VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Unsecured Patient Database at the VA Long Beach Healthcare System

March 28, 2018
15-04745-48

ACRONYMS

CPRS	computerized patient record system
DUA	Data Use Agreement
ISO	Information Security Officer
LBHCS	Long Beach Healthcare System
OIG	Office of Inspector General
OI&T	Office of Information and Technology
SCI	spinal cord injury
SCI/D	spinal cord injuries and disorders
SPI	Sensitive Personal Information
SSN	Social Security Number
USC	University of Southern California
VA	Department of Veterans Affairs
VHA	Veterans Health Administration

Executive Summary

Why the OIG Did This Review

In July 2015, the Office of Inspector General received allegations stating that an unauthorized Microsoft Access database was operating at the VA Long Beach Healthcare System (LBHCS). Specifically, the database created by personnel at LBHCS was not approved for use by VA's Office of Information and Technology (OI&T). The allegations further stated that the unauthorized database hosted Sensitive Personal Information (SPI) and that all of the Veterans Health Administration's (VHA) 24 Spinal Cord Injury (SCI) Centers had access to the database through a SharePoint intranet portal. The anonymous complainants also stated that unsecured veteran SPI was stored on a server outside of VA's protected network environment.

What the OIG Found

The OIG substantiated the allegation that an unauthorized Microsoft Access database was created by LBHCS SCI employees to capture patient demographics and to provide a repository for all SCI Centers to track patient data. Specifically, OI&T officials did not approve the use of Microsoft Access to support the capturing of patient outcomes data and the facility Privacy Officer was not made aware of its existence. Therefore, the facility Privacy Officer could not meet the requirements of VHA policy. Due to data encryption limitations, VA policy and the Technical Reference Model restricts the use of Microsoft Access to limited circumstances that were not applicable here.

Consistent with the allegation, the OIG found multiple instances of databases that hosted SPI in violation of VA policy. For example, the OIG team identified several Microsoft Access databases hosting SPI patient data that were stored on a network file share that provided restricted access for each SCI Center. VA policy states that information concerning an individual will not be maintained in an unauthorized system of records. Since the Microsoft Access program was not an approved system of records, the databases were not authorized to host patient SPI. The OIG noted that the former Executive Director, National SCI Program Office, authorized the creation of the Microsoft Access database and the collection of SPI patient data.

The OIG also substantiated that veteran SPI was hosted on an external server, located at the University of Southern California, without a formal Data Use Agreement (DUA) authorizing such activity. In addition, the OIG noted this server could be accessed from the internet using default logon credentials. SCI personnel manually entered clinical information obtained from VA's Computerized Patient Record System onto the university server in order to test the functionality of the supporting database. VA policy states that external information systems hosting VA data must be authorized under a formal DUA and appropriate safeguards must be established to secure the confidentiality of SPI. Despite this policy, LBHCS did not have a

formal agreement with the University of Southern California that authorized the transfer of information or defined security and confidentiality controls for the protection of SPI.

Based on interviews conducted during site visits in December 2015 and August 2016, these incidents occurred because: (1) the former Executive Director, National SCI Program Office, was unaware of Privacy Act requirements for official VA systems of records and did not discuss the data collection activities with the facility Privacy Officer; (2) the former Executive Director was unaware of VA security policies regarding Microsoft Access database use for storing veteran's SPI and did not obtain a security approval from OI&T personnel; (3) OI&T personnel did not conduct periodic reviews of SCI data collection activities to ensure that VA's information security and privacy requirements were met; and (4) the former Executive Director did not perform required due diligence and did not exercise proper security and privacy practices when sharing veteran SPI with an external non-federal entity due to a lack of awareness of VA information security and privacy requirements. As a result, veteran's sensitive data were put at risk of unauthorized access and disclosure.

What the OIG Recommended

The OIG recommended the Under Secretary for Health ensure that the Spinal Cord Injury and Disorders program staff comply with VA's Privacy Program and information security requirements for all veteran sensitive data collected. In addition, the OIG recommended the Executive Director for the National Spinal Cord Injury Program Office discontinue storing SPI in unauthorized Microsoft Access databases. The OIG also recommended the Acting Assistant Secretary for Information Technology ensure that Field Security Services and VA's Privacy Service implement improved procedures to identify unauthorized uses of SPI and take appropriate corrective actions.

Management Comments

The Executive in Charge, Office of the Under Secretary for Health, and the Executive in Charge for the Office of Information and Technology concurred with the recommendations. Specifically, the Executive in Charge, Office of the Under Secretary for Health, reported that an information security officer has been assigned to the Spinal Cord Injury National Program Office to review and correct information security deficiencies for all databases that host veteran sensitive information. In addition, the Executive in Charge reported that upon notification of improper data storage and use of an older version of Microsoft Access, the National Program Office began storing veteran sensitive data using approved versions of Microsoft Access and Microsoft Excel.

The Executive in Charge for the Office of Information and Technology reported that VA has an active project to develop and implement a capability to prevent the execution of unauthorized software programs using McAfee Application Control and will work towards implementing an approved software application whitelist. Once complete, the appropriate personnel will be trained consistent with their roles and functions. The Executive in Charge also reported that in November 2017, information security officers validated all 24 SCI program sites were no longer using unauthorized versions of Microsoft Access databases.

