VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Adverse Effect on Patient Care Due to Removal of a Computer-Assisted Survey Instrument

September 29, 2017
16-00838-348

ACRONYMS

EP	Elevated Privileges
IRB	Institutional Review Board
NCHCS	Northern California Health Care System
OIG	Office of Inspector General
OI&T	Office of Information and Technology
PODS	Prescription Opioid Documentation and Surveillance
PMC	Pain Management Clinic
VA	Department of Veterans Affairs

Highlights: Review of Alleged Adverse Effect on Patient Care Due to Removal of a Computer-Assisted Survey Instrument

Why We Did This Audit

In September 2015, the OIG received an allegation that the Office of Information and Technology (OI&T) removed the Prescription Opioid Documentation and Surveillance (PODS) application from a VA server at the Northern California Health Care System (NCHCS) Pain Management Clinic (PMC). The complainant alleged the removal of PODS without replacing it was potentially harmful to veterans who were at increased risk of accidental overdose. PODS was a local application and was used only at the NCHCS.

What We Found

We substantiated the allegation that OI&T removed the PODS application. PODS was a Microsoft™ Access-based, computer-assisted survey instrument that used medical and mental health questionnaires to obtain information from patients. It was accessed directly by patients within the PMC using terminals in kiosk mode prior to their face-to-face clinical evaluations with PMC clinicians.

According to the NCHCS Chief of Staff, PODS was "not a standard of care." In addition, PMC clinicians told us PODS was not necessary for prescribing and tracking opioid medications. The clinicians reported they clinically evaluated and assessed patients' medical history to determine the required level of monitoring and long-term opioid therapy.

Because PODS was a survey tool that was only used locally and not needed to meet an appropriate standard of care, and PMC clinicians reported they could provide requisite care without PODS, we concluded its removal did not put veterans at increased risk of accidental overdose.

Although not part of the allegation, during our review we found OI&T failed to protect the integrity of VA's enterprise and the security of the information it stored by allowing patients and the PMC clinicians to use PODS. According to NCHCS's Compliance Officer, PODS was started as a research project approved by their Institutional Review Board in 2006. After the research ended in 2012, PMC clinicians continued to use PODS as a clinical assessment tool until it was removed in July 2015.

However, PODS was an unsupported Class III software application that did not meet VA system requirements, which created an unnecessary risk that veterans' sensitive information could be inappropriately accessed. We were unable to test for a data breach because PODS was removed prior to the OIG receiving the allegation. These security concerns existed because OI&T Region 1 staff failed to follow their standard operating procedures for the assessment and removal of Class III software. Without ensuring procedures are followed for the deployment of Class III software, the integrity and security of veterans' data could be compromised.

What We Recommended

We recommended the Acting Assistant Secretary for Information and Technology

implement appropriate controls to ensure that Class III software is not installed on VA networks without a formal technical review and authority to operate, and that training is provided to OI&T Region 1 staff on the treatment of Class III software.

Agency Comments

The Acting Assistant Secretary for Information and Technology concurred with our recommendation and provided an OI&T policy that addressed the intent of the recommendation. We consider the recommendation closed.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

RESULTS AND RECOMMENDATIONS

Finding

Removal of the Prescription Opioid Documentation and Surveillance Application Did Not Put Veterans at Increased Risk of Accidental Overdose

In September 2015, the Office of Inspector General (OIG) received an allegation that the Office of Information and Technology (OI&T) removed the Prescription Opioid Documentation and Surveillance (PODS) application from a VA server at the Northern California Health Care System (NCHCS)[1] Pain Management Clinic (PMC). The complainant alleged the removal of PODS without replacing it was potentially harmful to veterans who were at increased risk of accidental overdose. PODS was a Microsoft™ Access-based, computer-assisted survey instrument that used medical and mental health questionnaires to obtain information from patients. It was accessed directly by patients within the PMC using terminals in kiosk mode prior to their face-to-face clinical evaluations with PMC clinicians.

