US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

Improper Sharing of Sensitive Information on Cloud-Based Collaborative Applications

Review	24-01330-29	April 22, 2025

BE A

VOICE FOR VETERANS

REPORT WRONGDOING

vaoig.gov/hotline | 800.488.8244

OUR MISSION

To serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

CONNECT WITH US

Subscribe to receive updates on reports, press releases, congressional testimony, and more. Follow us at @VetAffairsOIG.

PRIVACY NOTICE

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.

Visit our website to view more publications.
vaoig.gov

Executive Summary

The VA Office of Inspector General (OIG) received a hotline allegation from a VA medical center employee regarding the improper sharing of sensitive information on VA's internal network. The complainant reported that an employee could search for fellow VA employees on the internal network and find documents and emails that contained sensitive personal information. Among these documents were human resources paperwork, such as interview questions and reference checks, performance awards, and personally identifiable information (PII) for veterans getting surgery.

Sensitive personal information is the term VA uses to encompass PII and protected health information (PHI). It refers to any information about an individual that is maintained by VA and can be linked to that individual. It is protected by law and VA policy.[1] US laws require appropriate administrative, physical, and technical safeguards to protect personal information and limit its uses and disclosures without the individual's authorization.[2] VA policy requires VA information system users who access sensitive personal information in the course of their official duties to avoid its unauthorized disclosure and prohibits other users from accessing the information without a business need.[3]

The objective of this review was to evaluate the merits of the allegation.

What the Review Found

The OIG found sensitive personal information was accessible by VA users who had no business need to access it.[4] Furthermore, the OIG noted that the type of sensitive personal information accessible should not have been hosted on the systems it was found on, as the information exceeded the systems' security authorizations.[5] The OIG determined this was a national issue

[1] VA Handbook 6500, *Risk Management Framework for VA Information Systems*, *VA Information Security Program*, February 24, 2021; VA Directive 6502, *VA Enterprise Privacy Program*, May 5, 2008.

[2] The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat 1896, codified at 5 U.S.C. § 552a.

[3] VA, *Updated Department of Veterans Affairs Information Security Rules of Behavior for Organizational Users for Fiscal Year 2024*, September 28, 2023.

[4] Appendix A describes the review scope and methodology.

[5] VA Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment*, October 15, 2014; VA Handbook 6502.5, *Procedures for Establishing and Maintaining Privacy Act Systems of Records*, April 5, 2024. VA identifies privacy information authorized in an information technology system using a privacy threshold analysis and privacy impact analysis. If the information is subject to the Privacy Act, a system of records notice is published in the Federal Register. The notice identifies the system, the data collected, and how the data will be used.

because the hosting systems are cloud based and the information was observable by any authorized VA employee, regardless of location.[6]

The OIG team focused this review on two systems in which it observed improperly shared sensitive personal information: the Office of Information and Technology's (OIT) Microsoft Office 365 Multi-Tenant (O365 MT) system and the Veterans Health Administration's (VHA) Integrated Veteran Care Provider Profile Management System (PPMS). O365 MT and PPMS are distinct systems. Both systems use cloud-based Microsoft applications such as SharePoint. VA policy and OIT guidance apply to both systems.[7]

Collaborative applications that allow file sharing in the Office 365 suite include OneDrive, SharePoint, and Teams. OIT's Connectivity and Collaboration Services (CCS), which is responsible for the O365 MT system, has set Teams permissions to default to a private setting but explained that users can still change file access attributes using the different O365 MT applications.

Guidance published by OIT emphasizes that Teams owners and SharePoint owners and administrators are responsible for ensuring they are sharing properly. OIT's *Strategic Plan for Fiscal Years 2024 to 2026* states that a key objective for securing VA and veterans' data is to enforce least privileged access. This means limiting all users' information access to only those applications and data they need for their role in the organization.[8]

The observed security deficiencies occurred because VA does not have adequate controls to prevent, detect, and correct inappropriately set permissions for the sharing of sensitive information among the Office 365 collaborative applications.

The following are control weaknesses the OIG identified:

- SharePoint administrators did not always have full control over their SharePoint sites, resulting in a lack of knowledge of the permissions for and content of the sites.[9] VA-wide enforcement of standardized administration and recommended architecture would give administrators greater control of the permissions and

[6] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. National Institute of Standards and Technology (NIST), NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011.

[7] VA Directive 6500, *VA Cybersecurity Program*, February 24, 2021. The Office of the Assistant Secretary for Information and Technology and the Office of Information Security are responsible for VA's cybersecurity program. Full details on the sensitive information exposed appear in appendix B.

[8] VA Office of Information and Technology, *Strategic Plan, Fiscal Years (FY) 2024 to 2026*, March 1, 2024.

[9] SharePoint administrator responsibilities include troubleshooting issues for users and site owners, managing permissions, and assisting users with content and permissions.

content of SharePoint sites they are responsible for and help prevent improper sharing.[10]

- Although OIT has published instructions on secure administration of Teams and SharePoint, it lacks enforcement mechanisms to ensure standardized processes are followed across the organization.[11] These mechanisms can improve consistency of administration and oversight, help control permissions, and prevent improper sharing.
- OIT has not expanded roles and responsibilities of information security and privacy staff to include the routine review of Teams and SharePoint site permissions and content. Ensuring that routine duties include these reviews can improve the consistency of administration and oversight and help detect and correct excessive permissions and improper sharing.
- OIT has not broadly implemented automated tools, supported with training, to enable the timely and routine detection and correction of improperly shared and unauthorized content agencywide. These tools and their related policies can help OIT identify and detect excessive permissions and unauthorized content and prevent improper sharing.
- Training for SharePoint administrators is not standardized. Requiring standardized training for SharePoint administrators and owners to clarify and reinforce data security requirements would help protect sensitive personal information by controlling permissions on file-sharing applications.

While OIT has responded to the evolving risks and is attempting to mitigate them, VA will need to enhance control coverage to apply security in depth, agencywide. This is because other VA offices may implement these collaborative applications outside the direct control of OIT.

If VA is not able to implement controls to adequately protect sensitive personal information—including from misuse by insiders—it may cause harm to individuals whose information is improperly accessed and disclosed, and the department may face legal liability, remediation costs, and a loss of public trust.[12]

[10] Microsoft recommends flat information architecture in SharePoint Online for improved performance, easier management, and simpler navigation. Flat architecture refers to minimizing the use of nested subsites. VA follows Microsoft best practices.

[11] Communications from OIT on secure administration are in appendix C.

[12] NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010; VA Directive 6500, *VA Cybersecurity Program*.

What the OIG Recommended

The OIG recommended that the assistant secretary for information and technology and chief information officer ensure facilities and programs remove unauthorized sensitive personal information from collaborative application sites.[13] The assistant secretary should also direct facilities and programs to standardize SharePoint administration and inventory and consolidate their SharePoint sites, implement enforcement mechanisms, expand roles and responsibilities for privacy officers and information system security officers, implement automated tools to detect and correct improper sharing agencywide, and mandate standardized training for SharePoint administrators and owners.

