DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS BENEFITS ADMINISTRATION

Mishandling of Veterans' Sensitive Personal Information on VA Shared Network Drives

REVIEW | REPORT #19-06125-218 | OCTOBER 17, 2019

The mission of the Office of Inspector General is to serve veterans and the public by conducting effective oversight of the programs and operations of the Department of Veterans Affairs through independent audits, inspections, reviews, and investigations.

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

The VA Office of Inspector General (OIG) conducted this review in response to a hotline allegation that veterans' sensitive personal information was stored on shared network drives on the VA Enterprise network and was likely accessible to other network users. The allegation was made by a veterans service organization (VSO) officer working with veterans served by the Milwaukee, Wisconsin, VA Regional Office (VARO). Accredited VSO officers have access to the network to assist veterans with filing VA disability claims through the Veterans Benefits Management System (VBMS), the web-based electronic claims-processing system of the Veterans Benefits Administration (VBA).

Sensitive personal information—any information about an individual that is maintained by VA and can be linked to that individual—is protected by law and VA policy. U.S. laws require appropriate administrative, physical, and technical safeguards to protect personal information and limit the uses and disclosures of that information without the individual's authorization. VA policy requires VA information system users who access sensitive personal information as part of their official duties to avoid its unauthorized disclosure and prohibits other users from accessing the information without a business need.

What the Review Found

The OIG team found that veterans' sensitive personal information was left unprotected on two shared network drives, where it was accessible to VSO officers who did not represent those veterans. Senior Office of Information and Technology (OIT) representatives told the team that other authenticated network users with access to the shared drives also could have accessed that information regardless of their business need. The OIG determined that mishandling this sensitive personal information was a national issue because the problem was not limited to the Milwaukee VARO. Authorized users, regardless of their location, who remotely connected to VA's network could have had access to the same shared network drives.

The mishandling of sensitive personal information occurred for three reasons. First, certain users were knowingly or inadvertently negligent in their use of shared network drives to store veterans' sensitive data despite VA security policy prohibiting such activity. Second, no technical controls were in place to prevent negligent users from storing sensitive personal information on the shared network drives. Third, due to a lack of oversight, OIT and VBA personnel failed to discover and remove any sensitive personal information stored on shared network drives.

Without better protection, veterans and VA are at risk. Veterans are at significant risk of unauthorized disclosure and misuse of their sensitive personal information. This has the potential to expose veterans to fraud and identity theft. Also, if a breach of sensitive personal information

were to occur, VA could incur the expense of notifying and offering credit protection services to individuals whose sensitive personal information was involved. VA could also lose credibility with veterans who trust that their sensitive personal information is being appropriately secured. Although VA's Data Breach Response Service determined that the storing of sensitive personal information on the shared network drives did not meet the criteria for a data breach and did not require notifications, it is important that VA improves its controls and oversight to mitigate future risk.[1]

What the OIG Recommended

The OIG recommended that the assistant secretary for information and technology and the under secretary for benefits provide remedial training to users on the safe handling and storage of veterans' sensitive personal information on network drives. The OIG also recommended the assistant secretary for information and technology establish technical controls to ensure users cannot store veterans' sensitive personal information on shared network drives. Furthermore, the OIG recommended the assistant secretary for information and technology implement improved oversight procedures, including facility-specific procedures, to ensure veterans' sensitive personal information is not being stored on shared network drives.

Management Comments

The assistant secretary for information and technology and the under secretary for benefits concurred with all three recommendations and provided corrective action plans that are responsive to the recommendations. The OIG considers Recommendation 2 closed based on actions reported and documentation provided. The OIG will monitor implementation of the planned actions for Recommendations 1 and 3 and will close the recommendations when the OIG receives sufficient evidence demonstrating progress in addressing the identified issues.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

[1] VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information,* March 12, 2019. The term "breach" means the potential acquisition, access, use, or disclosure of VA sensitive personal information in a manner not permitted by law or VA policy which compromises the security or privacy of the information. A breach excludes the unintentional acquisition, access, or use of sensitive personal information by a VA workforce member that does not result in the further use or disclosure in a manner not permitted by law or VA policy, or when there is a low probability the information has been compromised.

