Department of Veterans Affairs
Office of Inspector General

Healthcare Inspection

VistA Outages Affecting Patient Care
Office of Risk Management and Incident Response
Falling Waters, WV

Report No. 09-01849-39

December 3, 2009

VA Office of Inspector General
Washington, DC 20420

To Report Suspected Wrongdoing in VA Programs and Operations

Telephone: 1-800-488-8244 between 8:30AM and 4PM Eastern Time, Monday through Friday, excluding Federal holidays

E-Mail: vaoighotline@va.gov

Contents

Executive Summary

The VA Office of Inspector General (OIG), Office of Healthcare Inspections reviewed allegations that there are an increasing number of Veterans Health Information Systems and Technology Architecture (VistA) outages that affect patient care and that the Office of Risk Management and Incident Response (RMIR) does not perform risk management, but only reports incidents to higher echelons within the Office of Information and Technology (OI&T).

We did substantiate the allegation that RMIR was only reporting system outages via Daily Incident Reports to higher echelons and does not manage, track, or trend risks related to system outages. Further investigation revealed substandard maintenance practices and an aging infrastructure that contributed to the loss of this critical patient care system. No patient safety incidents were reported, but the after action report and staff interviews showed that patient care was seriously affected.

The Root Cause Analysis Report revealed that the system outage was caused by hard disk failures in conjunction with outdated storage system firmware. OI&T maintenance had not performed a firmware upgrade which had been directed by the vendor 2 years prior. In addition, a report from the vendor identified significant issues relating to the aging infrastructure with critical recommendations that OI&T has not addressed.

We recommended that:

- **T**he Office for Enterprise Operations and Field Development provide a plan that addresses VistA outages and solutions that may include a backup system with a high availability configuration at VAMCs not currently supported by a Regional Data Processing Center.
- The Office for Information Protection and Risk Management establish and track performance measures that monitor essential medical IT systems such as VistA.
- The Office for Information Protection and Risk Management perform and report on risk management for essential medical IT systems.
- The Office for Enterprise Operations and Field Development provide a status report on all significant medical IT system failures or outages affecting patient safety and care to the Under Secretary of Health.
- The Office for Enterprise Operations and Field Development develop a plan that addresses the aging medical IT infrastructure in Regions II and III and provide to the Under Secretary of Health.

OI&T concurred and submitted appropriate implementation plans.

DEPARTMENT OF VETERANS AFFAIRS
Office of Inspector General
Washington, DC 20420

TO: Assistant Secretary for Information and Technology (005)

SUBJECT: Healthcare Inspection – VistA Outages Affecting Patient Care, Office of Risk Management and Incident Response, Falling Waters, WV

Purpose

The VA Office of Inspector General (OIG), Office of Healthcare Inspections reviewed allegations that there are an increasing number of Veterans Health Information Systems and Technology Architecture (VistA) outages that affect patient care and that the Office of Risk Management and Incident Response (RMIR) does not perform risk management, but only reports incidents to the higher echelons. As an example, the complainant pointed to a 23-hour VistA outage that occurred on March 16, 2009, which affected patient care for the entire North Texas Healthcare System.

Background

A. VistA

VistA is an integrated system of software applications that directly supports patient care at Veterans Health Administration (VHA) healthcare facilities. It connects VHA facilities' workstations and PCs with nationally mandated and locally adapted software applications that are accessed by end users through a graphical user interface known as the Computerized Patient Record System (CPRS).

B. VistA Responsibility Realigned to OI&T

Approximately 2 years ago the responsibility of VistA software and infrastructure support was realigned under the Office of Information and Technology (OI&T). Program management for VistA is performed by the Office of Enterprise Development. The Office of Enterprise Operations and Infrastructure is responsible for the VA's IT Operations and maintaining the infrastructure.

C. Responsibility for Risk Management and Mitigating Service Disruptions

Under the OI&T umbrella, the Office of Information Protection and Risk Management (IPRM) oversees funding and all information and technology activities relating to information protection and security, including privacy and records management, cyber security, risk management and incident response, business continuity, and IT field security operations. IPRM also develops, implements, and oversees policies, procedures, and training on safeguarding veterans' personally identifiable information (PII) with which VA has been entrusted.

IPRM's responsibilities are spread among five offices:

- Privacy and Records Management.
- Cyber Security.
- Risk Management and Incident Response.
- Business Continuity.
- IT Field Security Operations.

