US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Audit of Security and Access Controls for the Patient Advocate Tracking System-Replacement

Audit	25-01781-71	July 7, 2026

OUR MISSION

To conduct independent oversight of the Department of Veterans Affairs that combats fraud, waste, and abuse and improves the effectiveness and efficiency of programs and operations that provide for the health and welfare of veterans, their families, caregivers, and survivors.

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.

Executive Summary

Patient advocates, who support communication between veterans and staff at Veterans Health Administration (VHA) facilities, use the Patient Advocate Tracking System-Replacement (PATS-R) to document their contacts with veterans. The system collects and maintains veterans' sensitive personal information, which VA is legally obligated to protect.[1] The VA Office of Inspector General (OIG) initiated this audit to determine whether PATS-R had sufficient security controls from March 2025 through January 2026 to ensure information in the system was safeguarded in accordance with federal law and information security standards. While the OIG recognizes that VHA is undergoing a reorganization to improve care and operations, this report's findings and recommendations are important to ensure VHA and the Office of Information and Technology (OIT) safeguard sensitive information, promote information security, and strengthen governance.

At the beginning of this audit in March 2025, the OIG team informed OIT senior officials that the low-impact categorization for PATS-R may be inappropriate, and the team continued to brief officials about its initial findings during the subsequent months. In response, VA officials (1) updated the PATS-R risk categorization to moderate impact with some additional controls to protect privacy; (2) demonstrated to the OIG team in December 2025 that the system now restricts access to medical records for unauthorized users; and (3) automated the deactivation process for expired or inactive accounts to ensure assigned users are current and have only the access they need.

While this progress is notable, the OIG made five recommendations in this report to ensure PATS-R is correctly assessed and categorized, that system users have a continued business need to access veterans' medical records, that user roles are correctly configured, and that users have updated guidance. VA concurred with all recommendations, provided action plans, and requested closure of recommendation 1.

What the Audit Found

OIT staff inappropriately assigned PATS-R a security categorization impact value of "low risk," which resulted in fewer security controls than would be appropriate for a system that contains veterans' sensitive personal information. This occurred when the oversight of PATS-R was transferred in November 2023 from OIT's Benefits and Memorial portfolio to the VA Office of Enterprise Integration, which was renamed the Office of Strategic Initiatives in September 2025. At that time, the system was also transferred from a stand-alone, physical environment to a cloud-based environment. The OIG team found that during the transition, OIT did not go through

[1] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073.

all the necessary steps of the risk management framework, including reevaluating the privacy impact assessment.[2] The low-risk categorization potentially jeopardized the confidentiality, integrity, and availability of veterans' data. The OIT information system security officer said control mitigations and an elevated risk categorization (to "moderate" impact) were put in place in March 2025 as a result of the OIG's preliminary findings. However, the moderate risk level may still be insufficient because access controls were not working as intended and because the program office was not consistently reviewing users to ensure they were authorized to use PATS-R based on their roles.

The OIG team also found that

- the security controls in PATS-R designed to restrict access to medical records were not functioning correctly, which allowed access to medical records for users who were not authorized;
- many system users who needed PATS-R access to do their job told the OIG team they did not use PATS-R to access the necessary medical records; and
- the Office of Patient Advocacy did not provide sufficient guidance to regional networks or medical facilities to provision and review roles, remove unused accounts, and update training materials.

The deactivation process to remove users from PATS-R was also not automated until after the OIG team briefed the Office of Patient Advocacy in May 2025.

Next Steps

The OIG found the action plans were responsive to the intent of the recommendations. Based on the actions taken and evidence provided by VA, the OIG considers recommendation 1 closed. The OIG will continue to monitor VA's implementation of corrective actions and close the remaining recommendations when sufficient evidence demonstrates progress in meeting the intent of the recommendations and addressing the identified risks.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

[2] VA Handbook 6500, *Risk Management Framework for VA Information Systems VA Information Security Program*, February 24, 2021.

Contents

Abbreviations

eMASS	Enterprise Mission Assurance Support Service
FISMA	Federal Information Security Modernization Act
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
PATS-R	Patient Advocate Tracking System-Replacement
VHA	Veterans Health Administration
VISN	Veterans Integrated Service Network

Introduction

VA is required by law to ensure the safe sharing of sensitive personal information within its systems.[3] The Patient Advocate Tracking System-Replacement (PATS-R)—one of VA's electronic systems of record—documents contacts between Veterans Health Administration (VHA) patient advocates and veterans, beneficiaries, or their representatives. PATS-R collects, uses, disseminates, creates, and maintains veterans' sensitive personal information and communicates with systems internal to VA. Additionally, PATS-R communicates with the Computerized Patient Record System. This record system displays protected health information and personally identifiable information and enables clinicians to enter, review, and continuously update all order-related data connected with any patient.

- **Sensitive personal information** includes information that is individually identifiable, such as health data and personal details that are privacy-protected.
- **Personally identifiable information** is information that can distinguish an individual's identity, such as their name, social security number, or biometric records, either alone or when combined with other personal or identifying information linkable to a specific individual, such as date and place of birth or mother's maiden name.[4]

Establishing appropriate security controls for information systems like PATS-R is critical to complying with federal law and reducing the risks of unauthorized use or disclosure of veterans' sensitive personal information.[5] Security controls are the safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of a system and its information.[6]

The VA Office of Inspector General (OIG) has issued two reports related to the Patient Advocacy Program and two on VA cloud security over the past nine years (see appendix A). This audit was initiated to determine whether PATS-R had sufficient security controls from March 2025 to January 2026 to ensure confidentiality and data integrity and to safeguard veterans' sensitive personal information in accordance with federal law and information security standards.

[3] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073.

[4] National Institute of Standards and Technology (NIST) Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.

[5] FISMA.

[6] NIST Special Publication 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.

The OIG recognizes that VHA is undergoing a reorganization to enhance veteran care and delivery, operational consistency, and communication and decision-making. The OIG's findings and recommendations in this report can help inform these efforts, promote information security, and improve governance.

Patient Advocacy Program

The Patient Advocacy Program was established in 1990 to help advance VHA's efforts to improve customer service, help veterans access quality care, and provide a way to address healthcare delivery issues. The program seeks to ensure patients' complaints are identified, resolved, classified, and used to improve overall service to veterans. The program promotes patient satisfaction and contributes to VHA initiatives aiming for world-class customer service. The Office of Patient Advocacy was established in June 2017 to ensure patient advocates work on behalf of veterans seeking and receiving healthcare services from VHA.[7] The office standardizes processes, procedures, and training to support patient advocacy, establishes operational models, establishes a data framework to support leaders' awareness and decision-making, and ensures VHA fulfills legal responsibilities.

Governance Structure and Responsibilities

VHA's program policy defines the governance structure and responsibilities for managing the Patient Advocacy Program.[8] Staff at the national program office, in the regional Veterans Integrated Service Networks (VISNs), and at local medical facilities share responsibility for achieving program goals.