Contents

Abbreviations

ISSO	information system security officer
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
PHI	protected health information
PII	personally identifiable information
VARO	VA regional office
VBA	Veterans Benefits Administration
VBMS	Veterans Benefits Management System
VHA	Veterans Health Administration
VSO	veterans service organization

Introduction

The VA Office of Inspector General (OIG) conducted this review to assess a September 2018 hotline allegation from a Wisconsin veterans service organization (VSO) officer, working with veterans served by the Milwaukee, Wisconsin, VA Regional Office (VARO), that veterans' sensitive personal information was stored on the VA Enterprise network, where it was likely accessible by other users.[2] The complainant reported that personally identifiable information (PII) and protected health information (PHI) were unprotected on shared network drives. Any authorized network users, such as VSO officers or VBA employees, could potentially access the PII or PHI even without a business need. The OIG's objective was to evaluate whether veterans' sensitive personal information was effectively protected on the VA network as required. If this information is not properly protected, veterans are at risk of unauthorized access and potential misuse, such as medical identity theft.[3]

VSO Officer Roles and Responsibilities

VSOs offer veterans a variety of services, including assistance with applying for VA benefits. VA accredits officers from recognized VSOs—for example, the American Legion and Veterans of Foreign Wars—so that they are equipped to help prepare, present, and prosecute veterans' benefit claims.[4] Remotely located VSO officers use a VA-issued remote access program to connect to the Veterans Benefits Management System (VBMS), the web-based electronic claims-processing system of the Veterans Benefits Administration (VBA).

Types of Sensitive Personal Information

Sensitive personal information, which comes in many forms, should always be protected. Its protection is covered under laws including the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[5] VA's Privacy Program also requires

[2] Sensitive personal information is defined in 38 United States Code (U.S.C.) § 5727(19) and includes the following: (i) education, financial transactions, medical history, and criminal or employment history; and (ii) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, and biometric records. The VA Enterprise network consists of hardware, software, and delivery platforms on which VA mission and general support systems and capabilities are deployed. It is described at "VA EA Networks and Infrastructure Domain," VA website, accessed March 25, 2019, https://www.ea.oit.va.gov/EAOIT/VA_EA/VAEA_Networks-and-Infrastructure-Domain.asp.

[3] The OIG team only reviewed network drives that contained veterans' sensitive personal information. It did not observe third-party protected information.

[4] "VA Accreditation Program: How to Apply for VA Accreditation as an Attorney or Claims Agent," VA website, accessed February 28, 2019, https://www.va.gov/OGC/docs/Accred/HowtoApplyforAccreditation.pdf.

[5] Privacy Act of 1974, 5 U.S.C. § 552a (1974); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996), as implemented by 45 C.F.R., parts 160 and 164.

appropriate administrative, physical, and technical safeguards to protect personal information and limit the uses and disclosures of such information without an individual's authorization.

VA considers sensitive personal information and PII interchangeable. It uses both terms to refer to any information about an individual that is maintained by VA and can be linked to that individual—for example, medical records maintained by VA that can be linked to an individual through the individual's name, social security number, or date and place of birth. VA considers PHI a subcategory of PII. PHI is health and demographic data transmitted by, or maintained in, electronic or any other form or medium that can be used to identify an individual.[6]

Handling of Sensitive Personal Information

VA Directive 6502, *VA Enterprise Privacy Program*, requires that PII be kept confidential and properly controlled. All VA information system users must comply with all related policies, procedures, and practices.[7] All users of VA information must also conduct themselves in accordance with the annually signed rules of behavior concerning the disclosure or use of information.[8] Accordingly, VA employees and contractors must comply with the following responsibilities when handling sensitive personal information:

- Accessing records containing PII only when the information is needed to carry out their official duties
- Disclosing PII about veterans, employees, contractors, volunteers, interns, and business associates only in accordance with applicable federal privacy laws, regulations, and VA policies and procedures
- Taking privacy awareness training provided or approved by the VA Privacy Service on an annual basis
- Taking any role-specific privacy training provided or approved by the VA Privacy Service that is applicable to their official duties
- Reporting all actual or suspected breaches involving PII to their privacy officers within one hour of discovery[9]

According to VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, a breach refers to the potential acquisition, access, use, or disclosure of VA

[6] VA Directive 6502, *VA Enterprise Privacy Program*, May 5, 2008, page 5, item 1.b. "Note," page 22, item 5.f and page 23, item 5.g.