VA Management Comments and OIG Response

The acting assistant secretary for information and technology and chief information officer concurred with all six recommendations. OIT provided acceptable action plans for all recommendations and requested closure of recommendations 2 and 3. To support the closure request, the acting assistant secretary provided sufficient evidence showing that corrective actions were taken, and the OIG considers recommendations 2 and 3 closed. All other recommendations remain open, and the OIG will monitor progress and close each recommendation when adequate documentation demonstrates sufficient implementation steps have been taken. See appendix D for the full responses from the acting assistant secretary.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

[13] The recommendations addressed to the assistant secretary for information and technology and chief information officer are directed to anyone in an acting status or performing the delegable duties of the position.

Contents

Abbreviations

CCS	Connectivity and Collaboration Services
ISSO	information system security officer
IT	information technology
O365 MT	Microsoft Office 365 Multi-Tenant
OIG	Office of Inspector General
OIT	Office of Information and Technology
PHI	protected health information
PII	personally identifiable information
PPMS	Provider Profile Management System
VHA	Veterans Health Administration

Introduction

The VA Office of Inspector General (OIG) received a hotline complaint from a VA medical center employee in November 2023 alleging that sensitive personal information was accessible to other employees on the VA network. The objective of this review was to evaluate the merits of the allegation. Sensitive personal information is the term VA uses to encompass personally identifiable information (PII) and protected health information (PHI). It refers to any information VA maintains about an individual that can be linked to that individual, and it is protected by law and VA policy.[14]

Allegation

The VA medical center employee alleged that while on the VA network, an employee could search for fellow VA employees on the internal network and find documents and emails that contained sensitive personal information. Among these documents were human resources paperwork such as performance awards and descriptions of procedures for veterans getting surgery. The complainant added that the identifying information is accessible to those who do not have a need to know and that anyone on the VA network, including contractors nationwide, can see confidential data in documents that the staff members (the subjects of the search) worked on recently. The complainant also expressed concern about the potential for other sensitive information—such as confidential data about performance, contracting bids, and patient information—to be shared.

Cloud-Based File-Sharing Applications

VA uses Microsoft Office 365 for a variety of business functions, such as analytics, data mining, email, data transfers, collaboration, and project management. Office 365 is a cloud-based productivity system that includes applications such as Microsoft Teams, Word, Excel, PowerPoint, Outlook, and OneDrive.[15] Users can store and share files using SharePoint,

[14] VA Handbook 6500, *Risk Management Framework for VA Information Systems, VA Information Security Program*, February 24, 2021; VA Directive 6502, *VA Enterprise Privacy Program*, May 5, 2008; The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat 1896, codified at 5 U.S.C. § 552 a.

[15] Microsoft Teams provides VA internal users with instant messaging, group chat, voice/video internet calls, virtual teleconferencing, file sharing, and shared workspace. OneDrive for Business is cloud storage that enables internal VA users to manage their data and grant other internal users access to the data. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. National Institute of Standards and Technology (NIST), NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011.

OneDrive, and Microsoft Teams. SharePoint underpins each of these tools.[16] SharePoint administrators and owners are responsible for reviewing and updating permissions.

Privacy Protections

The Privacy Act of 1974, 5 U.S.C. § 552 a, is the foundation of public sector privacy law in the United States and it applies to federal agencies.[17] The Privacy Act limits data disclosure to those who need access for business purposes, such as sharing for an identified routine use or to perform agency work.[18] The Privacy Act also requires agencies to maintain appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records.[19]

VA follows the requirements of the Privacy Act. The department's policy dictates protecting all personal information that is maintained by, or for, VA regardless of the medium in which it is maintained.[20] The VA Office of Information and Technology's (OIT) *Strategic Plan for Fiscal Years 2024 to 2026* states that a key objective in securing VA and veterans' data is to enforce least privileged access. This means limiting all users' information access to the applications and data they need to accomplish their role in the organization.[21] VA policy further requires annual training and the agreement of VA information system users who access sensitive personal information in the course of their official duties to avoid its unauthorized disclosure, and the policy prohibits other users from accessing the information without a business need.[22] VA privacy protections and OIT guidance on secure use apply to all systems discussed in this review.

[16] "Collaborating with Teams, SharePoint, and OneDrive" (web page), Microsoft, accessed June 24, 2024, Microsoft Support.

[17] NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.

[18] 5 U.S.C. § 552 a(b)(1) Need to Know: "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains unless the disclosure would be (1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552 a(b)(3) Routine Uses: "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains unless the disclosure would be … (3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D)."

[19] 5 U.S.C. § 552 a(e)(10).

[20] VA Directive 6502, *VA Enterprise Privacy Program*, May 5, 2008. VA uses the term "maintained" for data collected, created, transmitted, used, processed, stored, or in the disposition process.

[21] VA Office of Information and Technology, *Strategic Plan, Fiscal Years (FY) 2024 to 2026*, March 1, 2024.

[22] VA, *Updated Department of Veterans Affairs Information Security Rules of Behavior for Organizational Users for Fiscal Year 2024*, September 28, 2023.

Additionally, policy that applies to Veterans Health Administration (VHA) systems directs that only approved individuals who meet all VA and VHA policy requirements are to be granted access to PII processed and stored on VA information technology (IT) systems.[23]

Aside from limiting access to sensitive information, VA is expected to comply with the Privacy Act requirement to inform the public about the record systems it maintains that house such information. It must publish a system of records notice in the Federal Register describing the existence and character of any new or modified system of records.[24] VA policy states[25]

> A SORN [system of records notice] is comprised of the Federal Register notice(s) that identifies the SOR [system of records], the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system. The requirement for agencies to publish a SORN allows the Federal Government to accomplish one of the basic objectives of the Privacy Act—fostering agency accountability through public notice.

Roles and Responsibilities

The Office of the Assistant Secretary for Information and Technology and the Office of Information Security are responsible for VA's cybersecurity program.[26] The assistant secretary for information and technology, who is also the chief information officer, has responsibilities that include monitoring, evaluating, and providing advice to the VA Secretary regarding all VA cybersecurity and privacy activities; overseeing implementation of the cybersecurity program; and directing and coordinating with VA administrations and staff offices to ensure that cybersecurity and privacy responsibilities are addressed for all VA IT.[27]

VA policies define information system security officer (ISSO) and privacy officer responsibilities.[28] Examples of responsibilities for ISSOs include verifying and validating that appropriate security measures are implemented and functioning as intended, interpreting patterns of noncompliance at a local level to determine their impact on levels of risk and overall

[23] VHA Directive 1080, *Access to Personally Identifiable Information in VA Information Technology Systems*, September 28, 2023.

[24] NIST Special Publication 800-122; 5 U.S.C. § 552 a(e)(4).

[25] VA Handbook 6502.5, *Procedures for Establishing and Maintaining Privacy Act Systems of Records*, April 5, 2024. A system of records is 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 identifier assigned to the individual; 5 U.S.C. § 552 a(e)(4).

[26] VA Directive 6500, *VA Cybersecurity Program*, February 24, 2021.

