VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Contractor Information Security Violations in the Alaska VA Healthcare System

September 7, 2016
15-01994-238

ACRONYMS

AVAHS	Alaska VA Healthcare System
COR	Contracting Officer's Representative
ISO	Information Security Officer
OIG	Office of Inspector General
VA	Department of Veterans Affairs
VISN	Veterans Integrated Service Network

Highlights: Review of Alleged Contractor Information Security Violations in the Alaska VA Healthcare System

Why We Did This Review

In December 2014, the VA Office of Inspector General (OIG) Hotline received an allegation that ProCare Home Medical, Inc. (ProCare) was improperly storing and sharing VA sensitive data on contractor personal devices in violation of Federal information security standards. More specifically, the complainant alleged that ProCare was allowing its employees to use personal computers and phones to access the company computer system and download VA sensitive data, including veterans' personal health information.

What We Found

We substantiated the allegation that ProCare employees, according to its staff, accessed electronic sensitive veteran data with their personal computers from home through an unauthorized cloud-based system without encryption controls. We also noted that ProCare employees or malicious users could potentially use personal devices on an unauthorized wireless network to access sensitive veteran information. In addition, we determined that ProCare was storing sensitive hard copy and electronic veteran information in an unsecured manner at their facility. We further noted that ProCare could not provide evidence that applicable ProCare personnel had completed VA-required security awareness training or signed the Contractor Rules of Behavior, prior to receiving access to VA sensitive data.

These security deficiencies occurred because VA did not provide effective oversight of ProCare personnel to ensure the appropriate protection of veteran information at the contractor facility. As a result, veteran sensitive information was vulnerable to loss, theft, and misuse, including identity theft or fraud. We found no evidence that veteran sensitive information was compromised.

What We Recommended

We recommended the VA Northwest Health Network management assign a local Contracting Officer's Representative and Information Security Officer to provide oversight of Alaska VA Healthcare System contractors. We also recommended the VA Northwest Health Network management, in conjunction with the Assistant Secretary for Information and Technology, conduct a site assessment of ProCare information security controls to ensure compliance with VA information security requirements.

Agency Comments

The Assistant Secretary for Information and Technology and the VA Northwest Health Network Acting Director concurred with our findings and recommendations and provided an appropriate corrective action plan. We will follow up on the implementation of the corrective actions.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Objective

We conducted this review to determine the merits of a Hotline complaint alleging that a Federal contractor, ProCare Home Medical, Inc. (ProCare), was abusing its authority and engaging in information security violations by accessing and storing veteran sensitive data using unauthorized personal devices.

Allegation and Background

In December 2014, the VA Office of Inspector General (OIG) received a Hotline complaint stating that ProCare—a company that supplies home oxygen to VA—was improperly storing and sharing VA sensitive data on contractor personal devices in violation of Federal information security standards. More specifically, the complainant alleged that ProCare was allowing its employees to use personal computers and phones to access the company computer system and download VA sensitive data, including veterans' personal health information.

ProCare

VA relies on contractors to supplement its employee workforce and support its programs, missions, and operational objectives. Since September 2013, VA has contracted with ProCare, located in Anchorage, AK, to provide home oxygen services. According to the ProCare owner, they service more than 300 veterans located in Veterans Integrated Service Network 20 (VA Northwest Health Network), which includes the Alaska VA Healthcare System (AVAHS).

AVAHS

The AVAHS offers primary, specialty, and mental health outpatient care. Services are provided through a joint venture with the U.S. Air Force on nearby Elmendorf Air Force Base, as well as through purchased care arrangements with the community hospitals. This AVAHS facility also features a comprehensive Homeless Veteran Service, consisting of a Domiciliary Residential Rehabilitation Program, Veterans Industries, Compensated Work Therapy Transitional Residence Program, VA Supported Program, and Outreach. In addition to the main facility in Anchorage, AK, the AVAHS offers services in community-based outpatient clinics in Fort Wainwright, AK; Kenai, AK; Wasilla, AK; and Juneau, AK.

Other Information

- Appendix A provides details on our scope and methodology.
- Appendix B provides comments by the VA Northwest Health Network Acting Director.
- Appendix C provides comments by the Assistant Secretary for Information and Technology.

RESULTS AND RECOMMENDATIONS

Finding

Contractors Committed Information Security Violations by Accessing and Storing VA Sensitive Information on Personal Devices

In December 2014, the VA OIG Hotline received an allegation that ProCare employees were improperly storing and sharing VA sensitive data on contractor personal devices in violation of Federal information security standards. More specifically, the complainant alleged that ProCare was allowing its employees to use personal computers and phones to access the company computer system and download VA sensitive data, to include veterans' personal health information.