[7] VA Directive 6500, *VA Cybersecurity Program*, January 23, 2019, page 29, item 3.s.(2).

[8] The VA Rules of Behavior are delineated in VA Handbook 6500, *Risk Management Framework for VA Information Systems—Tier 3: VA Information Security Program*, app. D, March 10, 2015.

[9] VA Directive 6502, page 6, item 2.c. and d, and page 19, item 3.n.

sensitive personal information in a manner not permitted by law or VA policy that compromises the security or privacy of the information. If the acquisition, access, or use of sensitive personal information by a VA workforce member is unintentional and does not result in the further use or disclosure in a manner not permitted by law or VA policy, or when there is a low probability the information has been compromised, it is not a breach.[10]

VA Handbook 6500.2 also establishes procedures for managing breaches. Subject to the handbook procedures, VA's Data Breach Response Service determines whether the reported event constitutes a breach that must be reported to the Department of Health and Human Services under the HIPAA Breach Notification Rule, and whether VA will notify the involved individuals of the event and offer them credit protection services.[11]

[10] VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, March 12, 2019, pages 22–23, sec. 5, "VA Criteria for Breach and Risk Assessment."

[11] VA Handbook 6500.2, page 1, item 2.a and page 4, item 1.

Results and Recommendations

Finding: Veterans' Sensitive Personal Information Was Inappropriately Stored on Shared Network Drives

The OIG substantiated the allegation that veterans' sensitive personal information was mishandled and left unprotected on shared network drives, where it was accessible to VA network users. Specifically, the OIG found that veterans' PII and PHI were stored on two shared network drives that were also accessible to VSO officers who did not represent those veterans. As VA information system users, VSO officers should not be able to access veterans' sensitive personal information without written permission or a business need.

The OIG found the mishandling of information occurred for three reasons: (1) user negligence, deliberately or inadvertently, through storing sensitive personal information on shared network drives; (2) lack of technical safeguards to prevent inappropriate storage; and (3) inadequate oversight to ensure compliance with VA rules of behavior.

Without better protection of sensitive personal information, veterans and VA are at risk. Unauthorized access to sensitive personal information can lead to improper disclosures of veterans' and other parties' information and can cause undue hardship for those involved. If a breach occurs, VA is responsible for notifying the involved individuals and offering credit protection services.[12] The VA's Data Breach Response Service ultimately determined that the presence of PHI or PII on the shared network drives did not meet the criteria for a data breach and therefore did not require notifications. However, without improvements, VA continues to be at risk of future disclosure or misuse.

What the OIG Did

In December 2018, the OIG team assessed the hotline allegation by interviewing the complainant, reviewing the shared drives for sensitive personal information, and meeting with information technology (IT) officials at the Milwaukee, Wisconsin, VARO to discuss observations.

The OIG team subsequently reviewed privacy security requirements and controls. The team also interviewed VSO officers in the VARO area and observed their system network access. In addition, the team interviewed Milwaukee VARO managers and staff, system owners, information system security officers (ISSOs), and privacy officers to identify responsibilities and oversight. The team also interviewed leaders and staff from the VA Office of Information and Technology's (OIT) Enterprise Security Operations and IT Operations and Services, the VBA privacy officer, the director of the VHA Privacy Compliance Assurance office, VHA Privacy

[12] VA Handbook 6500.2, page 25, item 7.a.(1).

and Records Assessment Division leaders and staff, and the director of the OIT Office of Information Security's Security Assessment & Validation Division. These interviews helped clarify the processes used to handle and store sensitive personal information and identify opportunities for improvement.

This report discusses the following issues related to the OIG's finding:

- Veterans' sensitive personal information was inappropriately stored on shared network drives.
- Multiple factors led to inappropriate handling of sensitive personal information.
- Mishandling sensitive personal information put veterans at risk.

Veterans' Sensitive Personal Information Was Inappropriately Stored on Shared Network Drives

In January 2019, the OIG team conducted a site visit and met with the complainant. During the visit, the complainant demonstrated how to access the VA network and data remotely using an authorized remote access program. After completing the login process, the complainant was automatically connected to VA shared network drives, and the OIG team noted that folders on two of the shared drives contained unprotected sensitive personal information.