[27] VA Directive 6500.

[28] ISSOs work for OIT's Enterprise Security Operations, while privacy officers work for the administrations, facilities, and staff offices they support.

effectiveness of the enterprise cybersecurity program, collaborating with facility privacy officers and others as appropriate for the implementation and assurance of reasonable safeguards, and ensuring that all VA information systems are compliant with the cybersecurity and privacy policies and procedures.[29]

Privacy officer responsibilities include assisting in the development of the system-level privacy policies and procedures, ensuring compliance with VA privacy policies and procedures, and working with the ISSO to monitor a system and its environment of operation.[30] VHA policy makes the privacy officer and ISSO jointly responsible for validating and monitoring the level of data access of VA staff based on established functional roles, reporting and documenting security and privacy incidents involving PII, and ensuring training levels of VA staff as appropriate to the privacy and security integrity of VHA data in VA IT systems.[31]

Individual owners of OneDrive accounts and Teams sites are responsible for ensuring they are sharing authorized sensitive information securely. SharePoint administrators manage site permissions and assist users with content and permissions.

[29] VA Handbook 6500; VA Directive 6500.

[30] VA Handbook 6500.

[31] VHA Directive 1080.

Results and Recommendations

Finding: VA Lacks Controls to Prevent Improper Sharing of Sensitive Information on Collaborative Cloud-Based Applications

The OIG team substantiated the allegation and found that sensitive information, including sensitive personal information, was accessible by VA users—most of whom had no business need to access the information.[32] Furthermore, the OIG noted that the type of sensitive information accessible should not have been on the systems because they were not authorized to host it.[33] Although the allegation originated from a medical facility, the OIG determined that this was a national issue because the hosting systems are cloud based and the information was observable by any authorized VA employee, regardless of location.[34]

The OIG team determined that the core issue concerned information-sharing permissions in Microsoft Office collaborative applications. Office applications such as OneDrive, SharePoint, and Teams are intended to promote collaboration. Individual owners of OneDrive accounts and Teams sites are responsible for ensuring they are sharing authorized sensitive information securely. SharePoint administrators manage site permissions and assist users with content and permissions. VA must balance users' ability to collaborate against the requirement to ensure the security and confidentiality of sensitive information.

If VA is not able to implement controls to adequately protect sensitive information—including from misuse by insiders—it may cause harm to individuals whose information is improperly

[32] According to VA Directive 6500, VA sensitive information is any information that has not been cleared for public release and has been collected, developed, received, transmitted, used, or stored by VA or by a non-VA entity in support of an official VA activity. According to 38 U.S.C. § 5727, the term "sensitive personal information," with respect to an individual, means any information about the individual maintained by an agency, including the following: (A) Education, financial transactions, medical history, and criminal or employment history; and (B) 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, or biometric records. VA Directive 6502 states that the term PII is interchangeable with the term "sensitive personal information," as defined in 38 U.S.C. § 5727 (19) and VA Handbook 6500." For simplicity, this report uses the term "sensitive information" to mean all these terms: sensitive information, sensitive personal information, and personally identifiable information.

[33] VA Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment*, October 15, 2014; VA Handbook 6502.5. VA identifies privacy information authorized in an information technology system using a privacy threshold analysis and privacy impact analysis. If the information is subject to the Privacy Act, a system of records notice is published in the Federal Register. The notice identifies the system, the data collected, and how the data will be used.

[34] NIST Special Publication 800-145.

accessed and disclosed, and the department may face legal liability, remediation costs, and a loss of public trust.[35]

The OIG's finding is based on the following determinations:

- Sensitive information was accessible to VA users on systems not authorized to host it.
- Inadequate controls over permissions led to the improper sharing of sensitive information.
- OIT has made efforts to mitigate the risk of improper sharing on collaborative applications.

What the OIG Did

The scope of the review was the security of sensitive VA information shared on cloud-based collaborative applications within VA's Microsoft Office 365 environment, which was implemented in February 2019. The team tested the circumstances described by the complainant and was able to replicate and substantiate them. The team expanded its research to better understand the sharing and collaboration capabilities of Office 365 but did not do an exhaustive search to identify all forms of sensitive information available or to count the instances.

The OIG team focused this review on two systems in which it observed improperly shared sensitive information: OIT's Microsoft Office 365 Multi-Tenant (O365 MT) system and VHA's Integrated Veteran Care Provider Profile Management System (PPMS). O365 MT and PPMS are distinct systems.[36] O365 MT is managed by OIT's Connectivity and Collaboration Services (CCS); PPMS is managed by the VHA Office of Integrated Veteran Care. Both systems use cloud-based Microsoft applications such as SharePoint.

Appendix A describes the review scope and methodology.

[35] NIST Special Publication 800-122; VA Directive 6500. Directive 6500 states: "Insider threat controls will be implemented to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and nontechnical information to identify potential insider threat concerns in accordance with the VA Insider Threat Program"; "Veterans Affairs Insider Threat Program Awareness and Reporting Tool" (web page), VA, Office of Operations, Security, and Preparedness, accessed May 21, 2024, https://www.osp.va.gov/insider_threat_program_awareness_reporting_tool.asp. VA defines an insider threat as "acts of commission or omission by an insider who intentionally or unintentionally compromises VA's ability to accomplish its mission."

[36] Each system is separately registered in VA's governance, risk, and compliance tool, the Enterprise Mission Assurance Support System.

Sensitive Information Was Accessible to VA Users on Systems Not Authorized to Host It

The OIG discovered sensitive information, including sensitive personal information, was accessible by VA users—most of whom have no business need to access the information. Furthermore, the OIG noted that the type of sensitive information accessible should not have been on the systems because they were not authorized to host it. The OIG team did not do an exhaustive search to identify all forms of sensitive information available. However, given the number of SharePoint sites hosted on the O365 MT system (over 200,000 as of July 15, 2024) and the type of sensitive information observed, the likelihood for more instances of improperly shared sensitive information based on incorrectly set permissions is high.

Sensitive Information Exposed

The OIG team found that a VA employee doing an internal network search for another VA employee could view documents shared by the other employee. If permissions for those documents were improperly set and the documents contained sensitive information, any employee who conducted a similar search would also have access to the sensitive information. Office 365 users can set permissions on their documents where they are stored, such as on OneDrive or SharePoint in Office 365. The team concluded that improper sharing of sensitive information occurred and that the documents observed were stored in Office 365 applications.

Aware that documents in Office 365 are stored in applications such as OneDrive and SharePoint, the OIG team members expanded the test by searching from their own VA OneDrive accounts for documents that might contain sensitive information. Based on the sensitive information observed that the team accessed in the same manner as any other employees might have and based on the fact that OIG team members did not have a need to know for that information, the team further corroborated the allegation that sensitive information was accessible on the VA network to other employees, contrary to Privacy Act provisions.[37] The types of sensitive information observed included financial, technical, and operational information as well as PII such as performance evaluations; Drug Enforcement Administration registration numbers; external healthcare providers' addresses, emails, and phone and fax numbers; financial information such as complete bank account information; and PHI such as patient names, the last four digits of social security numbers, and scheduled medical procedures.[38] Full details on the sensitive information exposed appear in appendix B.