The Office of Business Continuity is OI&T's center of excellence in the areas of IT contingency planning, emergency preparedness, and continuity programs. Business Continuity planning seeks to actively prevent disruption of VA mission-critical IT services, and to swiftly reestablish full functionality, if an interruption should occur. Business Continuity staff provides the framework for building resilience and capability for an effective response that safeguards the interest of VA and its administrations.

The Office of Risk Management and Incident Response (RMIR) is responsible for a cost-effective Information Risk Management framework that encompasses all data processing and information environments for VA. RMIR activities focus on Incident Resolution, Risk Management, Identity Safety, and Education and Policy.

RMIR is responsible for both information protection issues as well as IT incidents that include system disruptions affecting patient care. The OI&T Functional Statement lists the responsibilities of the RMIR to include the following:

- Establish and maintain a formal incident response capability.
- Provide relevant data on incidents to the appropriate organizations.
- Evaluate information sources, risk management systems, and mitigation techniques for efficiency, effectiveness and opportunities for improvement management.
- Develop strategies for education on incident mitigation and risk management techniques, and strategies for the prevention of negative incidents.
- Direct mitigation efforts in response to incidents.
- Coordinate with OI&T staff in areas of infrastructure and engineering.

D. VA North Texas Healthcare System

The VA North Texas Healthcare System (VANTHCS) consists of the main medical center, Dallas VA Medical Center (VAMC); the Sam Rayburn Memorial Veterans Center (SRMVC) in Bonham, Texas; and eight outpatient clinics in northern Texas. It is a component of Veterans Integrated Services Network (VISN) 17. The Dallas VAMC occupies an 84-acre campus providing multi-specialty outpatient clinics as well as:

- Acute Care Medical Center – 289 beds.
- Transitional Care Unit – 90 beds.
- Domiciliary Care Unit – 40 beds.
- Spinal Cord Injury Center – 30 beds.
- Telemetry Unit – 39 beds.
- Psychiatric Residential Rehabilitation Treatment Program – 56 beds.

SRMVC in Bonham, Texas, provides primary health care, nursing home care, and long-term rehabilitative care to eligible veterans. Located on a 78-acre site, SRMVC serves veterans in north Texas and southern Oklahoma, providing a full range of primary and geriatric care programs for the rapidly growing population of aging veterans. Facilities include:

- Nursing Home Care Unit – 139 beds.
- Domiciliary Care Unit – 224 beds.
- Psychiatric Residential Rehabilitation Therapy Program – 5 beds.

E. VistA Outage at VA North Texas Healthcare System

On March 16, 2009, there was a reported dual hard disk failure causing the loss of the CPRS and VistA for the entire VANTHCS for 23 hours. For 6 hours clinicians were not able to access patient medical records until a VistA Read Only system was made available. All medical notes and records were written on paper and added back to the VistA system at a much later date. There were no reported patient safety incidents during the event; however, the Dallas VAMC documented patient care lessons learned in an "After Action Report."

Scope and Methodology

The scope of this investigation was limited to determining whether the allegations had substance and to assess the impact to patient care during the VistA outage at VANTHCS on March 16, 2009. In regard to the allegation that the RMIR only reports incidents to higher echelons, we interviewed officials in the RMIR office, the IPRM office and other OI&T officials. We reviewed briefings and documents prepared by the IPRM and RMIR offices that described their roles, policies and procedures. For the allegation that the VistA outages are increasing we interviewed OI&T officials, VHA officials, the

Healthcare Systems Technical Support (HSTS) office, the HDI Patient Safety Office, several VAMC Directors, VAMC CIOs, VISN CIOs, and clinical providers and staff knowledgeable about the outage. We toured several departments within the medical center to determine if contingency computers were located on the units. We requested staff to demonstrate accessing the contingency computers to determine their competency.

This investigation involved a site visit to the VA North Texas HCS on June 22–24, 2009, where we interviewed clinical and administrative staff at the medical center. These interviews included:

a. The complainant by telephone on May 1, 2009, by telephone.

b. VANTHCS IT supervisor by telephone on May 12, 2009.

c. Director, Service Coordination for VHA, Office of Health Information by telephone on June 19, 2009.

d. DAS for Office of Risk Management and Incident Response on June 12, 2009.

e. Conducted a site visit to the Dallas VAMC on June 22–24, 2009, where interviews of clinical, administrative and IT staffs were performed.

f. Healthcare System Tech Support Team lead by telephone on July 17, 2009.

g. HP Expertise Center team lead by telephone on July 20, 2009.

h. DCIO and DAS for Information Protection and Risk Management on July 23, 2009.

i. OI&T Business Continuity team lead on August 3, 2009.

j. Director, HDI Patient Safety July 24, 2009.

k. Butler VAMC Director July 30, 2009.

l. Coatesville VAMC Director on August 3, 2009.

m. Hines VAMC Acting Assistant Director on August 3, 2009.