We substantiated the allegation that OI&T removed the PODS application in July 2015. According to the NCHCS Chief of Staff, PODS was "not a standard of care." In addition, PMC clinicians told us PODS was not necessary for prescribing and tracking opioid medications. The clinicians reported they conducted clinical evaluations and assessments of patients' medical history to determine the required level of monitoring and long-term opioid therapy for those patients. Because PODS was a survey tool that was only used locally and not needed to meet an appropriate standard of care, and PMC clinicians reported they could provide requisite care without PODS, we concluded its removal did not put veterans at increased risk of accidental overdose. We found the PODS application was a computer-assisted survey instrument that used medical and mental health questionnaires, but that it was not necessary to track opioid prescriptions.

In addition, PODS was an unsupported Class III software application[2] that was initially used as a research project and approved by the NCHCS's Institutional Review Board (IRB) in 2006. The application owner was a former clinical research coordinator and computer programmer/database architect who worked for NCHCS and the University of California Davis

[1] NCHCS is composed of a medical center, a rehabilitation and extended care facility, outpatient and dental clinics, and a substance abuse treatment center. PODS was being used at the VA medical center located in Sacramento, CA, where our review was conducted.
[2] Class III software consists of all products or interfaces installed on or interacting with VA computing environments that are not covered by the Class I or Class II definitions. Class I and II products are certified by OI&T's Product Development or Field Operations and Development, respectively, for deployment. Unlike Class I and II, Class III products are not automatically covered by OI&T Tier I and Tier II support commitments.

Medical Center Division of Pain Medicine. We found OI&T removed the PODS application because it did not meet VA system requirements.

However, we found OI&T failed to protect the integrity of VA's enterprise and the security of the information it stored when it allowed PMC clinicians to use PODS after the research period ended in 2012, creating an unnecessary risk that veterans' sensitive information could be inappropriately accessed. We were unable to test for a data breach because PODS was removed prior to the OIG receiving the allegation. These security concerns existed because OI&T Region 1 staff failed to follow their standard operating procedures for the approval and removal of Class III software, which should have resulted in an earlier detection of the underlying security issues associated with PODS. Without ensuring procedures are followed for the deployment of Class III software, the integrity and security of veterans' data could be compromised.

PODS Was Not a Required Clinical Tool

We found PODS was clinical software that PMC clinicians used as a supplement to their patient assessment process, but it was not a required clinical tool. According to the PMC clinicians we interviewed, PODS was a useful tool that aided them in the evaluation of their patients, but was not necessary for prescribing and tracking opioid medications. PODS was a local application used only at NCHCS and it was not used at any other VA facilities. According to the NCHCS Chief of Staff, PODS was a helpful tool but "not a standard of care." The patient self-assessment information from PODS provided an additional data set for clinicians to consider when determining the level of monitoring required for long-term opioid therapy recipients. The PODS assessment results were incorporated into the veterans' progress notes within VA's Computerized Patient Record System. PMC clinicians' clinical evaluations, however, remain central to determining the required level of monitoring and long-term opioid therapy for patients.

PODS Presented an Unnecessary Risk

OI&T failed to protect the integrity of VA's enterprise and the security of the information it stored, which created an unnecessary risk. According to the NCHCS Facility Chief Information Officer, the server that maintained PODS was taken offline due to security issues. In addition, an NCHCS IT Supervisor indicated that for PODS to be reinstalled, the application would need to be redesigned and approved by VA. However, the supervisor also indicated PODS was not supported on a national level and could not be converted to Class I software.[3] Further, according to an OI&T Region 1 Senior IT Analyst, PODS needed to be shut down because the database was not encrypted and contained personally identifiable information and protected health information, such as Social Security numbers.

[3] Class I software includes applications and commercial off-the-shelf product interfaces installed on or interacting with VA computing environments that have been certified by OI&T to comply with VA standards.

Therefore, anyone who had access to PODS could read and edit the database contents because the information was not secure.

The Region 1 Senior IT Analyst indicated there was no way to secure PODS to make him comfortable with giving direct access to patients. According to the Executive Director, OI&T Field Operations and Development, outages have occurred that were directly traceable to the deployment of Class III software. When deciding whether to use Class III software, VA should assess whether the benefits of using the software outweigh the risks involved. OI&T's Region 1 Standard Operating Procedures put responsibility for approving the production installation of Class III software on the OI&T Regional Director or delegate.[4] If the use of the software jeopardizes the availability of VA's systems, it represents an unnecessary risk.

