.

7. Also, the VHA Office of Research Oversight (ORO) was established by statute to ensure that VA research meets regulatory requirements. ORO and OIT officials have in the past collaborated on inspections of VA research space to identify information security deficiencies. VHA believes it is crucial to explore how best to increase collaborations between ORO and VA OIT.

8. Thank you for the opportunity to review the draft report. Attached is the complete action plan for the report's recommendations. If you have any questions, please contact my office.

Robert A. Petzel, M.D.

Attachment

Veterans Health Administration
Action Plan
OIG Draft Report, Department of Veterans Affairs: "Audit of VA's Systems Interconnections With Research and University Affiliates"

Recommendation 1: We recommend the Assistant Secretary for Information and Technology establish or update all Memoranda of Understanding and Interconnection Security Agreements needed to accurately reflect operational environments and require that research partners implement information security controls commensurate with VA's information security standards.

VHA Response:

VHA agrees with the Department of Veterans Affairs (VA) Office of Information Technology (OIT) concurrence. VHA provides additional comments.

VHA understands that:

- OIT has updated its Memoranda of Understanding (MOU)/Interconnection Security Agreement (ISA) templates which are used to document system interconnections.
- MOU/ISAs for seven external connections have already been updated and OIT, in conjunction with VHA, will ensure that all known connections have current MOU/ISAs which reflect the operational environment.
- OIT has identified three air gapped connections.
- Field guidance is to be published by OIT on documenting air-gapped connections with an MOU only.
- OIG will document all air-gapped connections by October 31, 2012.

Once this guidance is published, OIT has indicated that it will work with VHA to ensure the documentation of all known air-gapped connections is completed and issue field guidance related to the documentation of air-gapped networks.

VA Handbook 6500, Information Security Program, paragraphs 2a and 2b, already require the following:

2. Scope:

c. The security policies, procedures, and controls in this handbook apply to all VA employees, contractors, researchers, students, volunteers, representatives of Federal, State, local, or Tribal agencies, and all others authorized access to VA facilities, information systems, or information in order to perform an authorized activity.

d. The requirements in this handbook and appendices apply to all VA or contractor operated services and information resources located and operated at contractor facilities, at other government agencies that support VA mission requirements, or other third party utilizing VA information in order to perform an authorized VA activity.

However, when an Informed Consent Document and Health Insurance Portability and Accountability Act (HIPAA) authorization has been signed, VHA understands that these levels of control do not apply to the information that has been transferred and disclosed to another party, including an academic affiliate. This authorization states that the protection of these data is now the responsibility of another entity and would fall under those entities' policies. When VHA discloses its data pursuant to legal authorities other than an authorization signed by the subject of the data, VHA may enter into data use agreements (DUA) or other agreements that define security and confidentiality expectations that must be followed by an affiliate. In these instances VHA would expect that the affiliate meet the specific terms of the DUA or other agreement regarding security controls and privacy requirements.

VHA understands that VA's Enterprise Security Change Control Board (ESCCB) has established external (university) connections through the Trusted Internet Connection (TIC). Enforcement becomes the responsibility of the facility Chief Information Officer with oversight by the cognizant information security officer (ISO) and VA's Network Security Operations Center. The connection is required to be documented in an ISA/MOU and is included as part of the system security plan for the supporting Local Area Network (LAN). The security implications of the connection are evaluated by OIT prior to granting authority for the LAN to operate on the VA network. This evaluation is conducted as part of the Assessment and Authorization (A&A) for the LAN. Authorities for VA systems to operate are granted consistent with VA's continuous monitoring capability.

As part of its Continuous Readiness in Information Security (CRISP) Program, VHA emphasized its commitment to protect its system and data from unauthorized access and use which included the requirement to document, evaluate, and approve external connections to the VA network.

Recommendation 2: We recommend the Assistant Secretary for Information and Technology support the Under Secretary for Health by providing the information technology infrastructure needed to implement a centralized data governance and storage model to securely manage research information over the data life cycle.

VHA Response:

VHA agrees with VA OIT concurrence. VHA provides additional comments.

While VHA agrees that it is important to ensure an accurate inventory of all research data collected, data collection compliance with research protocols, and secure management of research information over the data life cycle, it is not clear to VHA whether the use of a centralized data governance and storage model is feasible or appropriate. Such a governance and management model would take considerable human and monetary resources. And a cost-benefit analysis has yet to be performed to determine whether the benefit to be gained by such a system is appropriate to the level of resourcing required to develop, implement, and manage it over time.

VHA's alternative action plan to address the recommendation is that VHA will convene a working group consisting of representatives from OIT and appropriate VHA leadership to meet with representatives of academic affiliates to be appointed by the Association of American

Medical Colleges (AAMC). A goal of the working group would be to develop a reference guide to facilitate the interactions between VA and its academic affiliates about how data can be appropriately inventoried and managed throughout its life cycle. The purpose would be to codify standardized processes and procedures that individual VA Medical Centers (VAMC) and affiliated academic partners can use to conduct research and safeguard the security of VA data at VAMCs and affiliates, as defined by VHA Directive 1200, Veterans Health Administration Research and Development Program.