We reviewed documents relating to this incident including the Automated Notification Report of the outage, Contingency plans, site logs and records, After Action reports, HSTS records, Hewlett Packard (HP) Customer Advisories, and OI&T incident reports.

We conducted the inspection in accordance with *Quality Standards for Inspections* published by the President's Council on Integrity and Efficiency.

Findings

A. Risk Management

We substantiated the allegation that the Office of Risk Management and Incident Response reports incidents to higher echelons and has not performed risk management for risks associated with VistA outages. The RMIR staff receives Automated Notification Reports (ANR), performs follow up calls to ensure accuracy, and prepares higher-level notification for upper management. The RMIR office did not have any trending data or performance measures relating to VistA incidents. The Daily Incident Reporting function was realigned to the Command Operations Center in July 2009.

B. VistA Outage Trends

We were not able to substantiate that VistA outages are occurring more frequently since OI&T does not collect that data. The tracking and trending of hardware failures and system outages to identify risks is not currently being done in the OI&T organization for VistA outages. The ANRs were not designed for tracking and trending system outages. Contrary to the name, ANRs are not generated automatically, but are input manually and reported voluntarily. As such, we found many inconsistencies, missing data, and incidents of outages with no ANR.

When the RMIR staff performed their reporting functions for the OI&T Daily Incident Report, they could not rely solely on the ANR reports due to incompleteness, but would call the site to get additional information. Recently on August 17, 2009, the Denver Regional Data Processing Center (RDPC) had a service disruption of all services to 16 VAMCs affecting thousands of patients for 4.5 hours. The ANR for this outage had few details and "unknown" listed as the duration of the outage.

We found 2,022 records in the ANR database on the OI&T Service Desk website that included the key word "Vista" for the period July 1, 2007, through June 30, 2009. Of the 2,022 ANRs there were 666 records that contained the words Service Disruption, Emergency Maint., Emergency Upgrade, System Down, or Unscheduled System Down. More than half, 334 of the 666 records, did not include the outage duration but listed the time as "unk" or unknown. The ANRs typically are not specific enough to track certain hardware failures or other root causes.

The minutes of the VHA-OI&T Operational Services Committee reflect that this issue was raised by VHA at the October 14, 2008, meeting and remained as an open item until closed and marked as unsatisfied on June 9, 2009. No explanation for closure was given, although the minutes stated the item "will be maintained on a Service Coordination listing and revisited for progress/improvement in the future."

C. Impact on Patient Care

During our onsite investigation at VANTHCS in June 22–24, we conducted interviews of providers and staff at the medical center to get an assessment of the impact to patient safety and care. During the interviews, we discussed the effectiveness of the contingency plans and what changes have been made subsequent to the outage. We found that as the time of the outage extended, an increasing number of coordination problems developed between the medical services, patient tracking was much more difficult, and coordination with the Pathology Lab to get test results became extremely difficult to manage. The facility conducted a "Hot Wash Up" meeting soon after the event and produced an "After Action" report that made some significant adjustments to improve coordination and patient care when future outages occur. There were two incidents that occurred during the outage, but these incidents were determined to be not directly related to the outage.

VistA "Read Only" (RO) is a contingency system that allows providers to view static health records. Although Vista RO had not been fully implemented at all VAMCs nationally and had not been implemented at VANTHCS prior to the system disruption, the technicians were able to make the system available to providers 6 hours after the outage began. Since the health records in VistA RO are static, the utility to providers decreases during extended outages.

We found that patient care had been significantly impacted by the loss of this critical medical system during this outage. During this outage it was found that the number and placement of contingency computers was not adequate. The contingency computers provided a patient summary that a clinician needed to scroll through to get an assessment of the patient history. There was additional confusion due to lack of training on the contingency computers and for the VistA RO system when it was made available. The paper forms used to request tests, pharmaceuticals, and to document procedures performed were short in supply and found to be poorly designed. Missing data on forms added to the confusion and delays. Many clinicians felt that the risks to patient safety increased dramatically as the outage continued. Reverting back to paper was more burdensome to some of the medical services than others, but getting the medical records updated was still in process at the time of our visit. The subsequent paper records require scanning into VistA imaging and do not have the same utility as the records in CPRS.