The corrective action plans from both Executives in Charge were responsive to the recommendations. The OIG will monitor implementation of the planned actions and will close the recommendations when it receives sufficient evidence demonstrating progress in addressing the identified issues.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Objective

The OIG conducted this review to determine the merits of allegations the Office of Inspector General received through its Hotline, stating that an unauthorized Microsoft Access database was hosting veteran Sensitive Personal Information (SPI) at the VA Long Beach Health Care System (LBHCS). The allegations further stated that all of VHA's 24 Spinal Cord Injury (SCI) Centers had access to the database through a SharePoint intranet portal. Furthermore, the OIG determined whether SPI was hosted at external sites outside of VA's protected environment and if controls were established to protect this information.

Background

The mission of the Veterans Health Administration (VHA) SCI System of Care is to support, promote, and maintain the health, independence, quality of life, and productivity of individuals with SCI throughout their lives. These objectives are accomplished through:

- Rehabilitation,
- Sustaining medical and surgical care,
- Patient and family education,
- Psychological care,
- Vocational care, and
- Research.

VA's 24 SCI Centers provide healthcare services for veterans with spinal cord injury and disorders (SCI/D). The SCI system of care requires a full interdisciplinary team of experts within SCI Centers and designated support clinics at other VA medical centers. The former Executive Director, National SCI Program Office, stated that she authorized the creation of a Microsoft Access database to collect patient outcomes data after VA's legacy Spinal Cord Injury and Disorders Outcomes Repository system was decommissioned. After its creation, the unpopulated Microsoft Access database was distributed to Management of Information and Outcomes coordinators. Subsequently, the Management of Information and Outcomes coordinators were responsible for transferring SCI patient data to their assigned network file share. During interviews with SCI personnel, the OIG team found that the former Executive Director also directed SCI personnel to enter sensitive patient data into a database maintained by the University of Southern California (USC) to test the functionality of the database under development.[1]

[1] VA Directive 6502, *VA Enterprise Privacy Program,* May 5, 2008.

RESULTS AND RECOMMENDATIONS

Finding 1 Database Hosting Veteran Sensitive Data Was Not Authorized or Properly Secured

The OIG team substantiated the allegation that an unauthorized Microsoft Access database was created by LBHCS SCI employees, under the direction of the former Executive Director National SCI Program Office, to capture patient demographics and to provide a repository for all SCI Centers to track patient data under their care. More specifically, OI&T officials did not approve the use of Microsoft Access to support capturing patient data and the facility Privacy Officer was not made aware of its existence. Therefore, the Privacy Officer could not meet the requirements of VHA Handbook 1080.01, *Data Use Agreements*. Due to data encryption limitations, VA Handbook 6500 and OI&T's Technical Reference Model restrict the use of Microsoft Access to limited circumstances that were not applicable in this situation. The OIG team noted that the former Executive Director, National SCI Program Office, authorized the creation of the Microsoft Access database and the collection of SPI patient data.

Consistent with the allegation, the OIG team found databases that hosted SPI in violation of VA policy.[2] For example, the team observed Microsoft Access databases hosting SPI patient data on a network file share that provided restricted access for each SCI Center. Furthermore, VA standards state that the Privacy Act requires the publication of specific information concerning systems of records.[3] Since the Microsoft Access program was not authorized to host SPI in accordance with VA Handbook 6500 nor approved as an official system of records, the databases should have never been created to maintain SCI patient data.

Criteria

VA Handbook 6500 states that database management requires the use of Federal Information Processing Standard 140-2-compliant data encryption to protect the confidentiality and integrity of VA data. In accordance with the One-VA Technical Reference Model, Version 17.3, Microsoft Access must be properly configured as a front-end client and no data at rest should be stored on the local system. Microsoft Access may only be used with sensitive data as part of a secured system when Microsoft Access is configured as a client front end to an appropriately secured Microsoft SQL Server or Microsoft SharePoint Server following VA security configuration baselines and connected via a FIPS 140-2-certified encrypted connection. Furthermore,

[2] VA Handbook 6500, *Risk Management Framework for VA Information Systems-Tier 3: VA Information Security Program*, March 10, 2015.
[3] VA Handbook 6300.5, *Procedures for Establishing and Managing Privacy Act Systems of Records*, August 3, 2017.

Microsoft Access usage is limited to databases supporting individual users' personal productivity and/or training as database administrators. Desktop database management systems may not be used to support line of business operations requiring data durability or persistence.

VA Handbook 6300.5 defines a system of records as

> Any group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

When an agency creates a retrieval method or cross-index arranged by personal identifier for randomly filed records, that record collection is a system subject to the provisions of the Privacy Act.[4] VA Handbook 6300.5 also states that system managers must work with the Privacy Officer or designee to ensure that procedures for access, correction, or amendment of records conform to records requirements[5] and that VA regulations governing the Privacy Act are being followed.[6] Furthermore, VA Handbook 6300.5 states that system managers must ensure that systems of records are not operated without first publishing the required notices within the *Federal Register* notice.

VA Handbook 6500 states that the VA

> Deputy Chief Information Officer for Service Delivery and Engineering and Information System Owners are responsible for the overall procurement, development, integration, modification, daily operations, maintenance, and disposal of VA information and information systems, including ensuring each system is assigned an Information System Owner and that the Information System Owner is responsible for the security of the system.