This workgroup would also evaluate current efforts to centralize research data storage for analysis purposes through the VA Informatics and Computing Infrastructure (VINCI) to determine the costs and if this system could accomplish the intent of this recommendation. Currently, VHA is implementing the Research Administrative Management System (RAMS), so in addition it would be crucial for the workgroup to consider if and how completion of the RAMS implementation could facilitate efforts to address the Office of Inspector General's (OIG) recommendations.

It is important for the workgroup to consider the requirements of other Federal research agencies (e.g. National Institutes of Health, Department of Defense, Department of Energy, and National Science Foundation); Federal regulatory agencies (e.g., Food and Drug Administration) as well as the needs of VA and its academic affiliates. Recent Government Accountability Office (GAO) reports have emphasized the need to reduce duplication and overlap among research conducted by Federal agencies, so these concerns need to be reviewed and considered as well.

Recommendation 3: We recommend the Assistant Secretary for Information and Technology direct Information Security Officers to partner with the Veterans Health Administration's Institutional Review Boards, research personnel, and research partners to routinely conduct joint oversight and monitoring of research labs to ensure security of sensitive veterans data, compliance of data collections with research protocols, and fulfillment of the Department's information security requirements.

VHA Response:

VHA agrees with the VA OIT concurrence. VHA provides additional comments.

VHA agrees that it is important that facility ISOs with research expertise be readily available to support the research community in ensuring the protection of sensitive information. VHA and VA OIT will develop an action plan that meets the needs of both organizations, including the need for Veterans Integrated Service Network (VISN) and VAMC leadership and officials to retain their abilities to exercise appropriate local authorities and responsibilities.

However, VHA has concerns about ISOs "partnering" with VHA Institutional Review Boards (IRB). This recommendation for a partnership is contrary to the intent of the Federal Policy (Common Rule) for the Protection of Human Subjects that IRBs serve as independent oversight bodies. Specifically, Title 38 Code of Federal Regulations Part 16 Section 109 (38 CFR 16.109) provides that: "An IRB shall review and have authority to approve, require modifications in (to secure approval), or disapprove all research activities covered by this policy." This does not restrict the ability of other officials to disapprove or halt research. Currently, ISOs participate as non-voting members of IRBs to assist IRBs in their oversight responsibilities.

Under the OIT action plan, ISOs will be directed, subject to availability, to participate with local VHA IRBs and research staff on periodic reviews of research labs to ensure that VA information security requirements are met. The current plan is for the local VHA Research Compliance Officer with support from the appropriate ISO and VHA Privacy Officer to lead the reviews. VHA and OIT will collaborate about establishing guidelines for participation of ISOs in IRB activities in accordance with the Common Rule. Target dates for establishment of these guidelines and performance of these reviews are to be determined.

Furthermore, the VHA Office of Research Oversight (ORO) was established by statute to ensure that VA research meets regulatory requirements. ORO and OIT officials have in the past collaborated on inspections of VA research space to identify information security deficiencies. This will continue. VHA and OIT will explore how best to increase their collaborations and will establish an action plan to do so. Target date for increased cooperation is to be determined.

Recommendation 4: We recommend the Under Secretary for Health develop and implement a centralized data governance and storage model that ensures accurate inventory of all research data collected, data collection compliance with research protocols, and secure management of research information over the data life cycle.

VHA Response:

Concur.

While VHA agrees that it is important to ensure an accurate inventory of all research data collected, data collection compliance with research protocols, and secure management of research information over the data life cycle, it is not clear whether the use of a centralized data governance and storage model is feasible or appropriate. Such a governance and management model would take considerable human and monetary resources. And a cost-benefit analysis has yet to be performed to determine whether the benefit to be gained by such a system is appropriate to the level of resourcing required to develop, implement, and manage it over time.

VHA will work with VA OIT to establish the workgroup as outlined in the response to Recommendation 2 to address issues related to Recommendation 2 and 4.

Another consideration is how to address a risk-benefit analysis in order to meet the spirit of the Executive Order 13563, Improving Regulation and Regulatory Review.

Recommendation 5: We recommend the Under Secretary for Health require the Office of Research and Development to partner with Information Security Officers to routinely conduct joint oversight and monitoring of research labs to ensure security of sensitive veterans data, compliance of data collections with research protocols, and fulfillment of the Department's information security requirements.

VHA Response:

Concur.

It is important that facility ISOs with research expertise be readily available to support the research community in ensuring the protection of sensitive information. VHA and VA OI&T

will develop an action plan that meets the needs of both organization, including the need for Veterans Integrated Service Network (VISN) and VAMC leadership and officials to retain their abilities to exercise appropriate local authorities and responsibilities. VHA has provided additional details in its comments to Recommendation 3.

In any event, any steps that are taken in addition to those which are already departmental policy should be done in conjunction with the proposed joint effort with AAMC, in the spirit of EO 13563 as previously noted.

Appendix E Office of Inspector General Contact and Staff Acknowledgments

OIG Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Michael Bowman, Director Wade Greenwell Jack Henserling William Hill George Ibarra Ryan Nelson Steve Slawson

Appendix F 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.