[37] 5 U.S.C. § 552 a(b)(1), (b)(3), and (e)(10).

[38] The Drug Enforcement Administration assigns registration numbers to healthcare providers, allowing them to write prescriptions for controlled substances that can be tracked to monitor potential fraud and abuse.

Authorizations Exceeded

The OIG also discovered that the level of sensitivity of the information exceeded what is authorized on the O365 MT and PPMS systems. Federal standards require organizations to identify all PII residing within or under their control. Privacy threshold analyses are used to determine whether a system contains PII, whether a privacy impact assessment or system of records notice is required, and whether any other privacy requirements apply to the information system.[39] For VA, a privacy impact assessment determines whether an existing system of records notice should be revised or a new system of records notice is required.

The type of sensitive information the team observed on the O365 MT system exceeded what the privacy impact assessment had authorized because it included personal information for non-VA employees—for example, VA patients and job applicants. According to the O365 MT privacy impact assessment, the VA O365 MT system is not a data storage or warehouse repository or the authoritative system for PII or PHI data. The information stored in O365 MT that is received from the VA Active Directory Information System on VA employees includes business contact information within the Global Address List for internal purposes only: employee name, work phone number, work location, and email address; when combined, this is considered PII.[40] Because O365 MT is not intended to be used to retrieve information about individuals using a unique identifier such as a name or social security number, a system of records notice is not required for the system.[41]

The information the team observed on the PPMS system also exceeded its privacy impact assessment. For example, the privacy impact assessment states that PPMS will collect and retain PII on non-VA healthcare providers—specifically a provider's tax identification number, which can be the social security number and the provider's date of birth—to facilitate payment to the provider for services rendered to a qualified veteran or beneficiary. However, as detailed in appendix B, the OIT team observed other sensitive information, such as medical licensing and banking information. PPMS is identified as a Privacy Act system, and a system of records notice is required for the system. The team noted that the PPMS system of records notice identifies categories of records in the system for VA and non-VA providers that were not identified in the privacy impact assessment but do reflect what the OIG observed.[42] The team discussed this discrepancy with PPMS officials and clarified how the system of records notice should reflect

[39] NIST Special Publication 800-122.

[40] VA, *Privacy Impact Assessment (PIA) for the VA IT [information technology] System called: Microsoft Office 365 Multi-Tenant*, September 22, 2020.

[41] VA, *Privacy Threshold Analysis for Microsoft Office 365 Multi-Tenant*, February 9, 2023.

[42] The PPMS system of records notice identifies categories of records in the system: VA providers' and non-VA providers' information such as name, national provider identifier/index, quality ranking total score, preferred provider, phone, email, billing address, license number, Drug Enforcement Administration registration number, certification, tax identification/social security number, and non-VA providers' date of birth.

the sensitive information identified in the privacy threshold analysis and privacy impact assessment. Officials agreed that they would need to update their privacy threshold analysis and privacy impact assessment and said they would check first to make sure the data listed in the system of records notice were correct. On July 9, 2024, PPMS officials provided a copy of an updated privacy threshold analysis that reflected the types of privacy records identified in the PPMS system of records notice. This privacy threshold analysis was pending approval.

Inadequate Controls Over Permissions Led to the Improper Sharing of Sensitive Information

The OIG found VA did not have adequate controls to prevent, detect, and correct inappropriately set permissions for the sharing of sensitive information among the Office 365 collaborative applications. While Office 365 applications promote collaboration, individual owners of OneDrive accounts and Teams sites are responsible for ensuring they are sharing securely. SharePoint administrators manage site permissions and assist users with content and permissions. In overseeing this, VA must balance users' ability to collaborate and the requirement to ensure the security and confidentiality of sensitive information.

The specific permissions-related weaknesses the OIG team identified were a lack of full administrator control, a lack of enforcement mechanisms, gaps in roles and responsibilities, insufficient use of automated tools, and inconsistent qualifications.

Administrator Control

SharePoint administrators do not always have full control over their SharePoint sites, resulting in a lack of knowledge of the permissions for and content of the sites.[43] For example, SharePoint administrators the team interviewed do not always have access to all the SharePoint sites at their facility. Other departments at their facility could create their own SharePoint pages without these administrators' knowledge. SharePoint administrators that the team interviewed explained they follow OIT's recommendations for newly created pages and are working to migrate their existing sites to the recommended architecture.[44] Doing so has its challenges. One administrator reported not having the ability to monitor the 800-some SharePoint pages at the facility and attempting to find out what pages are needed. Requiring standardized administration and the recommended architecture would give administrators greater control of the permissions and content of SharePoint sites they are responsible for and help prevent improper sharing. This is because the

[43] SharePoint administrator responsibilities include troubleshooting issues for users and site owners, managing permissions for the site, and assisting users with content and permissions.

[44] Microsoft recommends flat information architecture in SharePoint Online for improved performance, easier management, and simpler navigation. Flat architecture refers to minimizing the use of nested subsites. VA follows Microsoft best practices.

enforcement would prevent the creation of SharePoint sites outside authorized administrators' control and would ease administration, including managing site permissions and content.

Enforcement Mechanisms

Although OIT has published instructions on secure administration of Teams and SharePoint, OIT lacks enforcement mechanisms to ensure standardized processes are followed at facilities and by programs.[45] For example, current controls rely on SharePoint administrators and owners reviewing and updating permissions. CCS hosts a SharePoint Online Help Desk Tool that showed over 200,000 SharePoint sites in O365 MT as of July 15, 2024, with over 142,000 administrators. An OIT official stated staffing is insufficient to police all these SharePoint sites. The official confirmed that SharePoint administrators and owners are responsible for reviewing and updating permissions and that local privacy, information security, and OIT staff are not required to do so. The official added in an email that site and data owners often overlap as privacy and IT staff and the staff in that area do a tremendous job working with and reminding site and data owners of privacy and permission checks.

Although O365 MT and PPMS are distinct systems and managed by different program offices, each carries the risk associated with information-sharing permissions in the use of Microsoft collaborative applications. For example, one PPMS official expressed the difficulty of getting 170 VA medical centers, all medical support assistants, and over 1,000 people to try to maintain the permissions. As another example, not all SharePoint administrators interviewed were aware of CCS' SharePoint Online Help Desk Tool intended for facilities to keep up with the O365 SharePoint sites. Given the number of SharePoint sites and administrators, manual control is inadequate. Enforcement mechanisms could improve consistency of administration and oversight and help control permissions and prevent improper sharing. Examples of these mechanisms include ensuring SharePoint administrators have full control, assigning additional responsibilities to support staff, using automated tools to help detect overly broad permissions and unauthorized content, and requiring standardized training to ensure consistency in administrator qualifications. The team noted that other than at the site of the hotline complaint, staff at facilities and programs elsewhere were not aware of the sensitive information the OIG team observed until the team reported it to them. Since O365 MT and PPMS are distinct systems, and other VA offices could also implement Microsoft collaborative applications within other systems, enforcement mechanisms will need to be applied agencywide.

