VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Data Sharing Violations at the Palo Alto VA Health Care System

September 28, 2015
14-04945-413

ACRONYMS

ISO	Information Security Officer
OIG	Office of Inspector General
PAHCS	Palo Alto Health Care System
PHI	Protected Health Information
PII	Personally Identifiable Information
VA	Department of Veterans Affairs

To Report Suspected Wrongdoing in VA Programs and Operations:

Telephone: 1-800-488-8244

E-Mail: vaoighotline@va.gov

(Hotline Information: http://www.va.gov/oig/hotline)

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In October 2014, the House Committee on Veterans' Affairs provided the VA Office of Inspector General (OIG) a complainant's allegation that the VA Palo Alto Health Care System (PAHCS) Chief of Informatics entered into an illegal agreement with Kyron, a health technology company, to allow data sharing of sensitive VA patient information. This allegation involved veterans' personally identifiable information (PII), protected health information (PHI), and other sensitive information being vulnerable to increased risks of compromised confidentiality. Allegedly, sensitive VA patient information was transmitted outside of VA's firewall. The complainant also alleged Kyron personnel received access to VA patient information through VA systems and networks without appropriate background investigations.

We did not substantiate the allegations that the Chief of Informatics formed an illegal agreement with Kyron or that sensitive patient information was transmitted outside of VA's firewall. However, we substantiated the allegation that Kyron personnel received access to VA patient information without appropriate background investigations. We determined there was a signed agreement between PAHCS and Kyron and its personnel received access to de-identified VA patient information within VA's information technology enterprise. The agreement allowed Kyron, as part of a pilot program, to test technical implementation of its extraction software on a VA server by transforming de-identified VA patient information into structured patient profiles. The profiles allowed search and query of patient interventions and outcomes in more timely and cost-effective ways and facilitated data mining that could potentially assist VA in improving the delivery of healthcare.

Based on our interviews, review of available documentation and relevant criteria, and our judgment, we determined the Chief of Informatics, who was also the local program manager for the pilot program, failed to ensure Kyron personnel met the appropriate background investigation requirements before granting access to VA patient information. The Chief of Informatics also failed to ensure Kyron personnel completed VA's security and privacy awareness training. Further, the Information Security Officers (ISOs) failed to execute their required responsibilities in accordance with VA Handbook 6500, *Information Security Program,* by not providing PAHCS management and staff guidance on information security matters. More specifically, the ISOs did not coordinate, advise, and participate in the development and maintenance of system security documentation and system risk analysis prior to Kyron placing its software on a VA server. As a result, Kyron did not have formal authorization to operate its software on a VA server.

We concluded the lack of coordination between the Chief of Informatics and ISOs in executing the Kyron agreement potentially jeopardized the confidentiality of veteran's PII, PHI, and other sensitive information. The Chief of Informatics admitted to proceeding with the pilot before obtaining documented support from the local ISOs. In addition, the PAHCS and regional ISOs failed to execute their required responsibilities in accordance with VA Handbook 6500. After the OIG informed PAHCS officials of the initial results in November 2014, they discontinued Kyron's personnel access to VA de-identified patient information until Kyron's personnel received VA completed background investigations, appropriate security, and privacy training.

However, given the nature and seriousness of sensitive veteran data being vulnerable to increased risks of compromised confidentiality, we recommended the VA Assistant Secretary for Information and Technology take immediate action to ensure the local and regional ISOs determine the appropriate security level for Kyron's software and pilot program. We also recommended the VA Assistant Secretary for Information and Technology implement appropriate controls to ensure that unauthorized software is not procured or installed on VA networks without a formal risk assessment and approval to operate. We recommended the PAHCS management, in conjunction with VA's Assistant Secretary for Information and Technology, ensure Kyron personnel receive commensurate background investigations and obtain the required information security documentation that authorizes Kyron's software to operate.

Further, we recommended the PAHCS management, in conjunction with VA's Assistant Secretary for Information and Technology, require Kyron personnel complete security awareness training and sign the Contractor Rules of Behavior to ensure full awareness of VA information security requirements when accessing VA systems and networks. The Assistant Secretary for Information and Technology concurred with our findings and recommendations and provided an appropriate action plan. We will follow up on the implementation of the corrective actions.