The OIG team noted the information location, contents, and dates. The files the OIG team observed contained medical records, correspondence about medical examinations and disability claims decisions, and veterans' statements in support of their claims. The files contained a variety of sensitive veteran information including names, addresses, dates of birth, and phone numbers. These files dated back as far as 2016 and were available to any network users with permission to access the drives, regardless of their business need to do so.

In addition, the OIG team observed VSO officers associated with the Milwaukee VARO were connecting to VA's network both locally and remotely. The team saw that the VSO officers who connected to the VA network locally did not have access to either of the shared network drives with sensitive information folders that were accessible at the complainant's work site. However, VSOs who connected to VA's network remotely could access these drives. The reason for this difference is that VBA assigns network drives distinctly for local and remote users. IT operations personnel explained to the OIG team that the shared network drives were VBA resources and these drives were automatically connected to a remote user when the user logged onto VA's network. An IT operations official further explained that users could access the shared network drives without using the remote access program if they knew how to manually access the drives. The OIG team confirmed manual accessibility to the shared network drives while connected to the local network and identified files with veterans' sensitive information.

During the site visit, the complainant also noted reporting a similar issue to the VARO ISSO in 2016, who had entered the incident as a ticket in VA's Privacy and Security Event Tracking System. The OIG team further inquired about the incident and found that VA opened the security ticket in May 2016 and closed it in February 2017, after OIT decommissioned the file servers involved to resolve the ticket. In January 2019, the Milwaukee VARO ISSO opened a new ticket regarding the personal information on the shared drives. The VA Data Breach Response Service closed that ticket on March 11, 2019, declaring that all PII and PHI located on the shared drives had been removed and only one shared folder remained open for users as it was necessary to maintain working conditions.

The OIG team determined that mishandling veterans' sensitive personal information was a national issue because security concerns were not limited to the Milwaukee VARO. Specifically, senior OIT representatives said any VBA user with permission to access VA's network remotely would have had access to the shared drives hosting veterans' sensitive personal information. IT operations personnel stated that approximately 25,000 remote access users could have accessed the shared network drives.

Multiple Factors Led to Inappropriate Handling of Sensitive Personal Information

The OIG team found that several issues contributed to the failure to adequately protect veterans' sensitive personal information. These included user negligence, lack of technical controls, and inadequate oversight.

User Negligence

Based on interviews and reviews of existing business processes, the OIG team noted that some of the users storing personal information on the network shared drives were negligent, knowingly or inadvertently using shared network drives to store veterans' sensitive personal information despite VA security policy that prohibits such activity.

In accordance with VA Directive 6500, VA security requirements for managing sensitive information include annual security awareness training and agreeing to comply with the rules of behavior.[13] The training and rules of behavior include the following requirements:

- Users will only provide access to sensitive information to those who need it for their professional duties, including only posting sensitive information to web-based collaboration tools restricted to those who have a need to know and when proper safeguards are in place for sensitive information.

[13] VA Directive 6500, page 29, item 3.s.

- Users will protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, and will use encryption products approved and provided by VA to protect sensitive data.
- Users will protect sensitive personal information aggregated in lists, databases, or logbooks and will include only the minimum necessary sensitive personal information to perform a legitimate business function.

Several VA senior representatives said providing training or education was an important part of addressing this security issue. One representative said a solution was enhanced training, especially at facilities; another mentioned additional or custom training to reiterate expectations and raise security awareness of sensitive personal information.

Recommendation 1 addresses the need for VA's assistant secretary for information and technology and the under secretary for benefits to provide corrective and remedial training to users on the safe handling of sensitive personal information and shared drives.