VA Handbook 6500 further states that Information Security Officers (ISO), as OI&T Field Security Service agents, have the "responsibility to ensure the appropriate operational security posture is maintained for" information

[4] The Privacy Act of 1974, Public Law 93-579, Dec 31, 1974, 5 U.S.C. § Section 552a(e) stipulates that "each agency that maintains a system of records shall… publish in the *Federal Register* notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency."

[5] VA Handbook 6300.5; VA Handbook 6300.4, *Procedures for Processing Requests for Records Subject to the Privacy Act,* August 19, 2013; VHA Handbook 1605.1, *Privacy and Release of Information,* August 31, 2016.

[6] VHA Directive 1605.01, *Privacy and Release of Information,* August 31, 2016 replaced VHA Handbook 1605.1, *Privacy and Release of Information,* May 17, 2006.

systems. ISOs are also responsible for participating in security self-assessments and external and internal audits of system safeguards and program elements.

Allegations Substantiated

The OIG team substantiated the allegation that an unauthorized Microsoft Access database was created by LBHCS SCI employees to capture patient demographics and to provide a repository for all SCI Centers to track patient data under their care. OI&T officials did not approve the use of Microsoft Access to support the capturing of patient outcomes data and the facility Privacy Officer was not made aware of its existence. Therefore, the Privacy Officer could not meet the requirements of VHA Handbook 1080.01. Due to data encryption limitations, VA policy and the Technical Reference Model restrict the use of Microsoft Access to limited circumstances that were not applicable here.

The former Executive Director authorized the creation of the Microsoft Access database as a temporary replacement database after the legacy Spinal Cord Injury and Disorders Outcomes Repository was decommissioned in September 2015. In accordance with the Privacy Act of 1974, the legacy Repository system was reported to the Office of Management and Budget and recorded within its System of Record Notice No. 108VA11S. The notice identified that the following SPI was collected within the repository: name, Social Security Number, date of birth, registration date, outcome measures of impairment, social role participation, and satisfaction with life.

In August 2015, the former Executive Director instructed SCI personnel to create a Microsoft Access database to collect and store patient data, including name, SSN, and outcomes data. Copies of the unpopulated database were distributed to each of the 24 SCI Centers. Each center was responsible for maintaining its respective database on a network file share assigned by the National SCI Program Office. Beginning in September 2015, pursuant to the executive director's direction, coordinators in each SCI Center were instructed to start using the Microsoft Access database to collect all data, including for registering new patients.

The Microsoft Access databases also contained data elements from VA's Computerized Patient Record System (CPRS), including information from clinical treatment notes and outcomes assessments, which is considered protected health information and SPI. The collection of SPI within these Microsoft Access databases was not authorized to operate as an official system of record. This is because VA had not updated the *Federal Register* notice of any new use or intended use of a system from which information could be retrieved by an individual's assigned record number, as required by VA Handbook 6300.5.

In addition to potentially violating Privacy Act provisions, the Microsoft Access databases were not designed to afford the encryption protections

mandated by VA's Deputy Assistant Secretary for Information Security and Chief Information Security Officer.[7] VA policy further states that a database management system must have appropriate access enforcement and physical security controls, to include restricting user access to the database and auditing access to the hard drive. In addition, the database management system must be continuously monitored and scanned for unauthorized access. Despite this policy, SCI personnel did not implement appropriate security controls as required by VA policy and the Technical Reference Model. Conversely, a centralized database management system containing the proper security controls would be capable of meeting the relevant security requirements as mandated by VA's Deputy Assistant Secretary for Information Security.

Why This Happened

These incidents occurred because:

- The former Executive Director, National SCI Program Office, who assumed the role of system manager and information system owner, did not seek guidance and was unfamiliar with Privacy Act requirements for establishing an official VA System of Records and did not discuss data collection activities with the LBHCS Privacy Officer;
- The former Executive Director did not seek guidance and was unaware of VA security policies regarding the restricted use of Microsoft Access databases for storing veteran's SPI, and did not obtain a security review and approval from OI&T personnel; and
- OI&T personnel, after becoming aware of a potential unauthorized Microsoft Access database, did not conduct periodic reviews of SCI data collection activities to ensure that VA's information security and privacy requirements were met.

Specifically, the former Executive Director did not exercise due diligence, such as seeking security guidance, before directing the creation of the Microsoft Access database. The Executive Director also neglected to consult with the facility Privacy Officer to determine whether any Privacy Act violations could occur with this data collection activity. As a result, the Microsoft Access database operated as an unapproved system of records because VA had not updated the *Federal Register* notice of any new use or intended use of a system from which information could be retrieved by an individual's assigned record number. The former Executive Director also did not exercise due diligence by failing to obtain an OI&T security review in

[7] VA Deputy Assistant Secretary for Information Security Memorandum, *FIPS 140-2 Validated Full Disk Encryption for Data at Rest in Database Management Systems,* May 5, 2015.

accordance with VA Handbook 6500 prior to using the Microsoft Access database for data collection activities. Consequently, the Microsoft Access database was used to collect certain amounts of SPI without proper OI&T oversight and authorization.