What We Did

In May 2015, we performed an onsite review of the ProCare facility and the Anchorage VA Medical Center to evaluate the merits of the allegation. Specifically, we interviewed ProCare management and staff; observed contractor business processes for collecting, processing, and storing VA information; and inspected their facility. We also interviewed VA personnel to gain an understanding of VA's oversight of ProCare personnel and contracting practices. We evaluated this requested information and reviewed information security controls relative to VA and Federal requirements, as well as VA policies and procedures related to the oversight of contractors.

What We Found

We substantiated the allegation that ProCare employees, according to discussions with its staff, accessed electronic sensitive veteran data with their personal computers from home through an unauthorized cloud-based system without encryption controls. While we could not analyze ProCare employees' personal cell phones and tablets, we noted ProCare staff or malicious users could potentially use these personal devices on an unauthorized wireless network to access sensitive veteran information. We also determined that ProCare was storing sensitive hard copy and electronic veteran information containing protected health information in an unsecured manner on its server and computer workstations with deficiencies associated with physical security and logical access controls that are designed to protect these data from unauthorized access and disclosure.

Criteria

VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, requires that VA contractors adequately protect the confidentiality, integrity, and availability of sensitive information processed, stored, and transmitted. Furthermore, VA's contract with ProCare requires that contractor equipment be protected to reduce the risks from environmental threats and hazards, and the opportunities for unauthorized access, use, or removal.

Logical Access Control Deficiencies

During our site visit in May 2015, ProCare staff told us they could use personal computers from home with unauthorized cloud-based software that managed client information that was accessing and transmitting sensitive VA data without encryption controls and without VA's knowledge or permission. While we did not confiscate and analyze ProCare employees' personal cell phones and tablets, we determined ProCare staff or malicious users could potentially use these personal devices on a wireless network to access sensitive veteran information and proprietary vendor information. However, we found no evidence that veteran information was compromised. Furthermore, the contractor had not implemented encryption controls on the ProCare server or any other computers storing electronic VA data. VA Handbook 6500 requires encryption for the remote use, processing, storage, or transmitting of electronic VA sensitive information. Moreover, VA's contract with ProCare requires that the contractor implement authorization and encryption controls when using and accessing sensitive veteran information.

Physical Security Control Deficiencies

At the ProCare facility, we found several hard copy file folders containing sensitive veteran information in unsecured file cabinets and lying on desktops. In addition, we observed a server cabinet, storing electronic unencrypted sensitive veteran data, located in an unsecure area near open doors leading to an outside parking lot. In this same area, we also observed an unlocked shredder bin full of ProCare client sensitive information. The figure below shows a photo of the open and unsecured doors leading to the rear parking lot.

Figure. Open and Unlocked Doors to Rear Parking Lot at the ProCare Facility

Source: Photo taken by VA OIG at the ProCare facility in Anchorage, AK, in May 2015.

Personnel Control Deficiencies

While ProCare performed background investigations on its current employees, the contractor could not provide evidence that ProCare personnel, who accessed sensitive veteran data, had completed VA-required security awareness training or signed the Contractor Rules of Behavior. VA Handbook 6500, *Contractor Rules of Behavior*, describes expected behaviors and states that contractors must complete security awareness training and sign Contractor Rules of Behavior prior to gaining access to VA information. Furthermore, the policy states that Contracting Officer's Representatives (CORs), in consultation with local Information Security Officers (ISOs), must ensure that contractors complete annual security training and ensure VA's information security requirements are met. The COR did not maintain any evidence that ProCare staff had ever performed this training and signed the Contractor Rules of Behavior. In addition, the local ISO was unavailable to respond to our inquiries and the acting ISO could not provide this information. The Handbook also states that ISOs are responsible for ensuring compliance with Federal and VA information security requirements.

Why This Happened

These security deficiencies occurred because VA did not provide effective oversight of ProCare personnel to ensure the proper safeguarding of veteran information at the contractor facility. The COR, located in the State of Washington, did not ensure that VA information security requirements were met or that ProCare personnel had completed VA information security awareness training and Contractor Rules of Behavior training prior to accessing sensitive veteran data. ProCare personnel stated that VA personnel had never been onsite or contacted them to provide any training or guidance on how they should protect sensitive veteran information. We also noted that the local ISO had not performed a site visit of the ProCare facility to help ensure compliance with VA information security requirements. When information security requirements are complete, this information is maintained in VA's Talent Management System.

What Resulted

Due to the security control deficiencies identified, veteran sensitive information was vulnerable to loss, theft, and misuse, to include identity theft or fraud. Consequently, VA must provide improved oversight of ProCare contractors to ensure the proper safeguarding and handling of sensitive veteran data.