Information Security and Privacy Staff Roles and Responsibilities

OIT has not expanded roles and responsibilities of information security and privacy staff to include the routine review of Teams and SharePoint site permissions and content. For example,

[45] Communications from OIT on secure administration are in appendix C.

the OIG noted that OIT guidance was directed to SharePoint site administrators and owners and Teams owners, but not to VA ISSOs and privacy officers. Additionally, OIT has not provided information security and privacy staff with instructions for reviewing SharePoint permissions. Privacy officers and OIT staff the team interviewed, including ISSOs, stated they do not check SharePoint permissions. OIT staff and ISSOs stated that they focused on providing technical support for SharePoint sites, not on permissions or content. Privacy officers were not all familiar with the facilities' process to grant SharePoint access. SharePoint administrators interviewed stated they do not work routinely with facility ISSOs or privacy officers. Local ISSOs and privacy officers could be used as an enforcement mechanism. Ensuring that routine duties include review of permissions and content can improve the consistency of administration and oversight and help detect and correct excessive permissions and improper sharing.

Automated Tools

OIT has not broadly implemented automated tools and policies, supported with training, to enable the timely and routine detection and correction of improperly shared and unauthorized content agencywide. These tools and policies can identify excessive permissions and unauthorized content and help detect and correct improper sharing. Data loss prevention tools and policies can be used within Office 365 to monitor for and notify users about specific types of sensitive information at risk of inadvertent disclosure.[46] Data loss prevention program officials stated that until the data loss prevention program is fully implemented, VA must depend on users to protect sensitive data. In a June 2024 meeting, OIT officials confirmed it was also possible to provide automated tools to privacy and information security staff to review SharePoint permissions and content locally.

Administrator Training

Training for SharePoint administrators is not standardized. Administrators who were interviewed explained that their training had been self-taught—using Microsoft and VA online training resources, on-the-job training, or prior work experience. Although OIT has a VA SharePoint Certification Program, certification is not required for SharePoint administrators, privacy and information security staff, or data owners. Requiring standardized training for SharePoint administrators and owners to clarify and reinforce data security requirements would help protect sensitive personal information by controlling permissions on file-sharing applications.

[46] VA OIT, "DLP [data loss prevention]: Information on the Purpose of Data Loss Prevention," March 4, 2024.

OIT Has Made Efforts to Mitigate the Risk of Improper Sharing on Collaborative Applications

OIT has responded to improper sharing on collaborative applications in several ways, presented here and in greater detail in appendix C. OIT leaders interviewed noted the challenges of controlling sharing on Microsoft Office collaborative applications, said they work closely with Microsoft to identify emerging risks, and pointed to efforts they have made to mitigate the risks. They explained that as long as users have the authority to share documents, improper sharing will continue. The middle ground between "deny all" access and "allow all" access will rely on users.[47] To clarify OIT's statement, a security challenge inherent to collaborative applications is maintaining a balance between user privilege and control.[48] While various controls may be in place to protect information exchanged in collaborative environments, as long as the information owners have control over their sharing, their decisions will be the first to impact the security of the information. The security principle of least privilege, where a user's access privileges are restricted to the minimum necessary to accomplish assigned tasks, represents the balance point between user privilege and control.[49]

OIT leaders confirmed that SharePoint administrators and owners are responsible for reviewing and updating permissions. OIT has provided direction and guidance to SharePoint administrators and owners and Teams owners on secure administration of these applications, including reviewing and updating permissions.

OIT also planned to expand its limited data loss prevention capabilities. According to program officials, VA's data loss prevention program has some current capabilities that could help identify excessive permissions and unauthorized content. For example, when users share sensitive information from their OneDrive accounts, they will receive an alert. These processes have not been widely applied to identify improper sharing of sensitive personal information on SharePoint sites.

CCS planned a pilot program for September 2024 to help identify and restrict sharing of information on O365 MT applications. Data loss prevention program officials said that until the program is fully implemented, VA must depend on users to protect sensitive data. Moreover, because CCS manages the O365 MT system and not PPMS, the data loss prevention pilot

[47] "Deny all" is based on the concept of deny by default, and it means to deny all access or privileges by default and to allow access or privileges only by exception. "Allow all" is the opposite. NIST Computer Security Resource Center (CRSC) Glossary (web page), accessed October 29,2024, https://csrc.nist.gov/glossary/term/deny_by_default.

[48] Privilege is "a right granted to an individual, a program, or a process." NIST CSRC Glossary (web page), accessed October 29, 2024, https://csrc.nist.gov/glossary/term/privilege.

[49] Least privilege is "a security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks." NIST CSRC (web page), accessed October 29, 2024, https://csrc.nist.gov/glossary/term/least_privilege.

program will not apply to Microsoft collaborative applications used within PPMS or to other VA offices that may use these applications within other systems.

While OIT has responded to the evolving risks and is attempting to mitigate them, VA needs to extend control coverage across the organization. The OIG team observed improperly shared sensitive information on two distinct implementations of Office 365, and OIT manages only one of those. Since other VA offices can implement other systems using Office 365, controls should be applied broadly.

Conclusion

The OIG discovered sensitive information was accessible by VA users, most of whom had no business need to access it. Furthermore, the OIG noted that the type of sensitive information accessible should not have been on the systems because they were not authorized to host it. Facilities and programs were not aware of the sensitive information until the team reported it to them.

The OIG determined VA does not have adequate controls to prevent, detect, and correct inappropriately set permissions for the sharing of sensitive information among the Microsoft Office 365 collaborative applications. Multiple factors led to this determination. While OIT has responded to the evolving risks and is attempting to mitigate them, VA will need to enhance and extend controls agencywide. Current controls rely on SharePoint administrators and owners reviewing and updating permissions, timely direction and guidance provided by OIT to SharePoint administrators and owners and Teams owners, and limited data loss prevention capabilities. However, according to CCS' SharePoint Online Help Desk Tool, there were over 200,000 SharePoint sites in the O365 MT system alone as of July 15, 2024, and this tool does not track SharePoint sites on other systems' implementations of Microsoft collaborative applications, such as VHA's PPMS.

Unless VA broadly applies corrective actions to adequately protect sensitive information on cloud-based file-sharing applications, VA may inadvertently harm individuals whose information was improperly accessed and disclosed, as well as the department. Individual harms may include identity theft, embarrassment, and blackmail. Organizational harms may include a loss of public trust, legal liability, and remediation costs.[50]

[50] NIST Special Publication 800-122.

Recommendations 1–6

The OIG made the following recommendations to the assistant secretary for information and technology and the chief information officer:[51]

1. Take corrective actions to ensure that facilities and programs remove unauthorized sensitive information from collaborative application sites.
2. Direct facilities and programs to standardize SharePoint administration, inventory and consolidate their SharePoint sites, and enforce the recommended architecture to better control access and content at the facility or program level.
3. Implement enforcement mechanisms to ensure that facilities and programs are following standardized processes to secure SharePoint and Teams sites.
4. Expand roles and responsibilities of facility and program information system security officers and privacy officers to include the routine review of SharePoint and Teams site permissions and content.
5. Implement automated tools and policies, supported with training, to enable the timely and routine detection and correction of improper sharing and unauthorized content throughout VA.
6. Mandate standardized training for SharePoint administrators and owners to clarify and reinforce data security requirements.