In February 2015, the LBHCS ISO was aware of SCI personnel's intent to establish a Microsoft Access database to support data collection activities. While the ISO notified his supervisors of the potential unauthorized use of the Microsoft Access database, OI&T did not take steps to determine whether proper security safeguards were implemented to protect sensitive data. Moreover, OI&T still had not conducted a security review by the time of the site visit in August 2016 to determine if the Microsoft Access database was authorized to collect, store, and maintain SPI in accordance with VA policy. Specifically, OI&T did not ensure the database had proper security controls to ensure the confidentially, integrity, and availability of VA information.

Effects of Unauthorized Database

Creating an unencrypted Microsoft Access database and populating the database with veteran SPI created significant risks for potential disclosure of SPI to unauthorized personnel, as defined by VA policy. Furthermore, without appropriate security controls, including database encryption and password enforcement, the Microsoft Access database was vulnerable to access by unauthorized users without proper authentication. Without proper user access controls, the database files were vulnerable to modification and subject to data corruption by unauthorized personnel. Moreover, the use of a Microsoft Access database created an unapproved system of records and thus potentially exposed VA to penalties associated with the Privacy Act of 1974. As a result, veteran SPI was at risk of unauthorized disclosure.

Conclusion

VA has established information security controls that are designed to protect its networks from unauthorized access and prevent unauthorized disclosure of information. VA has restrictions on the disclosure of sensitive information and the creation of official system of records. Despite these policy requirements, the former Executive Director for the National SCI Program Office failed to exercise due diligence during the creation of a Microsoft Access database that would host veteran sensitive data. Consequently, it is imperative for VHA to ensure that the SCI program complies with the Privacy Act and VA's privacy and security requirements when collecting veteran sensitive data. In addition, facility ISOs and privacy officers must improve their oversight of SCI data collection activities to ensure their compliance with VA's Privacy Program and information security requirements.

Recommendations

1. The OIG recommended the Under Secretary for Health ensure the Spinal Cord Injury program complies with VA's Privacy Program and information security requirements for all veteran sensitive data collected.

2. The OIG recommended the Executive Director for the National Spinal Cord Injury Program Office discontinue the use of unauthorized versions of Microsoft Access for the storage of Spinal Cord Injury program data and implement an approved system to support its data storage and analysis needs.

3. The OIG recommended the Acting Assistant Secretary for Information Technology ensure that VA's Field Security Services and Privacy Service implement improved procedures to identify unauthorized uses of Sensitive Personal Information and train the facility information security officers and privacy officer to ensure that appropriate corrective actions are taken.

Management Comments

The Executive in Charge, Office of the Under Secretary for Health, and the Executive in Charge for the Office of Information and Technology concurred with the recommendations. For Recommendation 1, the Executive in Charge, Office of the Under Secretary for Health, reported that an information security officer has been assigned to the Spinal Cord Injury National Program Office to review privacy issues and information security requirements for all databases that host veteran sensitive information. In addition, the Executive in Charge reported that a privacy officer will be assigned to the Spinal Cord Injury National Program Office to review and correct any privacy related issues.

For Recommendation 2, the Executive in Charge, Office of the Under Secretary for Health, reported that upon notification of improper data storage and utilization of an older version of Microsoft Access, the National Program Office began storing veteran sensitive data on approved versions of Microsoft Access and Microsoft Excel. In addition, VHA is currently researching a permanent data repository solution for the legacy application that was decommissioned in 2015.

For Recommendation 3, the Executive in Charge for the Office of Information and Technology reported VA is piloting McAfee Application Control to define authorized software, control the software that can be installed on the system, and prohibit the ability for unapproved software to run on a system until the software is removed by script from devices. The Executive in Charge also reported this solution prevents the installation of specific applications. McAfee Application Control will provide an automated administration of both whitelist (authorized) or blacklist (unauthorized) software categories, along with approved exclusions for specific conditions.

Once complete, the appropriate personnel will be trained consistent with their roles and functions.

OIG Response

The corrective action plans from both Executives in Charge were responsive to the recommendations. The OIG will monitor implementation of the planned actions and will close the recommendations when it receives sufficient evidence demonstrating progress in addressing the identified issues.

Finding 2 University Was Hosting Unauthorized Veteran Sensitive Data

The OIG substantiated the allegation that veteran SPI was hosted on an external server without a formal Data Use Agreement (DUA) authorizing such activity. The OIG noted this server, located at the University of Southern California (USC), could be accessed from the internet using default logon credentials. SCI personnel manually entered clinical information obtained from VA's CPRS onto the external server to test the functionality of the supporting database. VA policy states that external information systems hosting VA data must be authorized under a formal DUA and appropriate safeguards must be established to ensure the security and confidentiality of SPI. Despite this policy, LBHCS did not have a formal agreement with the university that authorized the transfer of information or defined security controls for the protection of SPI.

These incidents occurred because the former Executive Director lacked an awareness of specific VA information security and privacy requirements when sharing veteran SPI with an external non-federal entity. In addition, the former Executive Director inappropriately presumed the SPI collected was properly de-identified, and therefore a formal DUA was not necessary. Consequently, SCI personnel did not consult OI&T officials or the facility Privacy Officer prior to transferring veteran SPI onto the university server. As a result, veteran sensitive data were at risk of unauthorized access and disclosure.