According to a VA Office of Information and Technology (OIT) PATS-R information system owner, who is the employee responsible for procuring, developing, integrating, modifying, operating, and maintaining the system, PATS-R replaced the original Patient Advocate Tracking System, which was decommissioned in November 2021. Two years later, PATS-R was transferred from the OIT Benefits and Memorial portfolio's Customer Relationship Management platform to the Veterans Experience Integration Solution platform, which at the time of this audit was operated by the VA Office of Enterprise Integration. The VA Office of Enterprise Integration was renamed the Office of Strategic Initiatives in September 2025. According to OIT, as of November 2023, VA's Veterans Experience Services is responsible for oversight of PATS-R. The Veterans Experience Integration Solution platform supports application connections to VA enterprise systems to retrieve veterans' data. Finally, according to the Patient Advocacy Program policy, each medical facility's PATS-R coordinator is responsible for adding, modifying, and removing system user accounts.

[7] Comprehensive Addiction and Recovery Act of 2016, Pub. L. No. 114-198, 130 Stat. 695.

[8] VHA Directive 1003.04, *VHA Patient Advocacy*, November 9, 2023.

VA's Governance, Risk, and Compliance Tool

During the time frame covered by this audit, VA used the Enterprise Mission Assurance Support Service (eMASS), a web-based governance, risk, and compliance tool, to generate a system security authorization package and automate the setting of security controls for VA systems in line with the National Institute of Standards and Technology's (NIST) risk management framework. The eMASS tool includes dashboard reporting, workflow automation, and continuous monitoring that replicates steps in the risk management framework. For instance, eMASS can establish process controls to obtain authorizations to operate for applications and systems. In addition, eMASS automatically calculates confidentiality, integrity, and availability levels for some information types based on risk assessment results, including the system privacy impact assessment and the business impact analysis.

- A **privacy impact assessment** determines the risks and effects of collecting, maintaining, and disseminating information in an identifiable form in an electronic system and examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.[9]
- A **business impact analysis** assesses operational functions and the effect that a disruption might have on them.[10]

According to federal standards, security categories should be based on the potential organizational impact if information and systems are jeopardized by events such as the unauthorized disclosure, modification, destruction, or disruption of access.[11]

NIST's Risk Management Framework

VA is required to comply with the Federal Information Security Modernization Act (FISMA) of 2014, which mandates that federal agencies secure information and systems that support their operations and assets.[12] NIST develops standards and guidelines for information security across the federal government. These standards, along with other publications, lay out the framework for managing risk through the design, development, implementation, operation, and disposal of information systems.[13]

---

[9] "Privacy impact assessment" (web page), NIST, Computer Security Resources Center, accessed July 29, 2025, https://csrc.nist.gov/glossary/term/privacy_impact_assessment.

[10] "Business impact analysis" (web page), NIST, Computer Security Resources Center, accessed July 29, 2025, https://csrc.nist.gov/glossary/term/business_impact_analysis.

[11] Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

[12] FISMA.

[13] NIST Special Publication 800-37, rev. 2, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy*, December 2018.

At VA, OIT is responsible for following NIST's risk management framework.[14] This includes completing a privacy impact assessment and business impact analysis as part of the initial step to prepare each information system. Figure 1 illustrates the seven steps of NIST's risk management framework life cycle.[15]

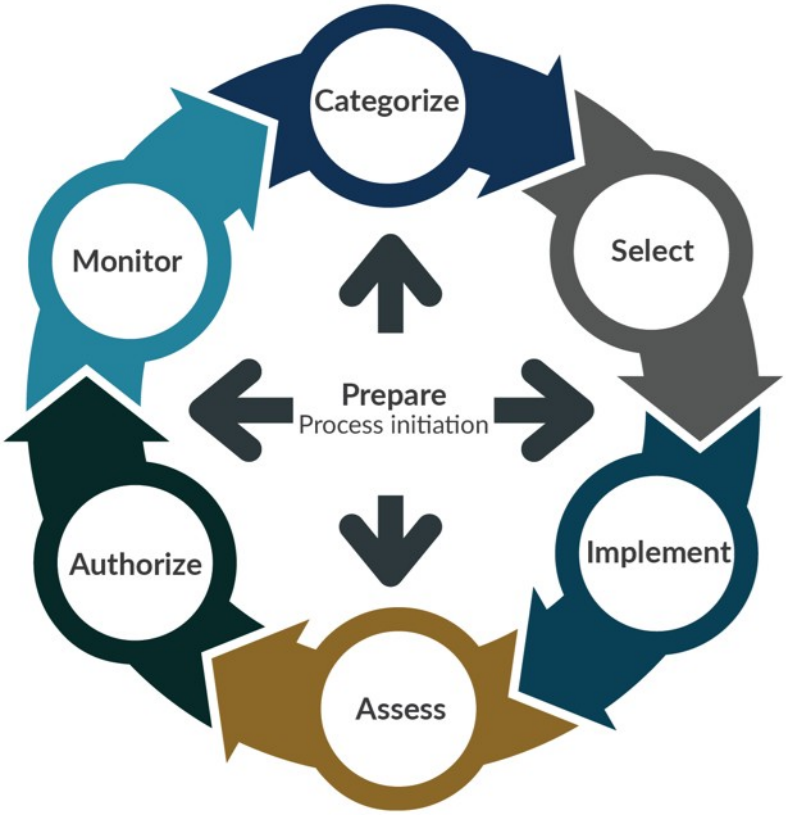

Figure 1. *VA OIG overview of the risk management framework.*
Source: NIST Special Publication 800-37.

The exact security controls that apply to a given system depend on the risk level of the data the system will contain.[16] Security categorization is a crucial part of the framework and a key step for understanding and documenting a system's characteristics and potential impacts.[17] The framework is required even for minor applications like PATS-R. NIST defines a minor application as an application that is not a "major application" but that still requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized

[14] VA Handbook 6500, *Risk Management Framework for VA Information Systems VA Information Security Program*, February 24, 2021.

[15] For more details on the risk management framework, see appendix A.

[16] NIST Special Publication 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020; VA Handbook 6500.

[17] NIST Special Publication 800-37, rev. 2.

access to or modification of the information in the application.[18] According to eMASS, OIT classified PATS-R as an assess-only minor application.

The NIST risk management framework process begins with a privacy threshold analysis, which identifies information systems that include sensitive personal information and shows whether a privacy impact assessment is needed.[19] A privacy impact assessment identifies privacy risks and their effects for an information system and should identify and evaluate processes to mitigate risk at every stage of system development. This assessment is required before VA can develop or procure information technology that collects, maintains, or disseminates personally identifiable information.[20] VA also uses the privacy analysis and assessment to evaluate the type of information that will be contained in a given system and to determine the appropriate security categorization level.[21]

- **Information type** (such as privacy, medical, proprietary, financial, investigative, contractor sensitive, or security management) is defined by an organization or, in some instances, by law, executive order, directive, policy, or regulation.[22]
- **Categorization levels** relate to the degree of privacy and security needed to avoid improper disclosure or misuse of the information or data; categorization takes into account the potential adverse effects of a breach on VA's operations, assets, or the individuals identified in the system.

For more information on security standards and guidelines, see appendix A.

[18] "Minor Application" (web page), NIST, Computer Security Resources Center, accessed July 9, 2025, https://csrc.nist.gov/glossary/term/minor_application.

[19] NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010; VA Handbook 6508.1, *Procedures for Privacy Threshold Analysis and Privacy Impact Assessment*, July 30, 2015.