PODS Was Unsupported Class III Software

OI&T removed PODS because it was unsupported Class III software that did not meet VA system requirements. Class III software consists of products or interfaces installed on, or interacting with, VA computing environments that have not been reviewed or certified for use by OI&T's Product Development or Field Operations and Development staff. Though generally referred to as "field-developed software," Class III products may originate from any non-product development source including field developers, non-information technology VA staff (for example, physicians), vendors, open source, research, or educational organizations. In addition, Class III products generally have a limited and non-standardized distribution across VA systems. Unlike Class I and II products and applications, PODS was not approved by OI&T's Product Development or Field Operations and Development and was not covered by OI&T's customer and maintenance support staff.

OI&T Did Not Follow Procedures

OI&T Region 1 staff did not follow their standard operating procedures for the assessment, implementation, and removal of Class III software. According to NCHCS's Compliance Officer, PODS was initially started as a research project and its use was approved by their IRB in 2006. After the research ended in 2012, PMC clinicians continued to use PODS as a clinical assessment tool until it was removed in July 2015. Specifically, in 2015 as part of Region 1's migration of servers, OI&T was tasked with identifying all applications that needed to be transitioned, such as PODS. However, we determined PODS was not approved by OI&T's Region 1 Director or delegate after the research phase ended in 2012. In addition, OI&T Field Operations and Development staff did not perform a technical review of PODS and recommend solutions that complied with national directives,

[4] Approval for Class III research software is obtained by the appropriate clinical oversight group or IRB. Once research ends, the user must request approval from the OI&T Region 1 Director to continue using the Class III software in production.

followed programming standards, and ensured PODS did not represent a security risk or create any system performance or data integrity issues.

According to an NCHCS IT Supervisor, OI&T allowed PODS to be hosted on a VA server but would not provide the required support. In addition, the IT Supervisor told us that while they were aware PMC clinicians continued to use PODS, they were unaware the research phase had ended. As a result, PODS was not removed from the network at the end of research in accordance with OI&T Region 1 Standard Operating Procedures that required software be removed at the end of approved studies. Consequently, the network was subject to the inherent security risks associated with this Class III software for over three years after research ended.

In 2015, OI&T realized that PODS was no longer in research and at that point, according to the IT Supervisor, the application was no longer approved to be installed on VA's system. Although PODS was approved by NCHCS's IRB, because it was on VA's network when research ended in 2012, OI&T should have conducted a risk assessment of PODS to identify potential risks, vulnerabilities, and threats to VA systems and sensitive information. As part of the certification and accreditation process, OI&T is responsible for ensuring that information systems, including major and minor applications, have effective security safeguards commensurate with potential risks to the system's information. Furthermore, OI&T is responsible for giving the information system owner an authorization to operate. While software such as PODS was developed to address a specific need identified at NCHCS and to improve service, the unregulated deployment of Class III software presented an unnecessary risk.

Conclusion

We substantiated the allegation that OI&T removed the PODS application. However, the removal of PODS did not put veterans at increased risk of accidental overdose because it was not required to meet an appropriate standard of care and PMC clinicians reported they could provide care without PODS. In addition, PMC clinicians told us PODS was not necessary for prescribing and tracking opioid medications. Furthermore, the clinicians reported they conducted clinical evaluations and assessments of patients' medical history to determine the required level of monitoring and long-term opioid therapy for patients. Class III software such as PODS, which PMC clinicians used as a supplement to their patient assessment process, can be a useful resource in providing comprehensive patient care. However, when deciding whether to use Class III software, VA should assess if the benefits of using the software outweigh the risks involved.

In addition, we determined OI&T's NCHCS staff were aware PMC clinicians were using Class III software but considered PODS to still be in the research phase. However, OI&T's Region 1 Standard Operating Procedures required the regional director or their delegate to approve the production installation of field-developed software such as PODS. Not

following procedures potentially jeopardized the confidentiality, integrity, and availability of VA's systems. Given the nature and seriousness of sensitive VA patient information being vulnerable to increased risks, it is vital for OI&T Region 1 leadership to ensure their staff follow procedures that address the treatment of Class III software.

Recommendation

1. We recommended the Acting Assistant Secretary for Information and Technology implement appropriate controls to ensure that Class III software is not installed on VA networks without a formal technical review and authority to operate, and that training is provided to Office of Information and Technology Region 1 staff on the treatment of Class III software.