Criteria

VHA Handbook 1080.01 states data owners must enter into a DUA before transferring or sharing VHA data with non-federal entities. The policy also states data owners must consult with the facility privacy officer to determine if the data can be shared and if relinquishing data ownership is appropriate. Furthermore, privacy officers must review all applicable DUAs and determine whether a privacy legal authority exists for sharing VHA data. In addition, non-federal entities that receive VHA protected health information shall establish appropriate administrative, technical, procedural, and physical safeguards in accordance with VA Handbook 6500.

VHA standards state health information must be properly de-identified to be considered not individually identifiable.[8] This policy also states the disclosure of information must not be made unless it is in the best interests of VHA and the veteran who is the subject of the disclosure.

[8] VHA Handbook 1605.1 Appendix B, *De-Identification of Data*.

Allegations Substantiated

The OIG team substantiated the allegation that USC was hosting SPI about SCI on a server located on its campus and under its control. Specifically, the team determined that the database server was physically located at USC's Image Processing and Informatics Laboratory located in Los Angeles, California. The database was developed by USC officials in coordination with SCI personnel to test database functionality that could eventually support a specific VHA Office of Rural Health project.

The USC server failed to meet VA's information security requirements for appropriate access controls to protect sensitive data. Specifically, the USC server allowed all users to gain access to the database by providing a default user name and weak password, contrary to VA policy. VA Handbook 6500 requires that external information systems comply with VA information security requirements, employ VA-defined security controls, and specify their use in a DUA. As such, any external system that processes, stores, or transmits VA information must meet system security controls for authentication and must enforce VA minimum password complexity requirements. In addition, ISOs must ensure that VA security and privacy requirements are met prior to the sharing of VA sensitive data.

During interviews with SCI personnel, the OIG team discovered that in April 2015, the former Executive Director for the National SCI Program Office authorized SCI occupational therapists to enter sensitive patient data into an external database maintained by USC. Under her direction, SCI personnel used data obtained from CPRS clinical notes to populate the external database. The OIG team found that occupational therapists were using the first initial of a patient's last name and the last four numbers of their SSN to form a unique record identifier that potentially violates VHA policy. The OIG team validated this by accessing the USC database and viewing SCI patient information. In accordance with VHA Handbook 1605.1, the use of CPRS clinical notes coupled with a patient record identifier does not ensure proper de-identification of patient data.

The LBHCS SCI Program Office sought to populate the USC database with patient data that was specific to VHA's Lifestyle Redesign® program. The LBHCS Spinal Cord Injuries and Disorders (SCI/D) Center planned to expand the Lifestyle Redesign® program to 12 additional SCI/D Centers that use telehealth programs serve a high percentage of rural veterans with spinal cord injuries and disabilities. The USC project database was developed by USC personnel for potential use in the data collection activities. However, no authorization was provided for the release of SCI patient data to USC officials. Specifically, the former Executive Director inappropriately presumed the information was properly de-identified and therefore failed to execute a DUA with USC in accordance with VHA Handbook 1080.01. In addition, the former Executive Director did not collaborate with USC officials to define the necessary security controls to protect veteran sensitive data in accordance with VA policy. Furthermore, OI&T personnel and the

Privacy Officer stated that they were not aware of the existence of this database.

In May 2016, the LBHCS ISO reported this incident to the VA Data Breach Response Service via the Privacy and Security Event Tracking System in accordance with VA standards.[9] In June 2016, the Data Breach Response Service determined, through a review and analysis, that the disclosure of the information did not meet the criteria for a data breach due to exclusions contained in applicable VA Policy. According to a USC memo provided to the LBHCS ISO, patient data were sanitized in accordance with standards defined by the National Institute of Standards and Technology.

Why This Happened

The creation of the USC database to host veteran SPI occurred because the former Executive Director neglected to perform the proper due diligence, such as seeking security guidance from the facility ISO and the Privacy Officer, as required by VA information security and privacy protection policies. In addition, the former Executive Director lacked an awareness of specific VA information security and privacy requirements when sharing veteran SPI with an external non-federal entity. Moreover, the former Executive Director inappropriately presumed the SPI collected was properly de-identified, and therefore a formal DUA was not necessary. Consequently, the former Executive Director failed to collaborate with the facility ISO and the Privacy Officer on the requirements for the authorized disclosure and the protection of sensitive health information. Therefore, a proper authorization for the release of sensitive information to USC officials was not obtained.

Effects of the Unauthorized Data Sharing

By disclosing VA sensitive personal information to USC personnel without proper authority, veteran sensitive data were put at risk of unauthorized access and disclosure. Furthermore, the use of inappropriate access controls, including weak passwords, placed veteran data at risk of unauthorized access, disclosure, and use resulting from the use of weak passwords.

Conclusion

The OIG substantiated the allegation that veteran SPI was hosted on a USC server without a formal information security agreement authorizing the activity. In addition, the OIG team noted that SCI personnel failed to properly de-identify sensitive veteran information that was shared with USC personnel. Data owners must enter into a DUA before sharing VHA data with non-federal entities. Furthermore, ISOs and privacy officers must take action to remediate the unauthorized disclosure of veteran SPI in accordance with VA policies and any other applicable law.

[9] VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, July 28, 2016.

Recommendation

4. The OIG recommended VA's Field Security Services and Privacy Service conduct a formal review of Spinal Cord Injury projects to identify acceptable disclosures of veteran Sensitive Personal Information and ensure that appropriate safeguards are implemented to protect the confidentiality of veteran data.