Linda A. Halliday

LINDA A. HALLIDAY
Deputy Inspector General

RESULTS AND RECOMMENDATIONS

Allegation

The Palo Alto Health Care System Chief of Informatics Entered Into an Illegal Agreement With a Contractor That Resulted in Data Sharing Violations

In October 2014, the House Committee on Veterans' Affairs provided the VA Office of Inspector General (OIG) a complainant's allegation that the VA Palo Alto Health Care System (PAHCS) Chief of Informatics entered into an illegal agreement with Kyron, a health technology company, to allow data sharing of sensitive VA patient information. This allegation involved veterans' personally identifiable information (PII), protected health information (PHI), and other sensitive information being vulnerable to increased risks of compromised confidentiality. Allegedly, sensitive VA patient information was transmitted outside of VA's firewall. The complainant also alleged Kyron personnel received access to VA patient information through VA systems and networks without appropriate background investigations.

Background

On July 7, 2014, the PAHCS Director signed an agreement with Kyron for 1 year to participate in a pilot program. The purpose of the pilot was to test a technical implementation for statistical analysis of patient progress notes. Kyron specializes in the development of software that mines clinical information. The agreement required Kyron's extraction software be installed on a VA server within its protected network firewall. The Kyron application uses a two-part process where records are first scanned to determine the structural layout of the record. The second part scans the records for instances of treatment and the outcome. Once complete, the data are aggregated to provide statistical models of treatments. Kyron only had access to output files that contain de-identified VA patient data.

Kyron's extraction software uses a combination of natural language processing and medical ontologies to transform structured and unstructured data into patient profiles by searching for medical terms that reference drugs, medical conditions, and other clinical data. The software analyzes data to identify treatment processes and outcomes that provide clinicians with a statistical model for making better decisions on the delivery of health care. This process is commonly referred to as clinical data analytics or clinical business intelligence. According to the Chief of Informatics, Kyron staff, and the ISOs, since entering into the pilot agreement, the PAHCS has conducted only one system data extraction of de-identified VA patient information.

What We Did

We conducted site visits at the PAHCS to assess the merits of the allegations. The OIG Criminal Investigations Division performed the initial visit and the

OIG Information Technology and Security Audits Division conducted a subsequent visit. We interviewed PAHCS's Chief of Informatics, who was the subject of the allegation, Information Security Officers (ISOs), and Privacy Officers to obtain information necessary to assess the allegations. We also interviewed Kyron personnel to assess their role in the alleged data sharing violations. In addition, we reviewed applicable Federal Information Security requirements, VA Directives, National Institute of Standards and Technology publications, and Kyron's pilot agreement. Further, we gained an understanding of Kyron's extraction process to determine whether the data contained only de-identified VA patient information.

What We Found

Based on our interviews, review of available documentation and relevant criteria, and our judgment, we determined there was no evidence that the PAHCS Chief of Informatics entered into an illegal agreement with Kyron or that sensitive VA patient information was transmitted outside of VA's firewall. On July 7, 2014, the PAHCS Director signed the agreement after VA attorneys and the PAHCS Chief and Deputy Chief of Staff approved the agreement. We determined the appropriate VA legal and management staff reviewed and signed the agreement. The agreement required Kyron's proprietary extraction software be installed and run on a VA server within VA's protected network firewall. We determined the extraction process did not require identifiable patient data as part of the generated output.

We also determined, as part of a two-layer control process, patient data were de-identified and a foreign key was used to replace a patient identifier in the output to protect data that could potentially have been incorrectly de-identified prior to the extraction process. In addition, this process was not in violation of the Health Insurance Portability and Accountability Act, Federal Information Security Management Act, National Institute of Standards and Technology guidance, or VA Handbook 6500, *Information Security Program*.