Conclusion

The AVAHS offers primary, specialty, and mental health outpatient care. ProCare, as a VA contractor, augments this care by providing in-home oxygen services to veterans. In performing its mission, VA must provide effective oversight of contractors to ensure the proper safeguarding and handling of sensitive veteran information. However, VA has not provided effective oversight of ProCare to ensure that contractors complied with VA information security requirements or that information security training was performed. As a result, we substantiated the allegation that ProCare, according to its staff, accessed sensitive veteran data with their personal

computers without encryption controls. In addition, veteran sensitive information was made vulnerable to loss, theft, and misuse, to include identity theft or fraud. Given the risks identified at the ProCare facility, it is vital for VA to ensure that contractors receive information security training and fully address the security control deficiencies. VA also needs to identify a local COR and ISO at the AVAHS to perform periodic site visits of the ProCare facility to ensure that VA information security requirements are met.

Recommendations

1. We recommended the VA Northwest Health Network management assign a local Contracting Officer's Representative and Information Security Officer to provide oversight of Alaska VA Healthcare System contractors.

2. We recommended the VA Northwest Health Network management, in conjunction with the Assistant Secretary for Information and Technology, ensure that ProCare personnel complete VA's information security awareness training and sign the Contractor Rules of Behavior.

3. We recommended the Assistant Secretary for Information and Technology conduct a site assessment of information security controls at the ProCare facility, to include a risk assessment to determine the extent that any sensitive veteran data may have been compromised and, if so, with appropriate corrective action, to ensure compliance with VA and Federal information security requirements.

Management Comments and OIG Response

The Assistant Secretary for Information and Technology and the VA Northwest Health Network Acting Director concurred with our findings and recommendations and stated that they have addressed or planned to address all our recommendations by March 2016. A COR was appointed and is working closely with the Veterans Integrated Service Network (VISN) 20 COR to monitor the contract vendor's performance and ensure they meet the VA Standards for privacy and information security. The VISN 20 ISO has been assigned to provide oversight of Alaska VA Healthcare System contractors with oversight from the Network 20 ISO. Although the local ISO was not available to provide evidence of training within VA's Talent Management System at the time of our site visit, VA informed us that information security training occurred in January 2016. We confirmed the existence of training certificates for 43 of 46 Procare staff on July 6, 2016. Based on the information provided and validation procedures performed, VA has taken sufficient actions to address Recommendations 1 and 2 and we have closed those recommendations.

The Assistant Secretary for Information and Technology asserted that VA found no evidence of ProCare employees using personal devices to access veteran sensitive data. However, we noted from interviews with ProCare

staff that they could access electronic sensitive veteran data with their personal computers from home through an unauthorized cloud-based system that did not use encryption controls. We will monitor the Office of Information and Technology's and VA Northwest Health Network's follow-up on the implementation of our remaining recommendations until all proposed actions are completed. Appendix B contains the full text of the VA Northwest Health Network Acting Director's comments. Appendix C contains the full text of the Assistant Secretary's comments.

Appendix A Scope and Methodology

Scope and Methodology

We conducted our review from February 2015 to June 2016. To conduct this review, we performed a site visit of the ProCare facility and the Anchorage VA Medical Center to evaluate the merits of the allegation. Specifically, we interviewed ProCare management and staff, observed contractor business processes for collecting, processing, and storing VA information, and inspected their facility. We also interviewed VA personnel to gain an understanding of VA's oversight of ProCare personnel and contracting practices. We evaluated this requested information and reviewed information security controls relative to VA and Federal requirements. We also examined applicable VA and Federal information security requirements, as well as VA policies and procedures related to the oversight of contractors.

Data Reliability

We did not use computer-processed data for this review. We relied on our site visit observations, review of documentation, and interviews. We determined these procedures to be reliable as related to the objectives of this 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.*

Appendix B Management Comments–VA Northwest Health Network Acting Director

Department of Veterans Affairs

Memorandum

Date: February 23, 2016

From: Acting Network Director, VISN 20 (496/10N20)

Subj: VAOIG-Draft Report: Review of Alleged Contractor Information Security Violations

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

1. I have reviewed the draft report and concur with the report's recommendations for recommendation 1. Below are the actions taken in regards to this recommendation.

2. [redacted] was provided a letter of delegation on Oct. 1, 2015, and has been working closely with both, [redacted], ISO), and [redacted] The VISN 20 [redacted], on monitoring the contract vendor's performance and ensuring the meet the VA Standards for privacy and information security. (b)(6)

3. At the direction of [redacted] ISO) the vendor completed the Security Training on Jan. 13, 2016. The Vendor is now compliant with the required Security Training. (b)(6)

4. Attached please find a copy of the contract amendment, the letter of delegation for [redacted] and a copy of the ProCare TMS Training completion List for 2-16. (b)(6)

5. Thank you for the opportunity to review the recommendations and respond. If you have any questions, please contact the VISN Prosthetic Network Manager, [redacted] at 360-567-[redacted] (b)(6)

(Original signed by:)

MICHAEL J. MURPHY, FACHE

Attachments*
- Contract Amendment
- Letter of delegation
- Copy of ProCare TMS Training completion list for 2-16.