[20] VA Directive 6508.1.

[21] NIST Special Publication 800-122.

[22] Federal Information Processing Standards Publication 199.

Results and Recommendations

Finding: VA's Security and Access Controls for PATS-R Do Not Effectively Safeguard Veterans' Sensitive Information

The OIG found that the PATS-R security and access controls were inadequate during the audit period, from March 2025 through January 2026. In particular, the system's security impact level was miscategorized and was not reevaluated until after OIT officials took action during the audit—and those efforts might still be insufficient. The absence of required security assessments and privacy impact analyses is a serious concern and potentially jeopardized the confidentiality, integrity, and availability of veterans' sensitive personal information. Furthermore, various access controls were not functioning as intended to ensure that only those system users who need access to patient records have such access.

Without effective security and access controls and without sufficient oversight and guidance, the Office of Patient Advocacy cannot effectively fulfill its legal obligation to protect veterans' sensitive information from unauthorized access.

What the OIG Did

The audit team reviewed results from the PATS-R security privacy threshold analysis and the privacy impact assessment to evaluate whether the system had adequate security controls and oversight when it was set up in eMASS. To determine whether OIT's decision to host PATS-R in a cloud-based environment met all applicable security requirements, the team also reviewed the system's business impact assessment and system security plan. The team interviewed the PATS-R information system security officer and the information system owner, as well as 23 system users, and reviewed selected security and privacy controls to determine whether they were functioning as intended. In addition, in May and June 2025, the team surveyed a statistical sample of VA employees who use PATS-R so the OIG could evaluate whether (1) they knew medical records could be accessed through the system and whether (2) removing that privilege would affect their job responsibilities. See appendix B for more information regarding the audit's scope and methodology and appendix C for information on statistical sampling.

Security Controls

At the start of this audit in March 2025, the OIG team informed OIT that the low-impact risk categorization for PATS-R may be inappropriate. The OIG team learned that the January 2023 privacy impact assessment conducted by the privacy officer, PATS-R information system owner, and information system security officer recommended OIT assign a "high"-impact rating to PATS-R. A high value is appropriate when improper disclosure of information "could be expected to have a severe or catastrophic adverse effect" on organizational operations,

organizational assets, or individuals.[23] However, OIT officials did not follow the assessment rating and instead kept the system categorized as "low" impact—which means "the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect."[24]

The PATS-R information system owner, who is responsible for procuring, developing, integrating, modifying, operating, and maintaining the system, informed the OIG team that PATS-R was moved to a new cloud-based environment under the VA Office of Enterprise Integration in November 2023. According to NIST publications and VA policy, PATS-R should have undergone a new system impact assessment after it was moved and oversight was transferred. The system owner did not reevaluate PATS-R's security objectives and impact level as required. While the system owner acknowledged in September 2025 that the PATS-R security categorization should have been reevaluated when oversight was transferred, she could not justify why the reassessment was not done.

The PATS-R information system owner further acknowledged that PATS-R did not go through all the steps of the risk management framework process when system oversight was transferred from OIT's Benefits and Memorials portfolio to the VA Office of Enterprise Integration. The system owner said that when ownership of PATS-R changed, the Veterans Experience Integration Solutions team asked for a memo documenting completion of step 1 of the risk management framework (data security categorization); however, no such memo existed. A data security categorization memo would have provided an official designation of potential impact on information systems. During this audit, OIT did not provide the OIG team with any documentation to confirm the completion of the risk management framework steps when oversight was transferred or with a record of the chosen impact levels.

The PATS-R information system owner explained that because OIT considered PATS-R an assess-only minor application, the system inherited controls from its new hosting platform.[25] However, NIST advises that agencies are expected to exercise judgment in determining which of their applications are minor and in ensuring that the security requirements of even minor applications are addressed as part of a system security plan.[26]

According to OIT procedures, before an assess-only minor application can be hosted on the VA network, it must receive an approved security assessment package and have a security category of low or moderate. Assess-only minor applications, though, should also receive security assessments because of the risk and magnitude of harm that can be caused due to the loss,

---

[23] "High impact system" (web page), NIST, Computer Security Resources Center, accessed June 12, 2025, https://csrc.nist.gov/glossary/term/high_impact_system; Federal Information Processing Standards Publication 199.

[24] "Low impact system" (web page), NIST, Computer Security Resources Center, accessed June 12, 2025, https://csrc.nist.gov/glossary/term/low_impact_system.

[25] OIT, *Assess Only Requirements Standard Operating Procedure*, January 30, 2025.

[26] NIST Special Publication 800-18, rev. 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

misuse, unauthorized access, or modification of the data contained in the application. While PATS-R did receive an approved security assessment in January 2023, OIT officials said they did not heed that assessment's recommended impact level nor did they follow all the risk management framework steps when the Veterans Experience Integration Solution team began overseeing PATS-R later that year. As a result, the system was inappropriately categorized and did not have the required security and access controls applied.

According to the PATS-R information system owner, because the reassessment was not done, PATS-R remained at a low-risk level in eMASS for an extended period with no additional security controls to mitigate the risks of the system's new cloud-based environment. After the OIG team discussed PATS-R's low-risk categorization with OIT officials in March 2025, OIT officials completed a new privacy impact assessment in April 2025—at which time, the assessment recommended PATS-R be categorized as "moderate" in eMASS with additional controls to protect privacy. OIT officials set the system to moderate and said they assumed the risk level was appropriate because PATS-R has role-based access controls. Furthermore, an Office of Patient Advocacy official said their staff would periodically review users to determine whether they still needed access to the system.

The absence of the security risk reassessment and a new privacy impact assessment when PATS-R ownership was transferred is a serious concern. In particular, ignoring a privacy impact assessment can put veterans' sensitive personal information at risk. Because OIT did not complete the required assessments in a timely manner, it incorrectly categorized the PATS-R security risk and underestimated the potential impact of security breaches or other incidents. Ensuring that the risk categorization accurately reflects the Office of Patient Advocacy's practices would provide OIT and VA with assurance that PATS-R has the necessary controls to protect veterans' personal information.

Information Spills

Even though OIT officials upgraded PATS-R to a moderate risk categorization after the OIG team notified them of the issue, OIT still needs to ensure sufficient controls are implemented to prevent information spills. A spill is when information thought to be of a certain classification or impact level is transmitted to a system and subsequently determined to be of a higher classification or impact level, which requires corrective action.[27]

This is important because PATS-R, which is now categorized as a moderate-impact security system, communicates with the Computerized Patient Record System—a high-impact security system that contains sensitive personal information. In recommending that PATS-R should have a "high" categorization, the privacy impact assessment from January 2023 found that PATS-R contains veterans' sensitive personal information, including medications and medical records.

[27] NIST Special Publication 800-53, rev. 5.

According to that assessment, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft might result.

The new moderate risk level that OIT officials gave PATS-R in March 2025 falls short of the recommendations in the January 2023 privacy impact assessment. Meanwhile, if PATS-R does not have an appropriate security categorization, OIT may not have the necessary and complete controls in place to protect veterans' sensitive information.