VA Management Comments

The acting assistant secretary for information and technology and chief information officer concurred with all six recommendations and provided action plans for each. Appendix D includes the full text of the comments, which are summarized here.

Regarding recommendation 1, OIT reconfigured all Microsoft Teams and SharePoint Online sites to “private” by default and will also issue a memorandum mandating SharePoint security essentials training for all VA organizational users and clarifying the role of SharePoint owners in reviewing any sensitive information contained on their sites. The local privacy officer and ISSO will be charged with oversight.

OIT requested to close recommendations 2 and 3. The acting assistant secretary stated that centralized SharePoint platform administration is now in place, and OIT routinely executes and enforces user training and awareness to ensure a continued understanding of privacy needs at the facility level. To implement recommendation 3, OIT deployed privacy labels as the default and

[51] The recommendations addressed to the assistant secretary for information and technology and chief information officer are directed to anyone in an acting status or performing the delegable duties of the position.

retrofitted all related sites with them. In addition, OIT reported that it uses training and awareness of community practice to enforce permission reliability.

For recommendation 4, the acting assistant secretary explained that VA SharePoint site administrators and owners will establish SharePoint and Teams sites in accordance with VA SharePoint governance roles, responsibilities, and terms and must consult with facility privacy officers when PII and PHI will be used. OIT will also publish a memorandum clarifying the roles of SharePoint and Teams owners in routinely reviewing their site permissions and content with oversight from the local privacy officer and ISSO.

To address recommendation 5, the acting assistant secretary stated that OIT is piloting advanced tooling to automate review and awareness of site permissions errors, which will allow for automatic remediation, alerting, and reporting.

For recommendation 6, the acting assistant secretary stated staff have implemented a workflow requiring users to complete SharePoint security essentials training before site delivery. OIT will publish a memorandum to mandate the training and will also explore the possibility of adding the training as an annual requirement for all organizational users in the VA Talent Management System and as a part of the Rules of Behavior.

OIG Response

The acting assistant secretary for information and technology and chief information officer provided acceptable action plans for all six recommendations and requested closure of recommendations 2 and 3. To address recommendation 2, OIT submitted evidence of two notifications. One notification provided guidance on actions that need to be completed by Teams owners and SharePoint site owners to improve the security of content, and the other notification indicated that all Teams would be changed from public to private. For recommendation 3, the acting assistant secretary provided links to internal SharePoint sites: one that defines roles, responsibilities, and terms and another—a community of practice site—that supports training and awareness. The OIG agrees with closure of recommendations 2 and 3. All other recommendations remain open. The OIG will monitor progress and close each recommendation when adequate documentation demonstrates sufficient implementation steps have been taken.

Appendix A: Scope and Methodology

Scope

The review team conducted its work from February 2024 through October 2024. The scope of the review was the security of sensitive VA information shared on cloud-based collaborative applications in Microsoft Office 365, which VA implemented in February 2019.

Methodology

To review the allegation, the team tested the circumstances described by the complainant and was able to replicate the problem. Team members also reviewed federal law and guidance and VA policy regarding privacy protections and conducted research to better understand the sharing and collaboration capabilities of Office 365. The team did not perform an exhaustive search to identify all forms of sensitive information available or to count the instances. The VA Office of Inspector General (OIG) reported its observations of improperly shared sensitive personal information to facility and program privacy and information systems security staff. To corroborate the allegation, the team interviewed the complainant and other employees who witnessed the sensitive information. The team also interviewed facility and program privacy officers, information systems security officers, Office of Information and Technology leaders and staff, and SharePoint administrators to better understand the improper sharing, identify the causes, and develop recommendations.

Internal Controls

The review team assessed the internal controls of VA’s oversight of the sharing of sensitive information on cloud-based collaborative applications within VA’s Office 365 environment that were significant to the review objective. This included an assessment of the five internal control components: control environment, risk assessment, control activities, information and communication, and monitoring.[52] In addition, the team reviewed the principles of internal controls as associated with the objective. The team identified five components and six principles as significant to the objective.[53] The team identified internal control weaknesses during the review and proposed recommendations to address weaknesses in the following control components and principles:

- Component: Control Environment

[52] Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-14-704G, September 2014.

[53] Since the review was limited to the internal control components and underlying principles identified, it may not have disclosed all internal control deficiencies that may have existed at the time of this review.

    - Principle 2: Exercise Oversight Responsibility
- Component: Control Activities
    - Principle 11: Design (Control) Activities for the Information System
- Component: Information and Communication
    - Principle 14: Communicate Internally
- Component: Risk Assessment
    - Principle 7: Identify, Analyze, and Respond to Risk
- Component: Monitoring
    - Principle 16: Perform Monitoring Activities
    - Principle 17: Evaluate Issues and Remediate Deficiencies

Data Reliability

The review team did not depend on computer-processed data to develop findings, conclusions, or recommendations, so the team did not need to assess the reliability and accuracy of that type of data. The team did obtain evidence from interviews, documentation, and testing and observation, and the team determined that the evidence was sufficient and appropriate to provide a reasonable basis for findings and conclusions.

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*.

Appendix B: Information Exposed

During this review, the team observed improperly shared sensitive information on SharePoint sites that hosted Microsoft Word, Excel, and portable document format files. SharePoint is an online application for internal users to create internal internet sites to share data such as documents and information. Any content created for SharePoint is stored in the cloud. Access to the data is managed by the internal user (the VA employee), who can allow access by other internal users.

The team focused its review on two systems in which improperly shared sensitive personal information was observed: Office of Information Technology’s (OIT) Microsoft Office 365 Multi-Tenant (O365 MT) system and the Veterans Health Administration’s (VHA) Integrated Veteran Care Provider Profile Management System (PPMS). O365 MT is managed by OIT’s Connectivity and Collaboration Services (CCS). PPMS is managed by the VHA Office of Integrated Veteran Care.

VA’s Microsoft Office 365 Multi-Tenant

O365 MT is a cloud computing–based subscription service from Microsoft. O365 MT includes collaborative applications that allow file sharing such as OneDrive, SharePoint, and Teams. CCS has set Teams permissions to default to a private setting but also explained that users can change file access attributes using the different O365 MT applications.

On the O365 MT system, using the same access as any other authorized VA employees, the OIG team members observed the following types of sensitive personal information in documents hosted on SharePoint sites:

- Contractor personal identity verification information: names, titles, personal email address, and vendor name.
- Position recruitment information: name of incumbent, position, and position status.
- Patient procedure logs: patient name, last four numbers of social security numbers, procedure description time and date, and additional notes on use of anticoagulants or insulin.
- Interview notes for job applicants: applicant names, dates of interviews, and interview notes.
- Archived performance appraisals, VA Form 0750.
- Relocation incentive signed by a Veterans Integrated Services Network director.
- Fiscal year 2024 VHA senior executive service performance plan.
- Legal documents from the US Court of Appeals for Veterans Claims.