However, based on our interviews, review of available documentation and relevant criteria, and our judgment, we determined the Chief of Informatics, who was also the local program manager for the pilot program, failed to ensure Kyron personnel met the appropriate background investigation requirements in accordance with VA Handbook 6500, Appendix F before granting access to VA patient information. The Chief of Informatics also failed to ensure Kyron personnel completed VA's security and privacy awareness training. Further, the ISOs failed to execute their required responsibilities in accordance with VA Handbook 6500 by not providing PAHCS management and staff guidance on information security matters. More specifically, the ISOs did not coordinate, advise, and participate in the development and maintenance of information system security documentation and system risk analysis prior to Kyron placing its software on a VA server. Consequently, Kyron did not have authorization from VA's Office of

Information and Technology, through these ISOs, to operate its software on a VA server.

Background Investigations Not Performed

The Chief of Informatics did not ensure Kyron personnel had appropriate background investigations prior to receiving access to VA patient information and systems as required by VA policy. VA Handbook 6500 Appendix F, *Personnel Screening*, requires contractors to be subject to appropriate background screenings prior to accessing VA information or systems needed to perform their jobs.

In addition, Kyron personnel did not complete security awareness training or sign Contractor Rules of Behavior prior to our review. VA Handbook 6500 requires contractors receive background screening at the appropriate level, complete security awareness training, and sign Contractor Rules of Behavior prior to gaining access to VA information and systems. Without effective controls over background investigations and training for contractors, VA information systems and sensitive data will be at increased and unnecessary risk of loss and unauthorized disclosure by contractor personnel of unverified character and suitability.

Extraction Software Not Approved

In March 2014, the Chief of Informatics contacted the local ISO and Privacy Officer to coordinate the Kyron pilot program. However, the Chief of Informatics did not receive an official response from the ISO prior to the installation of Kyron's extraction software on a VA server or the data extraction performed in July 2014. The Chief of Informatics proceeded with the pilot before receiving input from the ISOs on the necessary processes, including system risk analysis and documentation. According to PAHCS's ISOs, the ISO group did not have a valid reason for not responding to the Chief of Informatics requests for assistance. The lack of coordination, communication, and the ISOs' failure to perform their required responsibilities in accordance with VA Handbook 6500 resulted in Kyron's software being used on a VA server without formal approval.

VA Handbook 6500 requires VA ISOs to manage their local information security programs and serve as the principal security advisors to system owners regarding security considerations such as applications, systems, implementation, and operation and maintenance. This includes assisting in the determination of an appropriate level of security commensurate with the impact level of new applications. Further, ISOs were required to assist with risk assessments to identify the Kyron application's risk classification within the existing certification and accreditation boundary. If the Kyron software were classified as a major application, it would require its own separate certification and accreditation package, whereas a minor application would inherit the same controls from the General Support System.

Conclusion

Beyond PAHCS's fundamental mission of delivering health care to veterans, VA has an opportunity to use veterans' medical data to achieve advancements in medical research and health care services. Clinical analytics can provide VA an essential tool for transformation by using information technologies that gather and analyze clinical data to help managers and clinicians make better decisions. Kyron's technical approach is consistent with current developments in optimizing health care outcomes using statistics and information technology. However, the lack of coordination and communication between the PAHCS's program proponents and ISOs resulted in Kyron having access to VA information systems without appropriate background investigations and training.

In addition, the control deficiencies resulted in the installation of Kyron's software on a VA server without approval and appropriate documentation. These actions potentially jeopardized the confidentiality, integrity, and availability of VA's systems. After the OIG informed PAHCS officials of the initial results in November 2014, they discontinued Kyron's personnel access to VA de-identified patient information until Kyron's personnel received VA completed background investigations. Given the nature and seriousness of sensitive VA patient information being vulnerable to increased risks, it is vital for PAHCS to ensure contractors receive background investigations and information security training. In addition, ISOs need to perform their information security responsibilities to ensure VA patient information and systems are protected.

Recommendations

1. We recommended the VA Assistant Secretary for Information and Technology take action to ensure the Palo Alto Health Care System Information Security Officers conduct a risk assessment of Kyron software to identify potential risks, vulnerabilities, and threats to VA systems and sensitive information.