The OIG's first recommendation is for OIT to enforce the VA policy that requires officials and staff to reassess an authorization when a significant change affects the security or privacy posture of an application system. Second, the OIG recommends that OIT officials reevaluate the risk determination for PATS-R and determine the appropriate security categorization level based on the sensitive personal information accessed in the system and based on the System Security Categorization Report, which designates the potential impact category for information systems.

Access to Medical Records

According to VHA, employees whose job responsibilities include complaint resolution need access to medical records in PATS-R.[28] However, the OIG team found that VA staff who are PATS-R users can access veterans' medical records through PATS-R, even though they did not have a need to know. This included users whose access to medical records should have been restricted because of their job responsibilities. NIST requires role-based access controls so users may access sensitive personal information only on a need-to-know basis. The team notified VHA and OIT officials in May 2025 about the PATS-R access control deficiency. OIT told the OIG team that it planned to correct the deficiency by October 2025. On December 11, 2025, OIT demonstrated to the OIG team that the system controls were working as intended to restrict access to medical records for unauthorized users.

Restricting Access

Each medical facility's PATS-R coordinator is able to set up user accounts that hide medical records to restrict access when a given user's job does not require them to access medical records. One facility PATS-R coordinator said he developed a questionnaire to determine a user's role and whether that user needs access to medical records through PATS-R based on their job description. However, according to patient advocacy staff, each VISN has its own methods to verify user roles and access needs, so there is no standardized process. Figure 2 shows a screenshot of the user request form in PATS-R, at the time of this audit, with the option to hide medical records.

[28] NIST Special Publication 800-53, rev. 5.

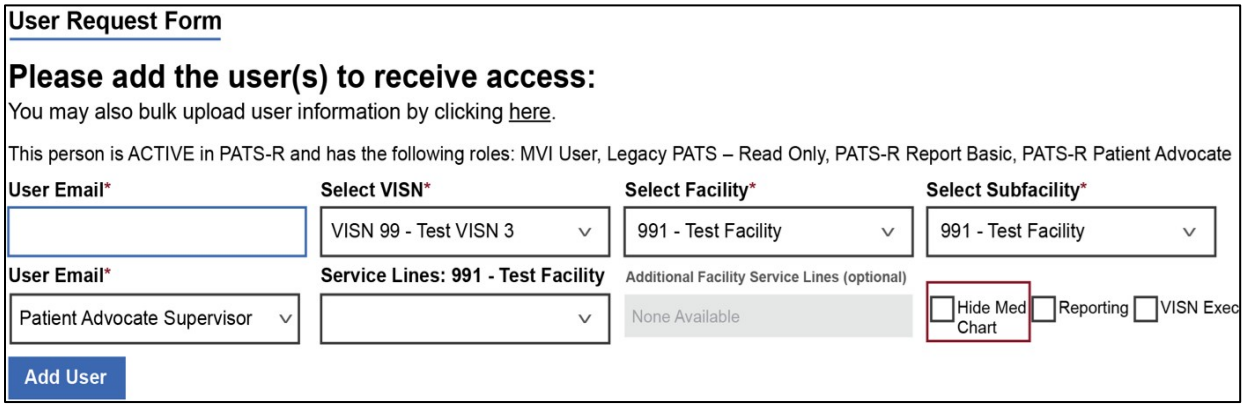

Figure 2. *Screenshot of the user request form in PATS-R and its "Hide Med Chart" function.*
Source: VA PATS-R Licensing and Provision Application (User Management App).

The audit team interviewed nine service-level advocates who use PATS-R: six clinical and three nonclinical. Service-level advocates can create cases and resolve veterans' requests related to care they receive at VA medical facilities. According to a veteran experience officer, a case is the entirety of a patient's concerns, which can include multiple requests potentially addressed by different service lines. These service lines organize patient care around specific diseases, interventions, or populations, such as inpatient or volunteer services.

The team found that the three nonclinical PATS-R service-level advocate users still had access to medical records. For example, one user said he had changed roles but did not lose access to medical records—a nurse manager became a facility manager and therefore no longer needed access to medical records, but did not lose access in PATS-R. The PATS-R coordinator said that after the audit team notified him in April 2025 about this particular user's unnecessary access to medical records, he changed the user role to hide medical records. However, a follow-up demonstration in May 2025 showed the user still had access even after the "hide med chart" restriction was placed on the user's account. VA officials acknowledged that the function to hide medical charts was not working as intended, and they planned to implement multiple changes to correct the issue, including hiding medical records by default. As previously mentioned, the OIG team confirmed OIT corrected the PATS-R system access controls deficiency, which included removing default access to medical records for unauthorized users. At the time of this report's publication, a provisioner must explicitly select the box to obtain access to medical records.

Accessing Records

Through the provisioning process, users can be given access to view medical records, demographics, and medication information. Of the nine service-level advocates the OIG team interviewed, six needed access to medical records as part of their job duties. These six users—which included nurse managers and social workers—already had access to medical records. However, three of the six users said they used the Computerized Patient Record System or the Joint Longitudinal Viewer (a system of record shared with the Department of Defense) rather

than PATS-R to view a veteran's medical records when determining how to address a complaint. Further, three of the six users did not know they could view medical records in PATS-R.

The OIG team surveyed a statistical sample of 261 VHA staff who were identified as active PATS-R users nationwide. The survey questions were designed to evaluate whether the users had access to medical records through any VA system. Users were also asked whether they knew before receiving the survey that medical records could be accessed through PATS-R and whether removing that access would affect their job duties.

As shown in figure 3, most respondents (77 percent) said they never used PATS-R to view medical records and were not aware the system had that functionality. Eighty-nine percent said losing medical record access in PATS-R would not affect their job responsibilities.

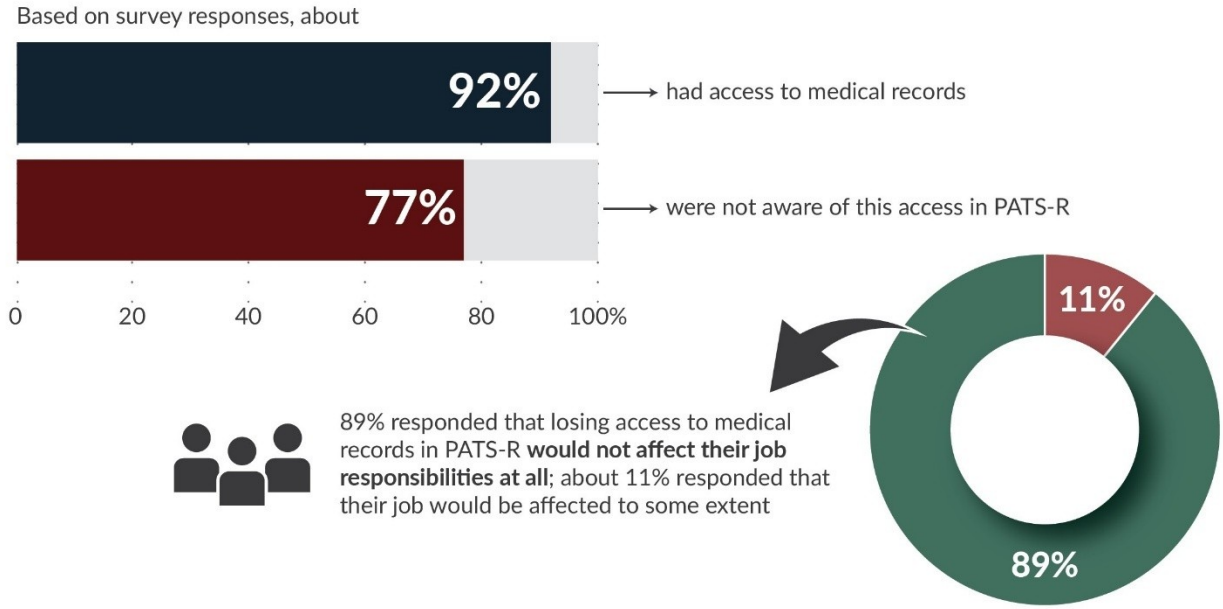

Figure 3. *Survey results from PATS-R users.*

Source: VA OIG analysis of survey results.