**OIG Note: The attachments were not included in this report. Copies may be obtained from the OIG Information Officer.*

Appendix C Management Comments–Assistant Secretary for Information and Technology

Department of Veterans Affairs

Memorandum

Date: February 9, 2016

From: Assistant Secretary for Information and Technology (005)

Subj: Draft Report, Review of Alleged Contractor Information Security Violations

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

Thank you for the opportunity to review the findings and recommendations in the Office of Inspector General (OIG) draft report, *"Review of Alleged Contractor Information Security Violations*" in Anchorage, AK. The Office of Information and Technology submits the attached written comments. If you have any questions, feel free to contact me at (202) 461-6910 or have a member of your staff contact Brian Burns, Deputy Assistant Secretary for Information Security at (202) 632-9070.

(Original signed by:)

LaVERNE H. COUNCIL

Attachment

Attachment

U.S. Department of Veteran Affairs
Office of Information and Technology (OI&T)
Comments on OIG Draft Report:
"Review of Alleged Contractor Information Security Violations"

OIG Recommendation 1: We recommended the VA Northwest Health Network management assign a local Contracting Officer Representative and Information Security Officer to provide oversight of Alaska VA Healthcare System contractors.

Response: Concur. OI&T requests closure of the Information Security Officer (ISO) portion of this recommendation. The VISN 20 ISO has been assigned to provide oversight of Alaska VA Healthcare System contractors with oversight from the Network 20 ISO. Documentation to support closure is attached.

OIG Recommendation 2: We recommended the VA Northwest Health Network management, in conjunction with the Assistant Secretary for Information and Technology, ensure that ProCare personnel complete VA's information security awareness training and sign the Contractor Rules of Behavior.

Response: Concur. OI&T requests closure of this recommendation. All required VA training for patient information protection was completed by ProCare personnel via VA's Talent Management System as of 6 January 2016. This training includes acceptance of the contractor Rules of Behavior. Copies of the ProCare personnel training certificates is attached to support closure. OI&T will continue to monitor compliance with the annual security awareness training and Rules of Behavior.

OIG Recommendation 3: We recommended the Assistant Secretary for Information and Technology conduct a site assessment of information security controls at the ProCare facility, to include a risk assessment to determine the extent that any sensitive veteran data may have been compromised and, if so, with appropriate corrective action, to ensure compliance with VA and Federal information security requirements.

Response: Concur. The VA Northwest Health Network management, in conjunction with the Assistant Secretary for Information and Technology, conducted a site assessment on 9 December 2015 to evaluate the security controls at the ProCare facility. That assessment found that corrective actions have been implemented, with the following results:

1. Back doors were locked, and all employees have been informed this is mandatory.
2. All hard copy files are in a locked file cabinet in a secure area when not in direct use. No hard copy files were in view during the visit.
3. Areas containing VA information are secure and require sign-in and a visitor pass; furthermore appropriate escort requirements are in place.
4. All electronic VA patient information is stored in an appropriate password-protected system.
5. Shred bins are locked and in secure areas only.
6. Use of email for transmitting VA information is encrypted and used by limited staff. The method was approved by the OI&T Information Security Officer. Otherwise only fax, telephone, and hard copy information transfer is used.

The vendor has completed a Contractor Security Control Assessment (CSCA), which has a pending action for a 1st Quarter Risk Assessment to be completed. The target date for compliance with the CSCA requirements is March 31, 2016. Thereafter, the VA Northwest Health Network management, in conjunction with the Assistant Secretary for Information and Technology, will conduct an annual site visit to ensure continued compliance.

Target Completion Date: March 31, 2016

OIG Draft Report Finding: "As a result, we substantiated the allegation that ProCare, according to their staff, accessed sensitive veteran data with their personal computers without encryption controls. Additionally, veteran sensitive information was made vulnerable to loss, theft, and misuse to include identity theft or fraud." – Page 9, Conclusion

OI&T Comments: A review by OI&T found no evidence of ProCare employees using personal devices to access veteran sensitive data. However, as reflected in the OIG report, that review did identify the presence of a contractor wireless network that could be used to gain unauthorized access to veteran data. An OI&T risk assessment determined that records that were potentially handled improperly were hard copies of medication-related home oxygen prescribed records.

Appendix D 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 Jack Henserling Ryan Nelson Richard Wright

Appendix E 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

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
U.S. Senate: Lisa Murkowski, Daniel Sullivan
U.S. House of Representatives: Don Young

This report is available on our Web site at www.va.gov/oig.