Additionally, the OIG team observed these examples of nonpersonal sensitive information:

- Financial indicator report, which detailed payments to vendors.
- Technical information for an information technology ticket related to deploying network hardware: gateway, subnet mask, network ID, and internet protocol addresses.
- Contractor cost information: number of resources, average cost per hour, total cost per hour, and total annual cost.
- Accounts receivable extract report (comparison of Veterans Health Information Systems and Technology Architecture receivables with Financial Management System receivables).[54]
- Facility contract project trackers: Electronic Health Record Modernization Program infrastructure updates with cost amounts, including facility location, project number, and project title.
- Facility major lease memorandum.
- Purchase card orders.

VHA's Integrated Veteran Care Provider Profile Management System

PPMS is a comprehensive repository of administrative information and the authoritative source of non-VA Providers for VHA. It offers validation and collection of other non-VA provider information and allows for workflow management and tracking. VA retains ownership rights over the data hosted in the cloud including the personally identifiable information (PII) portions of the records. PPMS uses Microsoft Dynamics 365, which integrates Office applications such as SharePoint Online.[55]

On PPMS, using the same access as any other authorized VA employees, the OIG team observed sensitive personal information for external VA health care providers in documents hosted on SharePoint sites:

- Credentialing date

[54] The Veterans Health Information Systems and Technology Architecture is an enterprise-wide information system built around an electronic health record and used throughout the VHA. It consists of nearly 160 integrated software modules for clinical care, financial functions, and infrastructure. The Financial Management System is a standardized, VA-wide accounting system that interfaces externally with the Department of the Treasury, the General Services Administration, the Internal Revenue Service, the Defense Logistics Agency, and various commercial vendors and banks for electronic billing and payment.

[55] Microsoft describes Dynamics 365 as a portfolio of intelligent business applications. Dynamics 365 for government is a government-community cloud.

- Tax identification number
- Name, date of birth, and gender
- Degree
- National Provider Identification number[56]
- National Uniform Claim Committee Health Care Provider Taxonomy code[57]
- Group/site location name and group National Provider Identification number
- Practice address, phone and fax numbers, email address, languages spoken at location, billing address, and billing phone number
- Medicaid number for the provider
- Practicing specialties
- Clinical Laboratory Improvement Amendments certification number[58]
- State license number and expiration date
- Drug Enforcement Agency number[59]
- Hospital affiliation
- Whether the individual is a healthcare plan provider
- Faxed documents with the provider's name, National Provider Identification number, driver's license number, and taxonomy code
- VA Financial Services Center Vendor File Request Form 10091, which contains the provider's name, social security number, National Provider Identification number, email address, phone number, home address, and complete bank account

[56] The National Provider Identification is a Health Insurance Portability and Accountability Act (HIPAA) administrative simplification standard. It is a unique identification number for covered healthcare providers. Covered healthcare providers and all health plans and healthcare clearinghouses must use their numbers in administrative and financial transactions under HIPAA.

[57] The Health Care Provider Taxonomy code set is an external, nonmedical data code set designed for use in an electronic environment, specifically in certain healthcare transactions. This includes the transactions mandated under HIPAA.

[58] The Clinical Laboratory Improvement Amendments of 1988 (42 U.S.C. § 263a) and the associated regulation (42 C.F.R. § 493) provide the authority for certification and oversight of clinical laboratories and laboratory testing.

[59] The Drug Enforcement Administration assigns registration numbers to healthcare providers, allowing them to write prescriptions for controlled substances that can be tracked to monitor potential fraud and abuse.

information (bank name, address, routing number, account number, and account type)—in some cases even a voided check as part of a direct deposit setup form[60]

- Signed VHA Veterans Care Agreements with provider’s National Provider Identification number
- VHA Vendor Registration Forms with a provider’s business name, complete address, telephone number, federal tax identification number, and National Provider Identification number
- Department of the Treasury Internal Revenue Service W-9 forms, Request for Taxpayer Identification Number and Certification, with provider’s name, address, and social security number

[60] VA Financial Services Center Vendor File Request Form 10091 is used to gather essential payment data from vendors (commercial, individual, and veteran) to establish or update vendor records to process electronic payments in accordance with 31 C.F.R. Part 208.

Appendix C: Steps Taken by OIT to Mitigate the Risk of Improper Sharing on Collaborative Applications

The Office of Information and Technology (OIT) has responded to the evolving risks of improper sharing on Microsoft collaborative applications and has been attempting to mitigate the risks. Current controls primarily rely on SharePoint administrators and owners and Teams owners reviewing and updating permissions. OIT has supported them with timely direction and guidance. Limited data loss prevention capabilities are also in use. OIT has published guidance and instructions in response to the evolving risk, summarized below.

- In February 2022, OIT published guidance to users on protecting personal data in Microsoft Teams, OneDrive, and SharePoint Online, with links to instructional materials.[61]
- In March 2023, OIT published frequently asked questions on SharePoint permissions.[62]
- In April 2023, OIT emailed a set of instructions required for all Teams and SharePoint owners and administrators. The actions were to improve the security of content in Teams, SharePoint, and OneDrive and were critical for those sites that contain personally identifiable information (PII) and protected health information (PHI).[63]
- In September 2023, the principal deputy assistant secretary for information and technology issued a memorandum, “Enhancing Privacy Protections in the Use of Microsoft Teams and SharePoint,” to under secretaries, assistant secretaries, and other key officials. The memo provided guidance on the secure setup and use of Teams and SharePoint permissions when a website contains PII, PHI, and sensitive personal information, and it included tasks to be completed by a certain date. The memorandum emphasized that SharePoint Online may not be used as the official record storage location for a Privacy Act system of records. Shared drives that have been restricted to personnel who have a need to know may be used as the official record storage location. Also, SharePoint administrators and owners are responsible for site content, including review of their Teams and SharePoint sites to determine

[61] VA OIT, “Protecting Personal Data in Microsoft Teams, OneDrive, and SharePoint Online,” February 4, 2022.

[62] VA OIT, “SharePoint Permissions FAQ,” updated/reviewed March 31, 2023.