Management Comments

The Acting Assistant Secretary for Information and Technology concurred with our recommendation. The Acting Assistant Secretary reported Class III software requires formal technical review and authorized privileges to install, as well as end-user training. He provided an OI&T policy that addressed elevated privileges (EP) for VA information system users. The policy indicates all EP users are required to complete the *Elevated Privileges for System Access* training, and users who are granted System Administrator access are required to complete the *Information Security Role-Based Training for System Administrators*. Users with EP are also required to sign the Elevated Privileges Rules of Behavior, which restricts users from making unauthorized changes to VA systems and employing hardware or software tools without specific approval from their supervisor, Information Security Officer, and Chief Information Officer.

OIG Response

The Acting Assistant Secretary's reported action is acceptable. Users are no longer allowed to install software on VA's network without obtaining EP, completing required training, and complying with the EP Rules of Behavior. We consider the recommendation closed. Appendix B contains the full text of the Acting Assistant Secretary's comments.

Appendix A Scope and Methodology

Scope

We conducted our review from April 2016 through July 2017. The review focused on the removal of the PODS application from a VA server located at the NCHCS PMC.

Methodology

In April 2016, we conducted a site visit at NCHCS to evaluate the merits of the allegation. We interviewed NCHCS officials and PMC clinicians to gain an understanding of PODS and its clinical application. In addition, we evaluated VA policies, procedures, and information security controls for software and protecting the integrity of VA's enterprise and the information it stores. We also obtained supporting documentation on PODS and the use of Class III software.

Data Reliability

We did not use computer-processed data. Our review consisted of interviews and examination of both email correspondence and criteria to assess and evaluate the statements made by those we interviewed.

Government Standards

We conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Appendix B Management Comments

Department of Veterans Affairs Memorandum

Date: August 24, 2017

From: Acting Assistant Secretary for OI&T, Chief Information Officer (005)

Subj: Draft Report, "Review of Alleged Adverse Impact on Patient Care Due to Removal of Computer-Assisted Survey Instrument." Project Number 2016-00838-DV-009

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

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, "Review of Alleged Adverse Impact on Patient Care Due to Removal of Computer-Assisted Survey Instrument." The Office of Information and Technology submits the attached written comments. If you have any questions, contact me at (202) 461-6910 or have a member of your staff contact Eddie Pool, Executive Director, Infrastructure Operations at 512-326-6002.

(Original signed by)

Rob C. Thomas, II

Attachment

For accessibility, the format of the original memo and attachment has been modified to fit in this document.

Attachment

Office of Information and Technology
Comments on OIG Draft Report,
Review of Alleged Adverse Impact on Patient Care Due to Removal of Computer-Assisted Survey Instrument
Project Number 2016-00838-DV-0095

OIG Recommendation 1: We recommended the Acting Assistant Secretary for Information and Technology implement appropriate controls to ensure that Class III software is not installed on VA networks without a formal technical review and authority to operate, and that training is provided to OI&T Region 1 staff on the treatment of Class III software.

Comments: Concur. In March 2015, VA implemented guidance for requesting elevated IT System privileges. Most end users do not require elevated privileges (EP); only staff requiring EP may request via the Electronic Permission Access System (ePAS) and must be approved by the Authority to Operate (ATO) System Owner. All users granted EP must complete Talent Management System (TMS) training courses, and sign the Elevated Privileges Rules of Behavior.

This recommendation has been fulfilled; Class III software requires formal technical review and authorized privileges to install, as well as end-user training. Please see the attached memorandum, "Elevated Privileges Guidance".

OI&T requests closure based on the evidence provided.

OI&T Comments on the OIG Draft Report Findings (if applicable):

OIG Finding: Page 3, paragraph 3. OIT Did Not Follow Procedures

Comments: In March 2015, VA implemented guidance for requesting elevated IT System privileges. Most end users do not require elevated privileges (EP); only staff requiring EP may request via the Electronic Permission Access System (ePAS) and must be approved by the Authority to Operate (ATO) System Owner. All users granted EP must complete Talent Management System (TMS) training courses, and sign the Elevated Privileges Rules of Behavior.

Appendix C OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Al Tate, Director Loralee Bennett Jennifer Kvidera Mathew Wiles

Appendix D Report Distribution

VA Distribution

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

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

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