The OIG's third recommendation calls on the under secretary for health to reevaluate whether there is a continued business need for maintaining users' access to medical records in PATS-R.

Guidance and Oversight

The OIG team found that the Office of Patient Advocacy did not provide sufficient guidance to VISNs or medical facilities for provisioning, reviewing roles, and removing unused accounts. Furthermore, according to a VISN PATS-R coordinator, the Office of Patient Advocacy did not provide updated training materials. Finally, the Office of Patient Advocacy did not create ways to monitor and hold the VISNs and medical facilities accountable for ensuring appropriate access

to veterans' medical records. Because the Office of Patient Advocacy did not provide effective oversight and guidance, networks and medical facilities may be inconsistently managing PATS-R users.

Reviewing Roles and Removing Accounts

According to the VISN 19 PATS-R coordinator and the program manager for the Office of Patient Advocacy, PATS-R user roles and job descriptions are not consistently reviewed or updated, especially for users who changed positions or those who needed their access level changed in the system. NIST requires enforcing the principle of least privilege for role-based access controls so that access controls are managed based on an individual's job function and access is revoked when an individual leaves the job or is reassigned.[29]

According to a facility PATS-R coordinator, the service line chiefs are expected to notify the coordinator when an employee's role changes. However, he said the Office of Patient Advocacy does not provide specific guidance for who is responsible for creating user accounts and reviewing roles in PATS-R. The Office of Patient Advocacy's program manager provided examples of where they discussed reviewing user roles and confirmed that the office provides quick reference guides for training, including setting up accounts in PATS-R. But the manager also acknowledged that the guide does not issue specific instruction on reviewing roles.

The facility PATS-R coordinator further explained his process for reviewing users on a quarterly basis and issuing a user list to the service line chiefs. He said he expects the chiefs to identify users who should keep access and those who have left the service line. However, only two PATS-R users at the coordinator's facility mentioned seeing requests to verify that they still needed access. The OIG team found that one PATS-R user account at the facility should have been inactive because the user said she had not accessed the system in over one year.

NIST requires organizations to disable accounts that have expired or are inactive.[30] VHA's process to remove users from PATS-R was manual—not automated—which increases the risk of inconsistent oversight. After the OIG team discussed the account deactivation process with the Office of Patient Advocacy in May 2025, according to OIT, this process was automated and an auto-deprovisioning routine was established to identify user accounts that were inactive for 90 days or more. These accounts were then deprovisioned, and OIT staff said this process will occur monthly going forward.

While OIT has informed the OIG that the deactivation process was automated for expired or inactive accounts, clear guidance telling the PATS-R coordinators to review user roles is still needed to help ensure staff maintain appropriate access. Without a recurring review of user roles,

[29] NIST Special Publication 800-53, rev. 5.

[30] NIST Special Publication 800-53, rev. 5.

VHA cannot ensure system roles are correctly configured to allow only authorized access for users. Therefore, the OIG's fourth recommendation calls on the under secretary for health to institute a process to ensure user roles are regularly reviewed and correctly configured to allow only authorized access to PATS-R.

Training Materials

A VISN PATS-R coordinator also told the audit team that much of the PATS-R training was outdated or unavailable. According to the Office of Patient Advocacy's program manager, a monthly community-of-practice call is open to all PATS-R users and a SharePoint site provides access to quick reference guides and training materials. The coordinator said that, while there is training available, most of the information and slides on the sites were outdated.

The OIG team confirmed that some user guides and training materials had not been updated for several years; the materials also referred to the previous, obsolete system instead of PATS-R. For example, the team found the Patient Advocate Training Program & Checklist contained broken hyperlinks to source information and outdated guidance, a point of contact listing for training resources was no longer valid, and some memos related to processes and programs were draft copies and incomplete. The program manager said training materials are typically reviewed annually but acknowledged that there had not been any updates in 2025, and also noted that there was no published guidance on how and when to add or remove users from the system. The program manager added that the office does not provide any guidance for determining roles and access for PATS-R users because the responsibility to do so lies with each individual facility. Recommendation 5 addresses the need for VHA to update PATS-R user guides and training materials.

Conclusion

Although PATS-R allows access to medical records and other sensitive information, VA officials miscategorized the system as low risk. This occurred because VA did not complete all risk management framework steps when oversight of PATS-R was transferred to the Office of Enterprise Integration. The low-risk categorization resulted in fewer security and access controls than would have been appropriate to protect veterans' sensitive personal information. OIT updated PATS-R's categorization to moderate risk after the team informed OIT of PATS-R's low security categorization, but that level still may be inadequate to safeguard veterans' sensitive personal information. The PATS-R information system owner said OIT is reassessing the system's categorization to determine the appropriate risk level.

Additionally, existing security controls in PATS-R—such as restricting access to medical records for staff who do not need it—are not functioning as intended, and according to the Patient Advocacy Program manager, no guidance exists to help staff review users' access to ensure that the appropriate level of access is maintained. Finally, the team found that some user guides and training materials were outdated, which leaves VISNs and facilities without the instruction they need to ensure user access is appropriate.

Recommendations 1–5

The OIG recommends the assistant secretary for OIT, who also serves as chief information officer, take the following actions:[31]

1. Ensure that authorizations are reassessed when a significant change affects the security or privacy posture of an application, consistent with the requirements of VA Handbook 6500.
2. Reevaluate the risk determination for the Patient Advocate Tracking System-Replacement and determine the appropriate security categorization level and system classification based on (1) the sensitive personal information maintained in the system and (2) the System Security Categorization Report.

The OIG recommends the under secretary for health take the following actions:

3. Reevaluate whether there is a continued business need to maintain access to veterans' medical records in the Patient Advocate Tracking System-Replacement.
4. Institute a process to ensure user roles are regularly reviewed for continued access and evaluate the effectiveness of the access control principle of least privilege to ensure roles for the Patient Advocate Tracking System-Replacement are correctly configured and allow access only for authorized users.
5. Update the Patient Advocate Tracking System-Replacement user guides and training materials.

[31] The recommendations addressed to the assistant secretary for OIT are directed to anyone in an acting status or performing the delegable duties of the position.