Management Comments

The Executive in Charge for the Office of Information and Technology concurred with the recommendation. The Executive in Charge reported that in November 2017 information security officers validated that all 24 SCI program sites were not using unauthorized versions of Microsoft Access databases. In addition, the Office of Information and Technology assigned an information security officer to the Spinal Cord Injury Program Office in November 2017. VA's Privacy Service recommended that VHA privacy officers and Compliance Offices work with the facility ISOs and conduct appropriate reviews of all sites storing SCI data.

OIG Response

The Executive in Charge's corrective action plan is responsive to the recommendation. The OIG will monitor implementation of the planned action and will close the recommendation when it receives sufficient evidence demonstrating progress in addressing the identified issues.

Appendix A Background

VHA has 24 SCI Centers established across the nation. These centers report through the National SCI Program Office and the SCI Executive Director. VHA's SCI System of Care provides a full range of care for veterans who have sustained a spinal cord injury or have neurologic impairments to the spinal cord. The SCI System of Care consists of an integrated network of care based on a hub and spoke model. SCI Centers serve as the hub. Each SCI Center has spoke sites designed to provide SCI patient treatment within designated areas. The scope of SCI Center services is to deliver primary care, specialty health care, and rehabilitation services to individuals with spinal cord injuries and disorders.

Historically, SCI Centers and clinical staff have used the Spinal Cord Injury/Disorders and Outcomes system to enter and track patients' outcomes over time. These outcome measures include the American Spinal Injury Association International Standards for the Classification of Spinal Cord Injury, Functional Independence Measure, Craig Handicap Assessment and Reporting Technique, Functional Assessment Measure, Duke Severity of Illness Checklist, Diener's Satisfaction with Life Scale, and Kurtzke Expanded Disability Status Scales.

USC Lifestyle Redesign® Project

The Lifestyle Redesign® program, developed by the Occupational Therapy Department at USC, is a treatment approach designed to improve health and wellness by managing chronic conditions with healthier lifestyles. The Lifestyle Redesign® program focuses on identifying barriers and facilitators that are associated with an individual's management of particular disease conditions, including spinal cord injury and multiple sclerosis. Once the problems are identified, therapists work closely with the individuals to develop goals that focus on appropriate lifestyle changes to manage the conditions.

LBHCS-USC Collaboration

In 2012, the LBHCS SCI/D Center, in collaboration with USC, piloted an Office of Rural Health project that focused on the prevention and management of pressure ulcers for high-risk rural Veterans with SCI/D and disorders. Subsequently, the Lifestyle Redesign® program was administered to 14 eligible veterans and all participants reported accomplishing their short-term goals of adopting lifestyle changes with a high degree of satisfaction. The initial outcomes indicated the Lifestyle Redesign® program was a viable occupational intervention when helping veterans with SCI/D to better manage their health risks and enhancing their quality of life.

Appendix B Scope and Methodology

Scope

The OIG team conducted its review work from October 2015 through February 2017. It focused the review on the National SCI Program Office and at select SCI/D Centers. It also conducted a site visit to the USC Image Processing and Informatics Laboratory in Los Angeles, California. The lab collaborates with scientists worldwide to conduct pioneering biomedical imaging and informatics technologies research and participates in clinical research and development services. The OIG team contacted the VHA's Office of Rural Health to discuss VHA-funded projects, including the National SCI Program Office's implementation of the Lifestyle Redesign® program to high-rural-population SCI Centers. The team also evaluated the allegations in connection with VA and federal regulations related to the Privacy Act, Privacy Program, and information technology security requirements.

Methodology

To accomplish its objectives, the OIG team reviewed applicable laws, regulations, policies, procedures, and guidelines. During its review, the team conducted site visits to the National SCI Program Office, the SCI Centers located at the LBHCS, and VA's Puget Sound Health Care System. The OIG team also interviewed SCI personnel. The site visits provided the team with an understanding of the SCI program and its standard of care for veterans suffering with spinal cord injuries. The team also gained an understanding of data collection that was conducted by the LBHCS SCI Center and the National SCI Program Office. In addition, the OIG team examined the types of medical data associated with the treatment of SCI patients, accreditation requirements, and Management of Information and Outcomes coordinators' reporting responsibilities. Furthermore, the OIG team collaborated with VA's Office of Accountability Review in connection with its Administrative Investigation involving the operations and management of the National SCI Program Office and reviewed the relevant findings.

Data Reliability

The OIG team did not request computer-processed data or financial data for this review. It examined copies of computer images of SCI patient information taken from CPRS and determined them to be reliable and sufficient for the review.

Government Standards

We conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.* The evidence obtained provides a reasonable basis for the findings and conclusions based on the review objective.

Appendix C Management Comments – Office of the Under Secretary for Health

Department of Veterans Affairs Memorandum

Date: December 22, 2017

From: Executive in Charge, Office of the Under Secretary for Health

Subj: OIG Draft Report—Review of Alleged Unsecured Patient Database at the VA Long Beach Healthcare System

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

1. Thank you for the opportunity to review and comment on VA Office of Inspector General (OIG) draft report Department of Veterans Affairs: Review of Alleged Unsecured Patient Database at VA Long Beach Healthcare System. I concur with both recommendations to my office and provide corrective actions to address the concerns raised in this report. I also provide general and technical comments on the findings in the draft report (attached). The Department of Veterans Affairs (VA) Office of Information and Technology (OI&T) and VA's Field Security Services and Privacy Service will respond to recommendations 3 and 4 respectively.