2. We recommended the VA Assistant Secretary for Information and Technology implement appropriate controls to ensure that unauthorized software is not procured or installed on VA networks without a formal risk assessment and approval to operate.

3. We recommended the Palo Alto Health Care System Management, in conjunction with VA's Assistant Secretary for Information and Technology, ensure Kyron personnel receive commensurate background investigations and obtain formal authorization to operate Kyron software on VA networks.

4. We recommended the Palo Alto Health Care System Management, in conjunction with VA's Assistant Secretary for Information and Technology, require Kyron personnel to complete security awareness training and sign the Contractor Rules of Behavior to ensure full

awareness of VA information security requirements when accessing VA systems and networks.

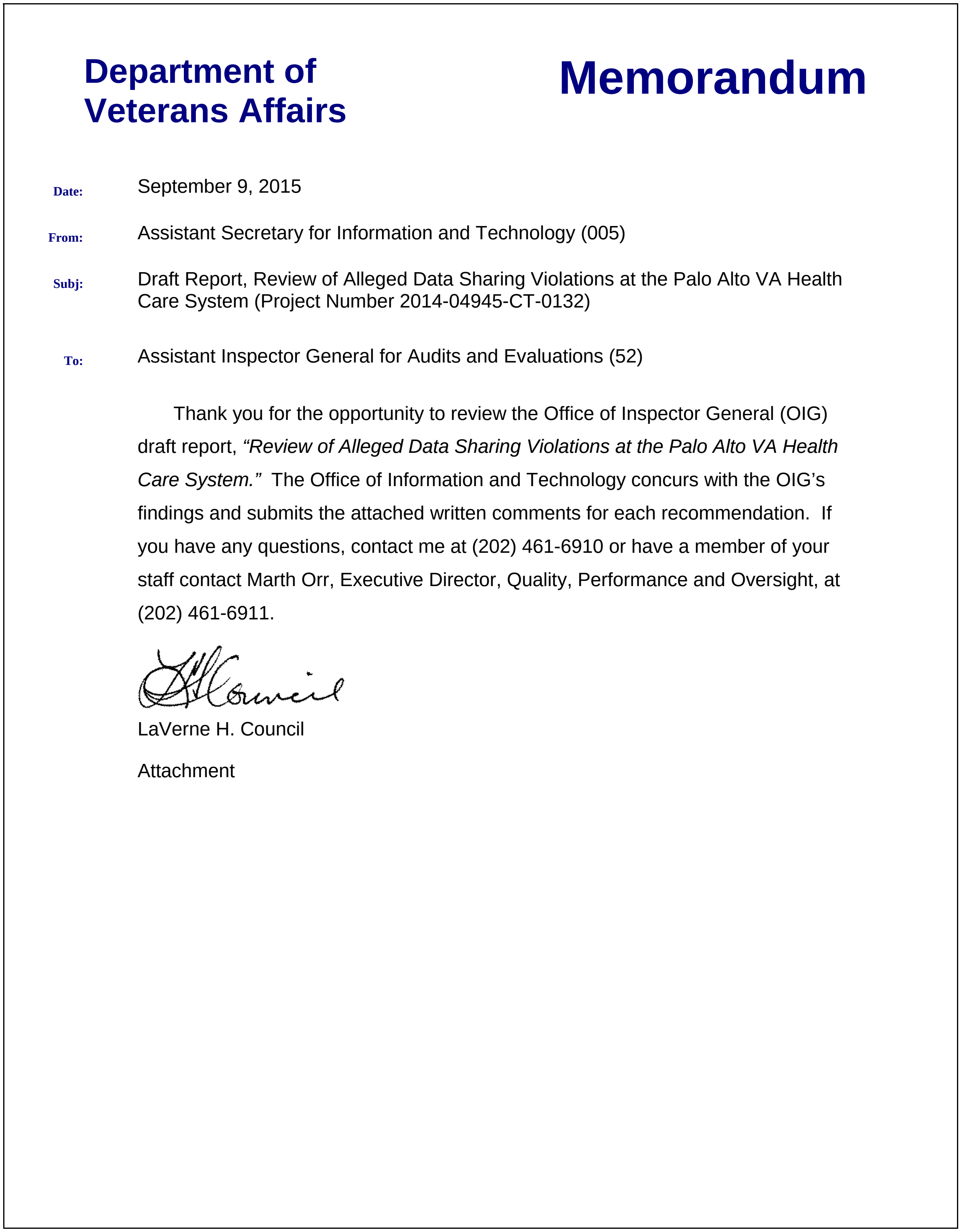
Management Comments and OIG Response

The Assistant Secretary for Information and Technology concurred with our findings and recommendations and plans to address all our recommendations by October 2015. We will monitor the Office of Information and Technology's progress and follow up on the implementation of our recommendations until all proposed actions are completed. Appendix A contains the full text of the Assistant Secretary's comments.

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 A Assistant Secretary for Information and Technology Comments



Department of Veterans Affairs

Memorandum

Date: September 9, 2015

From: Assistant Secretary for Information and Technology (005)

Subj: Draft Report, Review of Alleged Data Sharing Violations at the Palo Alto VA Health Care System (Project Number 2014-04945-CT-0132)

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 Data Sharing Violations at the Palo Alto VA Health Care System."* The Office of Information and Technology concurs with the OIG's findings and submits the attached written comments for each recommendation. If you have any questions, contact me at (202) 461-6910 or have a member of your staff contact Marth Orr, Executive Director, Quality, Performance and Oversight, at (202) 461-6911.

LH Council

LaVerne H. Council

Attachment

Attachment

U.S. Department of Veteran Affairs
Office of Information and Technology (OI&T)
Comments on OIG Draft Report:
"Review of Alleged Data Sharing Violations at the Palo Alto
VA Health Care System"

The following comments are submitted in response to the recommendations in the OIG draft report:

Recommendation 1: We recommended the VA Assistant Secretary for Information and Technology take action to ensure the Palo Alto Health Care System Information Security Officers conduct a risk assessment of Kyron software to identify potential risks, vulnerabilities, and threats to VA systems and sensitive information.

Response: Concur. The Assistant Secretary for Information and Technology will take action to ensure the Palo Alto Health Care System Information Security Officers conduct a risk assessment of Kyron software to identify potential risks, vulnerabilities, and threats to VA systems and sensitive information.

Target Completion: October 2015

Recommendation 2: We recommended the VA Assistant Secretary for Information and Technology implement appropriate controls to ensure that unauthorized software is not procured or installed on VA networks without a formal risk assessment and approval to operate.

Response: Concur. The Assistant Secretary for Information and Technology will implement appropriate controls such as network access control technology to ensure that unauthorized software is not installed on VA networks without a formal risk assessment and approval to operate.

Target Completion: September 2015

Recommendation 3: We recommended the Palo Alto Health Care System Management, in conjunction with VA's Assistant Secretary for Information and Technology, ensure Kyron personnel receive commensurate background investigations and obtain formal authorization to operate Kyron software on VA networks.

Response: Concur. The Assistant Secretary for Information and Technology will ensure Kyron personnel are properly cleared before obtaining formal authorization to operate Kyron software on VA networks.

Target Completion: September 2015

Recommendation 4: We recommended the Palo Alto Health Care System Management, in conjunction with VA's Assistant Secretary for Information and Technology, require Kyron personnel to complete security awareness training and sign the Contractor Rules of Behavior to ensure full awareness of VA information security requirements when accessing VA systems and networks.

Response: Concur. The Assistant Secretary for Information and Technology will require Kyron personnel to complete security awareness training and sign the Contractor Rules of Behavior to ensure full awareness of VA information security requirements when accessing VA systems and networks.

Target Completion: September 2015

Appendix B OIG Contact and Staff Acknowledgments

OIG Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Al Tate, Director Michael Bowman, Director George Ibarra Ryan Nelson Steven Slawson

Appendix C Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel

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
Department of Homeland Security

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