[63] VA OIT Communication Tools List, “Action Required for all Teams and SharePoint Owners/Admins,” email, April 27, 2023.

whether PII, PHI, or sensitive personal information is used and assure that appropriate permissions are in place.[64]

- In September 2023, VA sent an email to all VA mailboxes announcing that to address potential vulnerabilities and safeguard sensitive data across the enterprise, it changed the privacy default setting for all Microsoft Teams from public to private. Additionally, all public Teams would be automatically converted to private and users would be able to launch only private Teams.[65]
- In December 2023, OIT published guidance to users on sharing securely in OneDrive.[66]
- In January 2024, OIT published guidance to users on discovering and limiting permissions on OneDrive.[67]
- In February 2024, OIT published guidance on switching Teams from public to private access to reflect the policy change, adding or removing additional owners on a personal OneDrive, and the Microsoft Delve tool. The Delve guidance emphasized that Delve does not change privacy settings but does allow users to see content that was shared in Teams meetings, in OneDrive, or on SharePoint sites.[68]
- In March 2024, OIT informed its staff of the Data Loss Prevention and Data Discovery Analytics and Labeling production pilot for labeling. This represented an initial effort to automate the identification of VA sensitive data.[69]
- In April 2024, OIT published instructions to administrators on how to remove a SharePoint user group that would grant access to all VA users.[70]
- In June 2024, OIT published instructions for users to add sensitivity labels to files in Microsoft Office 365 products (Outlook, Word, Excel, and PowerPoint).[71]

[64] Principal deputy assistant secretary for information and technology (005), “Enhancing Privacy Protections in the Use of Microsoft Teams and SharePoint,” memorandum to under secretaries, assistant secretaries, and other key officials, September 8, 2023.

[65] VA, “VA Changes All Microsoft Teams from Public to Private,” email, September 28, 2023.

[66] VA OIT, “OneDrive: Sharing Securely in OneDrive,” December 18, 2023.

[67] VA OIT, “OneDrive: Discovering and Limiting Permissions,” January 29, 2024.

[68] VA OIT, “MS [Microsoft] Teams: Request to Switch a Private Team to a Public Team,” February 6, 2024; “OneDrive: Add or Remove Additional Owners on your Personal OneDrive,” February 12, 2024; “Delve: General Information for the M365 Delve Tool,” February 28, 2024.

[69] VA OIT, “Varonis Automated Labeling of VA Sensitive Data,” March 19, 2024.

[70] VA OIT, “SharePoint: Remove the Group that Grants Access to All VA Users,” April 22, 2024.

[71] VA OIT, “M365: Adding Sensitivity Label,” June 4, 2024.

To mitigate risks, OIT has implemented a SharePoint governance site that identifies roles and responsibilities for SharePoint leaders, users, administrators, owners, and content-owning organizations; guidance on SharePoint information architecture; and links to SharePoint training. This site is not publicly accessible. OIT has also published a SharePoint Online Help Desk Tool that catalogs SharePoint sites and their administrators within the Microsoft Office 365 Multi-Tenant system. This tool is not publicly accessible.

According to program officials, VA's data loss prevention program also has some capabilities that could help identify excessive permissions and unauthorized content. Data loss prevention is a collection of tools and policies that can be used within Office 365 to monitor and notify users about specific types of sensitive information.[72] Examples of defined or structured content include social security numbers, Drug Enforcement Agency numbers, International Classification of Diseases codes, credit card numbers, US bank account and routing numbers, US driver's license numbers, and internet protocol addresses. Sensitive information can also be found in unstructured content. These tools and policies can be configured to identify sensitive information within Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams.

[72] VA OIT, "DLP [data loss prevention]: Information on the Purpose of Data Loss Prevention," March 4, 2024.

Appendix D: VA Management Comments

Department of Veterans Affairs Memorandum

Date: March 6, 2025

From: Acting Assistant Secretary for Office of Information and Technology and Chief Information Officer (005)

Subj: Improper Sharing of Sensitive Information on Cloud-Based Collaborative Applications (Draft Report) (VIEWS 12417924)

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

1. Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, Improper Sharing of Sensitive Information on Cloud-Based Collaborative Applications (Project Number 2024-01330-AE-0056).

2. The Office of Information and Technology (OIT) submits the attached written comments. OIT acknowledges the OIG's findings, concurs with the OIG's recommendations, and provide a corrective action plan and target implementation date or closure evidence for each of the OIG's recommendations to the Department.

The OIG removed point of contact information prior to publication.

(Original signed by)

Eddie Poole

Attachment

Attachment

Office of Information and Technology
Comments on Office of Inspector General Draft Report,
“Improper Sharing of Sensitive Information on Cloud-Based Collaborative Applications”
Project Number 2024-01330-AE-0056

(VIEWS 12417924)

Recommendation 1: Take corrective actions to ensure that facilities and programs remove unauthorized sensitive information from collaborative application sites.

Comments: The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs. OIT completed a basic privacy configuration change for all Microsoft Teams sites and SharePoint online sites, setting them by default to “private.” OIT will also publish an action memorandum that will mandate SharePoint security essentials training for all VA organizational users and clarify the role of SharePoint owners in reviewing any sensitive information contained on their sites with oversight from the local Privacy Officer and Information System Security Officer.

Expected Completion Date: June 30, 2025.

Recommendation 2: Direct facilities and programs to standardize SharePoint administration, inventory and consolidate their SharePoint sites, and enforce the recommended architecture to better control access and content at the facility or program level.

Comments: Concur. Centralized SharePoint platform administration is now in place. OIT executes and enforces user training and awareness on a routine basis to ensure a continued understanding of privacy needs at the facility level.

Completed Date: May 31, 2024.

VA requests closure of Recommendation 2.

Recommendation 3: Implement enforcement mechanisms to ensure that facilities and programs are following standardized processes to secure SharePoint and Teams sites.

Comments: Concur. VA OIT deployed privacy labels as the default and retrofitted all related sites with the private label. OIT uses training and awareness of community practice to enforce permission reliability.

Completed Date: May 31, 2024.

VA requests closure of Recommendation 3.

Recommendation 4: Expand roles and responsibilities of facility and program information system security officers and privacy officers to include the routine review of SharePoint and Teams site permissions and content.

Comments: Concur. VA SharePoint site administrators and owners will establish SharePoint and Teams sites as outlined in the VA SharePoint governance roles, responsibilities, and terms. VA SharePoint site administrators and owners shall consult with the facility privacy officer when personally identifiable information and personal health information will be used. To further document the roles of the facility and program Information System Security Officers and Privacy Officers, OIT will publish an action memo clarifying the role of SharePoint and Teams owners in routinely reviewing their site permissions and content with oversight from the local Privacy Officer and Information System Security Officer.

Expected Completion Date: November 30, 2025.

Recommendation 5: Implement automated tools and policies, supported with training, to enable the timely and routine detection and correction of improper sharing and unauthorized content throughout VA.

Comments: Concur. OIT is piloting advanced tooling to automate review and awareness of site permissions errors; this will allow for automatic remediation, alerting, and reporting.

Expected Completion Date: Pilot was completed in December 2024. Full implementation date is pending pilot outcomes in fiscal year 2025.

Recommendation 6: Mandate standardized training for SharePoint administrators and owners to clarify and reinforce data security requirements.

Comments: Concur. OIT implemented a workflow requiring users to complete SharePoint security essentials training before site delivery. OIT will publish a memorandum to mandate the training for standardization purposes. OIT will additionally explore adding the training as an annual requirement for all organizational users in the VA Talent Management System and as a part of the Rules of Behavior.

Expected Completion Date: September 30, 2025.

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 Keith Hargrove George Ibarra Tim Moorehead Kim Moss Nick Neagle
Other Contributors	Allison Tarmann Rashiya Washington

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

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

OIG reports are available at www.vaoig.gov.