VA Management Comments

The Deputy Secretary of VA, performing the delegable duties of the assistant secretary for OIT, concurred with recommendations 1 and 2. For recommendation 1, the Deputy Secretary reported that OIT took corrective action to address the categorization of PATS-R, and as an outcome of the reassessment, recategorized PATS-R to an overall moderate-impact level. He acknowledged that authorizations must be reassessed when a significant change affects the security and privacy of an application. He stated that reassessment was completed in June 2025 and requested closure of the recommendation.

For recommendation 2, the Deputy Secretary reported that OIT is collaborating with the system steward, information system security officer, and Office of Information Security officials to determine the appropriate security categorization level and system classification for PATS-R. This effort includes reviewing sensitive personal information in the system, reassessing impact levels, and reviewing and updating the System Security Categorization Report. He also stated that, as of December 2025, PATS-R is a minor application under Microsoft Azure Services and PATS-R will inherit its controls. The full text of the Deputy Secretary's response is included in appendix D.

The under secretary for health concurred with recommendations 3, 4, and 5. For recommendation 3, the under secretary reported that improvement has been made in reducing PATS-R users with medical record access. The under secretary noted that the Office of Patient Advocacy will reevaluate all user roles to determine whether there is a continued business need to access to veterans' medical records in PATS-R.

For recommendation 4, the under secretary reported that the Office of Patient Advocacy has begun communications with VISN patient advocate coordinators and facility patient advocate supervisors about this improvement effort. He stated that a work group is being formed to develop a standardized process and educational content.

For recommendation 5, the under secretary reported that the Office of Patient Advocacy is reviewing program quick reference guides for accuracy and updates, and a date indicating when they were last reviewed is being added. He also stated that older and obsolete versions of the quick reference guides will be properly archived. The full text of the under secretary's response is included in appendix E.

OIG Response

VA's corrective action plans are responsive to the intent of the recommendations. Based on the actions taken and evidence provided by VA, the OIG considers recommendation 1 closed. For the remaining recommendations, the OIG will monitor implementation of the planned actions and will close recommendations when VA provides sufficient evidence demonstrating progress in addressing the intent of the recommendations and the issues identified.

Appendix A: Background

Risk Management Framework

The National Institute of Standards and Technology's (NIST) risk management framework provides guidance for managing risk throughout information system design, development, implementation, operation, and disposal and in the environments in which systems operate.[32] At VA, the Office of Information and Technology (OIT) is responsible for following NIST's risk management framework, which provides a structured process that integrates information security and risk management activities into the system development life cycle.

Step 1: Prepare

The system steward or the information system owner prepares security and privacy plans, identifies key risk management roles, and develops both an organization-wide management strategy and a continuous monitoring strategy.

Step 2: Categorize

The system steward or the information system owner reviews the information processed, stored, and transmitted by the system and determines the potential adverse impacts of loss of confidentiality, integrity, and availability of the system. The information system security officer also reviews this information and works with the system steward and information system owner to provide input.

Step 3: Select

The system steward or information system owner selects, tailors, and documents the controls necessary to protect the system and organization in line with the risk in the security and privacy plan. Systems inherit some of the security and privacy controls from the cloud service provider, which the system steward and information system owner document. The system steward or information system owner also document any additional controls based on the security and privacy plans.

Once the controls are selected and documented, the information system security officer approves them. The strategy for continuous monitoring is also further developed and refined in coordination with the information system security officer.

[32] NIST Special Publication 800-37, rev. 2, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy*, December 2018.

Step 4: Implement

The system steward or the information system owner implements the controls for the system and the organization. The security and privacy plans created are also updated to reflect that controls have been implemented. The information system security officer reviews the control implementation.

Step 5: Assess

The system steward or information system owner determines whether the controls are operating as intended and whether they meet the security and privacy requirements of the system. A control assessor determines whether the submitted security and privacy controls are working as intended and approves the validation.

Step 6: Authorize

The authorizing official issues an authority to operate, confirming that the system or application has passed all requirements to become operational. The authority to operate is a formal declaration that sanctions the operation of a business product and explicitly accepts the risk to the agency. The length of the authorization varies based on the risks of a system as determined by the authorizing official.

Step 7: Monitor

When a system has an active authority to operate, the system steward or information system owner needs to maintain ongoing situational awareness regarding the security and privacy posture of the system. They also need to ensure the system supports the risks and continued management decisions that may affect the system. Continuous monitoring includes running scans to ensure the system continues to operate as designed. The information system security officer is also involved with monitoring the system for security threats and ensuring the controls are designed to protect against any new risks.

Prior Related VA OIG Reports

As noted in the introduction of this report, the VA Office of Inspector General (OIG) issued four reports before this audit relating to patient advocacy and VA cloud security. These past reports are summarized below.

- In March 2017, the OIG reported that the Veterans Health Administration (VHA) did not adequately capture patient complaint information and identify complaint trends, which resulted in missed opportunities to improve the delivery of health care

to veterans.[33] The OIG also found that Patient Advocacy Tracking System data were potentially vulnerable to unauthorized access due to missing security controls, inappropriate user access, and a lack of audit logs to record significant actions by users. Finally, VA did not have formal authorization to operate the system. The audit identified OIT did not apply the mandatory risk assessment and authorization process to the system.

- In March 2022, the OIG found that VHA lacked adequate governance over the Patient Advocacy Program.[34] VHA did not effectively issue and implement adequate policy, monitor complaint resolution practices, or provide guidance to responsible medical facility directors. This inadequate governance contributed to patient advocates and other program leaders not fully complying with requirements for managing complaints in fiscal year 2020.
- In September 2023, the OIG reported monitoring deficiencies related to step seven of the NIST risk management framework and VA not updating its guidance on security and privacy controls following a change in NIST guidance.[35] The OIG determined that OIT was not effectively overseeing the management of security and privacy controls to make sure the systems and the information they contain were protected commensurate with the risk associated with their misuse or unauthorized disclosure.
- In April 2025, the OIG found that VA users of Microsoft Office 365's collaborative applications could access sensitive personal information, and most of these users had no business need to access the information.[36] The OIG also noted that the type of sensitive information that was accessible should not have been on the systems because they did not have authorization to host it. The OIG determined that VA did not have adequate controls to prevent, detect, and correct inappropriately set permissions for the sharing of sensitive information among these applications.

[33] VA OIG, *Audit of the Patient Advocacy Program*, Report No. 15-05379-146, March 31, 2017.

[34] VA OIG, *Improved Governance Would Help Patient Advocates Better Manage Veterans' Healthcare Complaints*, Report No. 21-00510-105, March 24, 2022.

[35] VA OIG, *VA Should Strengthen Enterprise Cloud Security and Privacy Controls*, Report No. 22-03525-195, September 27, 2023; NIST Special Publication 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.

[36] VA OIG, *Improper Sharing of Sensitive Information on Cloud-Based Collaborative Applications*, Report No. 24-01330-29, April 22, 2025.

Appendix B: Scope and Methodology

Scope

The VA Office of Inspector General (OIG) team conducted its work from March 2025 through January 2026 to evaluate whether the Patient Advocate Tracking System-Replacement (PATS-R) had sufficient security controls to ensure confidentiality, data integrity, and the safeguarding of veterans' sensitive personal information in accordance with federal law and standards.