2. VHA, as the Health Insurance Portability and Accountability Act (HIPAA) covered entity, assumes full responsibility for ensuring the Spinal Cord Injuries and Disorders (SCI/D) National Program Office complies with HIPAA-specific privacy and security protection of patient data. SCI/D National Program Office will undergo a HIPAA compliance assessment after it implements corrective actions, scheduled for March 2018.

3. The SCI/D National Program Office must also comply with general (as opposed to HIPAA-specific) privacy and security protections that apply to any electronic data. The SCI/D National Program Office is collaborating with VA OI&T, VA Field Security Service, and select Veteran Integrated Service Network (VISN) Information Security Officers to develop and implement necessary corrective actions to comply with the Department's Privacy Program and Information Security Requirements. Dedicated Privacy and Information Security Officers will assist the SCI/D National Program Office to identify and correct potential problematic areas. The SCI/D National Program Office is now using Microsoft Access 2016 as approved by OI&T.

4. If you have any questions, please email Karen Rasmussen, M.D., Director, Management Review Service at VHA10E1DMRSAction@va.gov.

(Original signed by:)

Carolyn M. Clancy, M.D.

Executive in Charge – Office of the Under Secretary for Health

Attachments

Attachment

Veterans Health Administration (VHA)
Comments on OIG Draft Report
Review of Alleged Unsecured Patient Database at the VA Long Beach Healthcare System

VHA concurs with OIG's recommendations in the draft report and provides the following comments in response to the recommendations:

Recommendation 1: We recommended the Under Secretary for Health ensure the Spinal Cord Injury program complies with VA's Privacy Program and information security requirements for all veteran sensitive data collected.

VHA Comments: Concur. The Spinal Cord Injuries and Disorders (SCI/D) National Program Office, in collaboration with the Department of Veterans Affairs (VA) Office of Information and Technology (OI&T), VA Field Security Service (VA FSS), and Veterans Integrated Service Networks (VISN) 20 and 22 Information Security Officers (ISO), reviewed privacy issues and information security requirements for databases containing Veteran-sensitive information. Based on this review, the SCI/D National Program Office submitted a request to VA FSS for a designated ISO. As of November 2017, an ISO was assigned to SCI/D to thoroughly review and correct information security requirements of all databases that contain Veteran sensitive data within the SCI/D National Program Office.

A Veterans Health Administration (VHA) Central Office Privacy Officer will also be assigned to SCI/D to thoroughly review and correct any privacy issues within the SCI/D National Program Office. SCI/D will continue to review all existing data and technology security policies and processes, and will revise any policy or process as necessary. The VHA Office of Health Information Governance's Health Care Security Requirements and Privacy Compliance Assurance Programs will conduct a Health Insurance Portability and Accountability Act compliance assessment of the SCI/D National Program Office during the 2nd Quarter of fiscal year 2018 to ensure compliance with privacy and security requirements including only the approved versions of Microsoft Access and Excel are in use.

Status: In Process Target Completion Date: April 2018

Recommendation 2: We recommended the Executive Director for the National Spinal Cord Injury Program Office discontinue the use of unauthorized versions of Microsoft Access for the storage of SCI data and implement an approved system to support its data storage and analysis needs.

VHA Comments: Concur. In fall 2015, data previously stored in the Spinal Cord Injury and Disorders Outcomes (SCIDO) application was migrated to the Corporate Data Warehouse. Upon notification of improper data storage and utilization of unauthorized older version of Microsoft Access, newly submitted data to the Spinal Cord Injuries and Disorders (SCI/D) National Program Office was stored in Microsoft Excel as recommended by the Veterans Integrated Service Network (VISN) 20 Information Security Officer (ISO). Older data currently stored in a Microsoft Access database was reviewed by VISN 20 to ensure compliance with the Department of Veterans Affairs (VA) privacy and security requirements. The SCI/D National Program Office currently utilizes Microsoft Access 2016 as approved by the Department of Veterans Affairs Office of Information and Technology (OI&T). Both the current versions of Microsoft Access and Microsoft Excel are approved for use with sensitive data following constraints according to the OI&T Technical Reference Model.

Additionally, the SCI/D National Program Office is currently researching a permanent data repository solution as the SCIDO application was decommissioned in 2015. Although funding for a permanent repository is not available, interim solutions were implemented to maintain SCI/D business operations and reporting requirements as stipulated by policy and legislation. Specifically, in collaboration with OI&T, the VHA Office of Health Information Governance's Healthcare Security Requirements Program, and VA

Field Security Service (VA FSS), project initiation efforts are being planned to design and implement a more permanent solution.

Finally, the SCI/D National Program Office submitted a request to VA FSS for a designated ISO. As of November 2017, an ISO was assigned to SCI/D to thoroughly review and correct information security requirements of all databases that contain Veteran sensitive data within the SCI/D National Program Office. A Veterans Health Administration Central Office Privacy Officer will also be assigned to SCI/D to thoroughly review and correct any privacy issues within the SCI/D National Program Office. SCI/D will continue to review all existing data and technology security policies and processes and will revise any policy or process as necessary.