Lack of Technical Controls

The OIG team found that technical controls were not in place to prevent users from storing sensitive personal information on the shared network drives.[14] VA Directive 6502 requires system owners to assure that all proper measures are taken to ensure confidentiality of PII on all systems for which they are responsible, and that information owners collaborate with the system owners to ensure that data is being used according to uses set forth in the System of Records Notice.[15] The responsibility for establishing, maintaining, and monitoring department-wide information security policies, procedures, control techniques, training, and inspection requirements as elements of the department's information security program is assigned to the assistant secretary for information and technology.[16]

According to the director of the Office of Information Security's Security Assessment & Validation Division, VA does not currently have manual or automated processes in place to scan network drives to identify unauthorized use and storage of PHI or PII. In response to the unauthorized storage of sensitive personal information on the shared network drives, security officials have discussed planned changes to upgrade the network shared drives to make them mostly read-only, except where applications require write access.[17] The security officials said they are contemplating remedial training for users, migrating the shared drives to a more secure

[14] The National Institute of Standards and Technology (NIST) defines technical controls as security safeguards or countermeasures for an information system that are primarily implemented and executed through mechanisms contained in the hardware, software, or firmware components of the system.

[15] VA Directive 6502, page 18, items 3.l.(1) and 3.m.(1) applies to VSOs and VA employees.

[16] VA Directive 6500, page 20, item 3.c.(1) and 38 U.S.C. § 5723(b)(1).

[17] Write access grants the ability to read and modify files, which can include creating and deleting them.

environment on the network, and monitoring the drives periodically for sensitive personal information.

Recommendation 2 addresses the need for VA's assistant secretary for information and technology to establish technical controls to ensure users cannot store sensitive personal information on shared network drives.

Inadequate Oversight

The OIG team concluded that VA had no effective oversight in place to detect if users had violated the rules of behavior, such as storing sensitive personal information on the shared network drives. The OIG team determined that this lack of oversight occurred because VA did not have specific procedures for reviewing shared VA network drives for sensitive personal information. Despite existing policies and procedures to ensure privacy and security of veterans' sensitive data, users can deliberately or inadvertently violate security requirements that are defined in VA security policies and user rules of behavior. Currently, no VBA policy requires facility privacy officers and ISSOs to conduct privacy self-assessments or reviews that might have identified the information the OIG team observed. For example, while VA Directive 6502 states that privacy reviews shall be conducted as required, there was no formal instruction for privacy officers and ISSOs at VBA facilities to conduct privacy assessments or review shared VA network drives for sensitive personal information.[18]

According to VHA and VA privacy officials, VHA currently conducts periodic privacy and records management reviews of VHA, VBA, the National Cemetery Administration, the Board of Veterans' Appeals, and VA staff offices.[19] In contrast, the OIG noted during its review that VA had not implemented self-assessments for its privacy and records management programs outside of VHA. On April 5, 2019, the VA chief information officer approved a memorandum establishing yearly self-assessments of records management and privacy compliance for administrations, VA Central Office staff offices, and facilities, not just VHA. Consistent with the lack of a self-assessment program for non-VHA facilities prior to the April 2019 memorandum, the Milwaukee VARO privacy officer informed the OIG team that the facility had not been required to perform self-assessments and was scheduled for an assessment by the VHA Privacy and Records Assessment Division in August 2019.

Recommendation 3 addresses the need for VA's assistant secretary for information and technology to implement improved oversight procedures, including specific facility-level

[18] VA Directive 6502, page 7, item 2.k.

[19] Privacy reviews are mandated by VA Directive 6502, page 7, item 2.k. Records management reviews are mandated by VA Handbook 6300.1, *Records Management Procedures*, March 24, 2010, page 17, item 3. Current policy is to audit a third of facilities per year.

procedures, to ensure that sensitive personal information is not being stored on shared network drives.

Conclusion

The inadequate protection of sensitive personal information places veterans' data at risk and could undermine the credibility of VBA and VSOs in positions of trust. Veterans should have confidence that their sensitive personal information is handled strictly in accordance with federal laws and VA regulations.

Failing to secure sensitive personal information could result in avoidable VA expenses. If VA's Data Breach Response Service had determined that the unsecured data resulted in a reportable breach, VA would have been required to notify the subjects and offer them credit protection services. Although VA's Data Breach Response Service determined that the event did not meet the criteria for a data breach and therefore did not require notifications, the data were put at unnecessary risk. This determination of the lack of a specific breach notwithstanding, VBA and the OIT must provide adequate training, establish appropriate controls, and develop oversight protocols to help prevent improper disclosures and future breach incidents.

Federal law and VA information security and privacy programs have clear requirements to adequately protect sensitive personal information, yet the OIG substantiated the allegation that veterans' sensitive personal information left unprotected on shared network drives was accessible to up to 25,000 VA network users who did not all have a business need to access it.