Methodology

The team reviewed the PATS-R security privacy threshold analysis and privacy impact assessment to evaluate whether the system had adequate security controls and oversight when it was set up in the Enterprise Mission Assurance Support Service. The team also reviewed PATS-R's business impact assessment and system security plan to determine whether the Office of Information and Technology (OIT)'s decision to host PATS-R on the cloud met all applicable security requirements by setting the system at an appropriate risk level. The team interviewed the PATS-R information system security officer, the PATS-R information system owner, and system users.[37] The team also reviewed selected security and privacy controls for the system to determine whether they were functioning as intended.

The team surveyed a statistical sample of VA employees to learn more about the PATS-R user experience and to understand the security and access controls governing user actions in the system. The survey was distributed to 261 PATS-R users on May 19, 2025, and the survey remained open until June 4, 2025. The overall survey response rate was about 73 percent (190 users submitted completed responses). The team performed a detailed nonresponse bias analysis using auxiliary data of population demographics obtained from the Corporate Data Warehouse and the Personnel and Accounting Integrated Data System. This analysis used regression modeling of unit nonresponse, early response, and item response as a function of demographic characteristics. The nonresponse analysis indicated that while years of employment was significant in predicting unit nonresponse, no auxiliary variables were significant in predicting early response or item response. Considering the overall survey response rate, the nonresponse bias analysis, and characteristics of the survey population, the team concluded there was insufficient evidence that nonresponse bias affected the quality of the survey data. More detail about the sampling design and estimates is included in appendix C.

[37] System stewards and the information system owner are officials with statutory, management, or operational authority for specified information; they are responsible for establishing the policies and procedures governing an organization's generation, collection, processing, dissemination, and disposal of information.

Internal Controls

The team assessed internal controls to determine whether they were significant to the audit objective. This included consideration of the five internal control components: control environment, risk assessment, control activities, information and communication, and monitoring.[38] In addition, the team reviewed the principles of internal controls as associated with the objective and identified three components and five principles as significant.[39] The team identified internal control deficiencies during this audit and proposed recommendations to address those listed in table B.1.

Table B.1. VA OIG Analysis of Internal Control Components and Principles Identified as Significant

Component	Principle	Deficiency identified by this audit
Risk assessment	8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.	The Office of Patient Advocacy did not mandate a process to ensure user roles were regularly reviewed for continued access to PATS-R. Additionally, the Office of Patient Advocacy did not ensure access control principles for PATS-R were configured correctly to only allow access for authorized users.
Control activities	11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.	OIT did not reevaluate the risk determination for PATS-R and determine the appropriate security categorization level based on the sensitive personal information accessible in the system and approved risk assessments.
	12. Management should implement control activities through policies.	OIT did not enforce VA policy that requires applications to undergo an approved security assessment before being placed on the VA network.

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

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

Component	Principle	Deficiency identified by this audit
Information and communication	13. Management should use quality information to achieve the entity's objectives.	The Office of Patient Advocacy did not determine whether there was a legitimate continued business need to provide staff access to veterans' medical records in PATS-R.
	14. Management should internally communicate the necessary quality information to achieve the entity's objectives.	The Office of Patient Advocacy did not regularly update user guides and training materials.

Source: VA OIG analysis of internal control components and principles. The principles listed are consistent with the GAO's Standards for Internal Control in the Federal Government.

Data Reliability

The team requested and received a list of PATS-R users. An Office of Patient Advocacy application coordinator showed the team how to access PATS-R to generate the list of users. The team observed that all the required fields were included in the list and that the period for users was up to date. The data used were determined to be reliable for the purposes of this audit.

Government Standards

The OIG conducted this performance audit in accordance with generally accepted government auditing standards.[40] Those standards require that the OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on audit objectives. The OIG believes the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

[40] Government Accountability Office, *Government Auditing Standards 2024 Revision*, GAO-24-106786, February 2024.

Appendix C: Statistical Sampling Methodology

Approach

To accomplish the audit objective, the VA Office of Inspector General (OIG) team surveyed a statistical sample of Patient Advocate Tracking System-Replacement (PATS-R) users. The team used statistical sampling to quantify use of PATS-R for accessing medical records. This method was used to reduce the number of respondents burdened by the need to complete a survey and the cost of data collection and analysis.

Following up with survey recipients who are nonresponsive is crucial to ensuring proper representation of the population and to reducing bias in the results. Since following up with nonrespondents in a statistical sample is more cost-effective and timelier than a census approach, the team used statistical sampling for this survey instead of a complete census of the population.

Population

The original review population included over 25,000 users with PATS-R access as of May 15, 2025. The survey was open from May 19, 2025, through June 4, 2025. The team sent a pre-notice survey to a statistical sample of 264 employees. The team determined that three of the sampled employees were not in the scope of the review because either they would be out of the office for the entire survey window or they were not a PATS-R user. This resulted in a survey audience comprising 261 randomly selected employees.

Survey Sampling Design

The team selected a statistical sample of 264 PATS-R users from the population who use PATS-R for accessing medical records. The population was stratified by Veterans Integrated Service Network (VISN) and categorized in 18 strata as shown in table C.1.

Table C.1. Strata Table

VISN	Sample of VA employees who use PATS-R
1	10
2	15
4	13
5	10
6	15
7	17
8	19
9	11

VISN	Sample of VA employees who use PATS-R
10	23
12	16
15	12
16	15
17	15
19	14
20	13
21	12
22	21
23	13
Total	**264**

Source: VA OIG statistician's stratified population using data obtained from the PATS-R user list.

Sample Results from Survey Responses

Table C.2 summarizes the survey responses. Questions 1 through 5 are not included because they were demographic screening questions to verify respondents' location and position as well as questions to verify that respondents have or had access to PATS-R and how often they access the system.

Table C.2. Summary of Survey Response Data[41]

Question	Response	Sample count (%)	Sample size
Q6. "Do you currently have access to patient medical records in any VA system?"	Yes	175 (92%)	190
	No	15 (8%)	
Q7. "Do you use PATS-R to access patient medical records?"	Yes	97 (55%)	175
	No	78 (45%)	
Q8. "Were you aware prior to this survey that medical records are accessible within PATS-R?"	Yes	41 (22%)	186
	No	144 (77%)	

[41] Question 7 was used to identify which systems were used to access patient medical records including the Computerized Patient Record System or Joint Longitudinal Viewer system. Question 11 was a follow-up for respondents who said they used PATS-R to view medical records to identify the frequency of access. Question 13 was a free-text option for respondents to identify factors or reasons to choose to view medical records in PATS-R. Question 14 was also a free-text option for respondents to identify any concerns related to PATS-R or other information technology systems.

Question	Response	Sample count (%)	Sample size
	NA	1 (1%)	
Q9. “Are you able to view patient medical records directly within the PATS-R system?”	Yes	19 (10%)	186
	No	34 (18%)	
	I’m not sure	131 (70%)	
	NA	2 (1%)	
Q9 or Q10. “Are you able to or have you ever viewed patient medical records directly within the PATS-R system?”	Yes	20 (11%)	186
	No	164 (88%)	
	NA	2 (1%)	
Q12. “Would removing medical records from PATS-R impact your job duties?”	Yes, to a great extent	7 (4%)	186
	Yes, somewhat	5 (3%)	
	Yes, very little	8 (4%)	
	No, not at all	166 (89%)	

Source: VA OIG statistician’s analysis.