Status: In Process Target Completion Date: April 2018

Appendix D Management Comments – Office of the Assistant Secretary for Information and Technology

Department of Veterans Affairs Memorandum

Date: February 21, 2018

From: Executive in Charge for the Office of Information and Technology (005)

Subj: OIG Draft Report *Review of Alleged Unsecured Patient Database at the VA Long Beach Healthcare System*

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

Thank you for the opportunity to review the Office of Inspector General draft report, "Review of Alleged Unsecured Patient Database at the VA Long Beach Healthcare System." The Office of Information and Technology submits the attached written comments. If you have any questions, contact me at (202) 461-6910 or have a member of your staff contact Dominic Cussatt, Deputy Chief Information Officer and Chief Information Security Officer, Office of Information Security at 202-461-0044.

(original signed for:)

Scott R. Blackburn

Attachments

Attachment

Office of Information and Technology (OI&T)
Comments on OIG Draft Report:
"Review of Alleged Unsecured Patient Database at VA Long Beach Healthcare System"

OIG Recommendation 3: We recommended the Acting Assistant Secretary for Information Technology ensure that VA's Field Security Services and Privacy Service implement improved procedures to identify unauthorized uses of Sensitive Personal Information and train facility Information Security Officers and Privacy Officer to ensure that appropriate corrective actions are taken

OI&T Comments: Concur. VA has a solid well defined Technical Reference Model (TRM) that provides classification status for each identified software application on the VA Enterprise. The TRM maintains a current prohibited and unapproved software list and provides a process of submitting new TRM requests for reviewing and assigning classifications for new software titles discovered on the VA enterprise. VA provides daily scanning for applications across the VA using IBM BigFix and Microsoft SCCM/SCM. The two outputs are analyzed and merged using Business DNA (BDNA) to produce an enterprise list of installed applications. This installed list of applications is compared against TRM prohibited and unapproved software lists to identify current application titles and specific locations (with devices) that require prohibited and unapproved software remediation.

Software remediation of prohibited and unapproved software requires notification of a planned action including automating the removal scripts, and in many cases, manual IT support to remove. This is a continual process for software remediation of prohibited and unapproved software. At present, the VA has achieved 98% remediation of prohibited software and a 73% reduction of unapproved software. Further, OIT Infrastructure Operations conducts daily database scans through a combination of custom Powershell script, Idera and SCCM tools. That data is part of the Enterprise Database Inventory that is available to Privacy Officers for review of SPI. However, this process does not include MS Access Databases or the search of Protected Health Information (PHI)/Personally Identifiable Information (PII).

VA does have an active and funded project to develop and implement a Blacklist. This project focuses on the deployment of the Continuous Diagnostic and Monitoring (CDM) Software Asset Management (SWAM) Capability and is part of a greater CDM deployment effort in partnership with the Department of Homeland Security. Following NIST guidelines, VA will "prevent the execution of unauthorized software programs" using McAfee Application Control and will work towards building and implementing a whitelist. The VA solution begins with utilizing the end-user protection software installed on all systems (workstations and servers) throughout the Enterprise.

Currently the VA is piloting McAfee application control to define authorized software, control the software can be installed on the system, and prohibits the ability for unapproved software to run on a system until it be removed by script from devices. This solution prevents the installation of specific applications, an example of which is Kaspersky. Options with McAfee Application Control provide an automated administration of both whitelist (authorized) or blacklist (unauthorized) software categories along with approved exclusions for specific conditions. Remaining project activities are scheduled to be completed by May 25, 2018, for implementing a VA Blacklist with McAfee Application Control. The appropriate personnel will be trained consistent with their roles and functions.

Status: In Process Target Completion Date: September 2018

OIG Recommendation 4: We recommended VA's Field Security Services and Privacy Service conduct a formal review of Spinal Cord Injury projects to identify acceptable disclosures of veteran Sensitive Personal Information and ensure that appropriate safeguards are implemented to protect the confidentiality of veteran data.

OI&T Comments: Concur and complete. Once VA Field Security Services (FSS) was notified of the 24 SCI sites an action item was immediately executed to determine if the SCI program sites were using

Microsoft Access Database 2010 or prior versions. See attachment A for the action item and response examples attachments B and C. ISOs at all 24 SCI sites have conducted reviews and validated, with their respective facility SCI program, that they are not using MS Access Database 2010 or prior versions. As discussed previously any sites using MS Access 2016 are within Technical Reference Model (TRM) compliance. Additionally, the current SCI Program Director has been notified on how to obtain an ISO to provide on-going support and information security guidance to the National SCI Program. The Deputy SCI Director submitted a request for an ISO and FSS has assigned one as of November 30, 2017. This action is complete, see attachment D.

VA Privacy Service recommends that VHA Privacy Officers and the appropriate VHA Compliance Offices work with the facility Information Security Officers (ISOs) and conduct appropriate reviews of all sites storing SCI data. The Office of Quality, Privacy and Risk (QPR) conducts Privacy and Records Assessments at VA facilities but is limited in conducting assessments at VHA facilities. Based on the above information, OIT considers this recommendation completed.

Status: Complete Target Completion Date: Not Applicable

Appendix E OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Michael Bowman, Director Tom Greenwell George Ibarra

Appendix F Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals

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 is available on our website at www.va.gov/oig.