Until VA officials take steps to guard against user negligence, implement technical controls that prevent users from storing sensitive personal information on shared network drives, and issue oversight procedures to adequately monitor shared network drives, veterans' sensitive personal information remains at risk.

Recommendations 1–3

1. The assistant secretary for information and technology and the under secretary for benefits provide remedial training to users on the safe handling and storage of sensitive personal information on network drives.
2. The assistant secretary for information and technology establishes technical controls to ensure users cannot store sensitive personal information on shared network drives.
3. The assistant secretary for information and technology implements improved oversight procedures, including specific facility-level procedures, to ensure that sensitive personal information is not being stored on shared network drives.

Management Comments

The assistant secretary for information and technology concurred with all three recommendations and the under secretary for benefits concurred with Recommendation 1. For Recommendation 1, the assistant secretary for information and technology and the under secretary for benefits reported that VBA and OIT worked together to develop a quick reference guide regarding the use of shared network drives, which was distributed to all VBA field offices. In addition, VBA and OIT stated that local privacy and records management officers will provide additional guidance and training at the local level as needed. For Recommendation 2, VBA deferred to OIT. The assistant secretary for information and technology reported that OIT's IT Operations and Services, Infrastructure Operations, applied a permission change to the public drives making them read-only for VBA Citrix Access Gateway users. OIT provided documentation indicating action has been completed on all affected shared drives. For Recommendation 3, VBA deferred to OIT. The assistant secretary for information and technology reported that while VA currently has oversight procedures in place through policy and training, to strengthen controls VA will explore the option for a central solution to assist VA in detecting if users have violated policy by storing personal sensitive information on shared network drives. The target completion date for this effort will depend on project approval, funding, and resource availability. VA will provide additional details at the time of the report's 90-day follow-up.

OIG Response

The assistant secretary for information and technology's and the under secretary for benefits' comments and actions are responsive to the recommendations. OIT and VBA requested the OIG close Recommendation 1. Recommendation 1 remains open. The OIG will follow up to assess VA's efforts to provide guidance and training at the local level. OIT requested the OIG close Recommendation 2. The OIG considers Recommendation 2 closed based on actions reported and documentation provided. The OIG will also monitor the implementation of the planned actions for Recommendation 3 and will close Recommendations 1 and 3 when the OIG receives sufficient evidence demonstrating progress in addressing the identified issues.

Appendix A: Background

Remote Access Using Citrix Access Gateway

VBA allows VSOs to represent claimants for VA benefits. VSO officers are given remote access to the records of the individuals they represent. The officers are subject to a background investigation before being given access to sensitive personal information. They are also required to complete the VA Privacy and Information Security Awareness training and agree to the rules of behavior annually. VSO officers who have permission to do so access data through the Citrix Access Gateway. The gateway is a remote access solution for users with permission to access VA's network. The gateway provides a method of accessing VA applications without having to install the application on the user's equipment. Application client software is installed on a portal server, and it communicates with application server software on servers within the organization. The portal server communicates securely with the portal client as needed.

The gateway is an example of a remote access method using an application portal. The National Institute of Standards and Technology (NIST) describes an application portal in Special Publication 800-46:[20]

> A *portal* is a server that offers access to one or more applications through a single centralized interface.… [P]ortals protect information between client devices and the portal, and they can provide authentication, access control, and other security services.… A portal server transfers data to the client device as rendered desktop screen images or web pages, but data is typically stored on the client device much more temporarily than data for a tunneled solution is. (However, portals can be configured to allow clients to download content from the portal and store it on the client device or other locations outside the secure remote access environment.) Having the application client software centralized gives an organization more control over how the software and data is secured as opposed to more distributed remote access solutions. Portals limit the access that a teleworker has to particular application clients running on the portal itself. Those applications further limit the access the teleworker has to the servers inside the network.

[20] National Institute of Standards and Technology SP 800-46, Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, July 2016, page 7, item 2.2.2, "Application Portals."