Appendix D: VA Management Comments, Deputy Secretary of Veterans Affairs

Department of Veterans Affairs Memorandum

Date: March 20, 2026

From: Deputy Secretary of Veterans Affairs, Performing the Delegable Duties of the Assistant Secretary for Information and Technology and Chief Information Officer (005)

Subj: Office of Inspector General Draft Report, Audit of Security and Access Controls for the Patient Advocate Tracking System-Replacement (Project Number 2025-01781-AE-0073) (VIEWS 14388435)

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

1. Thank you for the opportunity to review the Office of Inspector General's (OIG) draft report, Audit of Security and Access Controls for the Patient Advocate Tracking System-Replacement (Project Number 2025-01781-AE-0073).

2. The Office of Information and Technology (OIT) is committed to safeguarding Veterans' sensitive personal information maintained in Department of Veterans Affairs information technology systems.

3. OIT submits the attached written comments in response to OIG's draft report. OIT acknowledges and concurs with OIG's recommendations 1-2. OIT is providing evidence showing OIT has fully addressed recommendation 1 and is providing a corrective action plan and target implementation date for recommendation 2. OIT defers to the Veterans Health Administration to respond to recommendations 3-5.

The OIG removed point of contact information prior to publication.

(Original signed by)

Paul R. Lawrence, PhD

Attachment

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 E: VA Management Comments, Under Secretary for Health

Department of Veterans Affairs Memorandum

Date: March 30, 2026

From: Under Secretary for Health (10)

Subj: Office of Inspector General Draft Report, Audit of Security and Access Controls for the Patient Advocate Tracking System-Replacement (VIEWS 14388435)

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

1. Thank you for the opportunity to review and comment on OIG's draft report on Audit of Security and Access Controls for the Patient Advocate Tracking System-Replacement. Attached is the Veterans Health Administration's (VHA) and Office of Information & Technology action plan.
2. VHA greatly values the OIG's assistance in ensuring that all stakeholders are unified in supporting VHA's vision of providing all Veterans with access to the highest quality care. Your collaboration is instrumental in helping us achieve our commitment to excellence in health care services for Veterans.

The OIG removed point of contact information prior to publication.

(Original signed by)

John J. Bartrum, JD, MBA

Attachment

Attachment

VETERANS HEALTH ADMINISTRATION (VHA) Action Plan

OIG Draft Report – Audit of Security and Access Controls for the Patient Advocate Tracking System-Replacement

(OIG Project Number 2025-01781-AE-0073)

Recommendation 1: Ensure that authorizations are reassessed when a significant change affects the security or privacy posture of an application, consistent with the requirements of VA Handbook 6500.

OIT Comments: Concur. The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs with the Office of Inspector General's (OIG) recommendation. VA acknowledges that authorizations must be reassessed when a significant change affects the security or privacy posture of an application, consistent with the requirements of VA Handbook 6500, VA Information System Contingency Planning.

OIG's finding and associated recommendation stemmed from the transfer of the Patient Advocate Tracking System – Replacement (PATS-R) from the Benefits and Memorials portfolio to the Veterans Experience Services portfolio under the Veterans Experience Integration Solution. At the time of the transfer, Step 1 of the Risk Management Framework process, including system categorization reassessment, had not been completed. At the time OIG initiated the audit, PATS-R was categorized as low–low–low (confidentiality, integrity, availability).

During the audit, OIT took corrective action to address the categorization of PATS-R. OIT reassessed PATS-R and, as an outcome of the reassessment, recategorized PATS-R as moderate–moderate–low, resulting in an overall moderate impact level. Supporting documentation reflecting the updated system categorization is documented in the System Security Categorization Report dated June 18, 2025.

OIT concurs that any future significant changes affecting the system's security or privacy posture will require reassessment in accordance with VA Handbook 6500 and Risk Management Framework requirements. VA requests closure of recommendation 1.

Completion Date: Completed June 2025. Ongoing compliance will occur as needed upon significant system changes.

Recommendation 2: Reevaluate the risk determination for the Patient Advocate Tracking System-Replacement and determine the appropriate security categorization level and system classification based on (1) the sensitive personal information maintained in the system and (2) the System Security Categorization Report.

OIT Comments: Concur. OIT is collaborating with the system steward, information system security officer, and Office of Information Security officials to determine the appropriate security categorization level and system classification for PATS-R.

The effort includes:

- Reviewing the sensitive personal information maintained within the system.
- Reassessing confidentiality, integrity, and availability impact levels.
- Reviewing and updating the System Security Categorization Report, as needed.

At the time OIG initiated the audit, PATS-R was a minor-assess only application under the Veterans Experience Integration Solution. As of December 2025, PATS-R, along with the other Microsoft Dynamics Customer Relationship Management solutions, are minor applications under Microsoft Azure Services (MAS-E). MAS-E is categorized as: confidentiality high, integrity high, availability moderate. PATS-R will inherit controls from MAS-E as the parent.

OIT is providing detailed analysis supporting the reevaluation.

Status: In Progress

Recommendation 3: Reevaluate whether there is a continued business need to maintain access to veterans' medical records in the Patient Advocate Tracking System-Replacement.

VHA Comments: Concur. Through the work of the VHA Office of Patient Advocacy (OPA) in partnership with the VA Office of Information and Technology, much improvement has been made in reducing PATS-R users with medical record access and ensuring only those who require access to the medial record and will use it within PATS-R have that access. OPA will reevaluate all user roles to determine whether there is a continued business need to access to veterans' medical records in PATS-R.

Status: In Progress

Recommendation 4: Institute a process to ensure user roles are regularly reviewed for continued access and evaluate the effectiveness of the access control principle of least privilege to ensure roles for the Patient Advocate Tracking System-Replacement are correctly configured and allow access only for authorized users.

VHA Comments: Concur. The VHA Office of Patient Advocacy supports the recommendation of a more standardized process to audit PATS-R users and has already begun communications with VISN Patient Advocate Coordinators (VPAC) and Facility Patient Advocate Supervisors (PAS) about this improvement effort. A work group including VPACs, PAS, and PATS Application Coordinators is being formed to develop a standardized process and educational content to support it.

Status: In Progress

Recommendation 5: Update the Patient Advocate Tracking System-Replacement user guides and training materials.

VHA Comments: Concur. The VHA Office of Patient Advocacy is currently reviewing program quick reference guides (QRG). All QRGs are being reviewed for accuracy and updates. In addition, a last reviewed date is being added to all QRGs to assist in managing user perception that QRGS are outdated. Concurrently, older versions of QRGs and those which are no longer needed will be properly archived to reduce misinformation and confusion.

Status: In Progress

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.
Audit Team	Al Tate, Director Jennifer Cheung Elijah Hancock Douglas Neesen Matthew Weber
Other Contributors	Andrew Eichner Juliana Figueiredo Jill Russell Jodi Treszoks

Report Distribution

VA Distribution

Office of the Secretary
Office of Accountability and Whistleblower Protection
Office of Congressional and Legislative Affairs
Office of General Counsel
Office of Public and Intergovernmental Affairs
Veterans Health Administration

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 vaoig.gov.