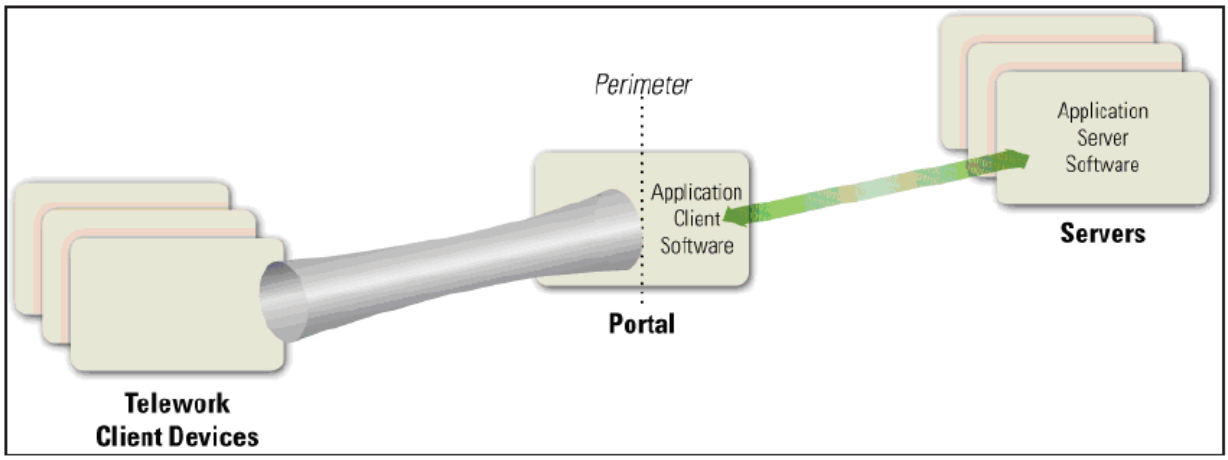

Figure A.1. *Portal architecture for remote access*
Source: National Institute of Standards and Technology SP 800-46, Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, July 2016, page 7, item 2.2.2 "Application Portals."*

Appendix B: Scope and Methodology

Scope

The OIG team conducted its work from December 2018 through June 2019.

Methodology

To accomplish its objective, the OIG team identified and reviewed applicable laws, regulations, VA policies, operating procedures, and guidelines related to managing sensitive data. The OIG team performed site visits in January 2019 that included the complainant's workplace and the following VSOs at the Milwaukee VARO:

- American Legion
- Disabled American Veterans
- The Military Order of the Purple Heart
- Paralyzed Veterans of America
- Veterans of Foreign Wars
- Wisconsin Department of Veterans Affairs

The OIG team reviewed privacy security requirements and controls. The team interviewed VSO officers in the VARO area and observed their system network access. The OIG team interviewed Milwaukee VARO managers and employees, system owners, ISSOs, and privacy officers to identify responsibilities and oversight activities. To understand the processes for handling and storing sensitive information and to identify opportunities for improvement, the team also interviewed leaders and staff from VA's OIT Enterprise Security Operations and IT Operations and Services and the VHA Privacy and Records Assessment Division, the VBA privacy officer, the director of the VHA Privacy Compliance Assurance office, and the director of the OIT Office of Information Security's Security Assessment & Validation Division.

Fraud Assessment

The OIG team assessed the risk that fraud, violations of legal and regulatory requirements, and abuse could occur during this review. The OIG team exercised due diligence in staying alert to any fraud indicators by taking actions such as engaging the OIG's Office of Investigations and reviewing possibly relevant OIG hotline complaints and concerns to identify potential indicators. The OIG did not identify any instances of fraud or potential fraud during this review.

Data Reliability

The OIG team did not use computer-processed data.

Government Standards

The OIG 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 OIG's findings and conclusions based on the OIG's review objective.

Appendix C: Management Comments—Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer

Department of Veterans Affairs

MEMORANDUM

Date: Sep 18, 2019

From: Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer (005A)

Subj: OIG Draft Report, Audit of VA's Mishandling of Veterans' Sensitive Personal Information on VA Shared Network Drives - Project No. 2019-06125-CT-0001

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

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, Audit of VA's Mishandling of Veterans' Sensitive Personal Information on VA Shared Network Drives (Project No. 2019-06125-CT-0001).

The Office of Information and Technology concurs with OIG's findings and recommendations and submits the attached written comments. For questions regarding OIT's comments on the draft report, please contact Martha Orr, Deputy Chief Information Officer for Quality, Performance, and Risk at (202) 461-5139.

/s/

Dominic Cussatt

Attachment

Department of Veterans Affairs (VA) Comments to Office of Inspector General (OIG) Draft Report,

Mishandling of Veterans' Sensitive Personal Information on VA Shared Network Drives [Project No. 2019-06125-CT-0001]

OIG Recommendation 1: The Assistant Secretary for Information and Technology and the Under Secretary for Benefits provide remedial training to users on the safe handling and storage of sensitive personal information on network drives.

Comments: Concur. The Veterans Benefits Administration (VBA) worked with the Office of Information and Technology (OIT) to develop a quick reference guide regarding utilizing shared network drives and has distributed the guide to all VBA field offices (Attachment A). Local Privacy and Record Management Officers will provide additional guidance and training at the local level as needed. The Department of Veterans Affairs (VA) requests closure of this recommendation.

OIG Recommendation 2: The Assistant Secretary for Information and Technology establishes technical controls to ensure users cannot store sensitive personal information on shared network drives.

Comments: Concur. OIT's IT Operations and Services, Infrastructure Operations has applied read-only permissions to the public drives for VBA Citrix Access Gateway, or CAG, users. The initial roll-out for this effort began on February 15, 2019. Change Order CO528739FY19 is attached for documentation purposes (Attachment B). This action has been completed and the affected shared drives are now read-only. VA requests closure of this recommendation.

OIG Recommendation 3: The Assistant Secretary for Information and Technology implements improved oversight procedures, including specific facility-level procedures, to ensure that sensitive personal information is not being stored on shared network drives.

Comments: Concur. While VA currently has oversight procedures in place through policy and training, to strengthen controls VA will explore the option for a central solution to identify sensitive information, auditing, and visibility on shared network drives. Such a solution would assist VA in detecting if users have violated policy by sharing personal sensitive information on shared network drives on the VA Enterprise network. The target completion date will depend on project approval, funding, and resource availability. VA will provide additional details at the time of the report's 90-day follow-up.

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

Appendix D: Management Comments—Under Secretary for Benefits

Department of Veterans Affairs

MEMORANDUM

Date: September 18, 2019

From: Under Secretary for Benefits (20)

Subj: OIG Draft Report – Review of Mishandling of Veterans' Sensitive Personal Information on VA Shared Network Drives [Project No. 2019-06125-CT-0001] VIEWS 01446792

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

1. Attached is VBA's response to the OIG Draft Report: Review of Mishandling of Veterans' Sensitive Personal Information on VA Shared Network Drives.

2. Questions may be referred to Ruma Mitchum, Program Analyst, at (202) 632-8987.

/s/

Paul R. Lawrence, Ph.D.

Attachments

Veterans Benefits Administration (VBA)

Comments on OIG Report

Review of Mishandling of Veterans' Sensitive Personal Information on VA Shared Network Drives [Project No. 2019-06125-CT-0001]

The Veterans Benefits Administration (VBA) concurs with OIG's findings and provides the following comments in response to the recommendations in the draft report:

Recommendation 1: The Assistant Secretary for Information and Technology and the Under Secretary for Benefits provide remedial training to users on the safe handling and storage of sensitive personal information on network drives.

VBA Response: Concur. The Veterans Benefits Administration (VBA) worked with the Office of Information and Technology (OIT) to develop a quick reference guide regarding utilizing shared network drives and has distributed this to all VBA field offices (Attachment A). Local Privacy/Record Management Officers will provide additional guidance and/or training at the local level as needed. The Department of Veterans Affairs (VA) requests closure of this recommendation.

Recommendation 2: The Assistant Secretary for Information and Technology establishes technical controls to ensure users cannot store sensitive personal information on shared network drives.

VBA Response: VBA defers to the Office of Information and Technology

Recommendation 3: The Assistant Secretary for Information and Technology implements improved oversight procedures, including specific facility-level procedures, to ensure that sensitive personal information is not being stored on shared network drives.

VBA Response: VBA defers to the Office of Information and Technology

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Review Team	Michael Bowman, Director Wade Greenwell Jack Henserling Shawn Hill George Ibarra

Report Distribution

VA Distribution

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

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and 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

OIG reports are available at www.va.gov/oig.