D. Root Cause Report and Recommendations

A report titled, "Dallas VA Medical Center Outage of March 16, 2009," which was dated April 3, 2009, was prepared by the VA Expertise Center for OI&T. It discussed the root cause for the outage, identified concerns, and made recommendations to reduce the risk of future VistA outages. This report had limited distribution within OI&T, but it was not made available to the medical center, the VISN Director, or VHA.

The report stated the following,

> The root cause of the failure was a double drive failure within 1.5 minutes of each other which will cause a single disk group EVA to hang. The two disks that failed were both older 36GB disks. While the disks were definitely reporting errors it has been determined that a later revision of the EVA firmware could have allowed the drive failures to be handled more gracefully by allowing enough time for the first failed drive to be removed from the configuration prior to the 2nd drive failure. This later firmware revision is in production on other EVA 5000s in the VA but it is possible other EVAs are also running this older firmware.

In a Customer Advisory from the vendor dated February 1, 2007, this firmware was recommended to be upgraded immediately. The fixes that were addressed in the newer version of firmware addressed many issues, but they included the suspected cause in this outage.

The contractor raised some areas of concern in the report and made recommendations regarding the aging infrastructure. The hard drives that failed were 36GB hard drives that had been in operation for 4–6 years and were nearing the end of their service life, December 13, 2009. There are approximately 1,600 of these 36GB drives still in service, but the report noted that a survey needed to be performed to determine the location of these drives and configuration of the systems at the VAMCs. Additionally, the report made recommendations to address higher risk single points of failure that could cause future outages. The recommendations included implementing a high availability configuration in those VAMCs that do not currently have them. This recommendation would provide redundancy in the event of certain VistA storage system failures. The contractor recommended that there should be at least two disk storage groups in systems that are not shadowed by a high availability configuration.

Conclusions

A. Patient Safety Secondary to Other Priorities

The OI&T and RMIR offices are not focused on risks affecting patient care and safety but rather on information protection and other IT priorities. The VA Expertise Report that identified the cause, risks, and recommendations to improve reliability of this critical medical support system was not provided to the VAMC, VISN, or VHA. This report identified that equipment had outdated firmware affecting this outage and made recommendations about system risks and configurations that VHA should be made aware of and have input toward resolution. The report brought to light aging infrastructure issues, the need to survey system configurations, and identified higher risk single points of failure. The fact that this root cause report, with implications for patient care and safety, had such a limited distribution and did not include VHA raises the highest concern.

Recent efforts by the OI&T to increase VistA reliability has focused on building Regional Data Processing Centers (RDPCs) for VistA processing and storage. Currently Regions I and IV rely on RDPC support. Providing RDPC support to Regions II and III is at least 2 years away. VANTHCS is located in Region II and has not been provided a schedule of when system upgrades to include RDPC support will occur. The locations and numbers of these older 36GB hard drives will not be known until OI&T conducts a survey to determine the components and configuration of many of the VAMC VistA systems.

B. Performance Measures

The collection of consistent data on VistA system and subsystems is essential for performance measures to be developed and monitored. Currently this critical system does not have the framework in place to track and trend outages and reliability of this critical medical support system. VHA has attempted to collect data for reliability analysis but was unable to do so, due to omissions, inconsistencies, and errors in the ANR reporting system. This issue was raised by VHA but could not be resolved by the VHA-OI&T Operational Services Committee, where it sat as an action item for 8 months before being closed as unsatisfactory. No reason was provided in the minutes to explain the difficulties or why action was not taken.

C. Contingency Plans, No Substitute for a Backup System

Contingency plans for system outages are necessary band aids that help mitigate the loss of a critical healthcare support system, but they are no substitute to a backup system. A contingency plan that is designed for a 4-hour or less outage may not be adequate for an outage of 24 hours. Contingency plans cannot anticipate all situations that may impact patient care and safety due to system outages. The Dallas VAMC "After Action Report" noted that more drills, training, patient tracking, inadequate forms, and locations of contingency computers were issues identified that needed to be addressed. During our interviews with medical staff, a common comment was that they were lucky to not have had a serious patient incident.

D. Redundancy and High Reliability

The "After Action" Report from VANTHCS made a recommendation that a second VistA system be available for redundancy and increased reliability. This recommendation was deemed not cost effective in the report; however, the VAMC Director did not know the cost of implementing this solution. The Director did strongly support the need for a high availability system as a backup.

Recent outages at the RDPCs that affected many VAMCs at one time demonstrate that local backup systems should be considered in order to minimize the impact of system outages on patient care.

Recommendations

Recommendation 1. We recommended that the Assistant Secretary for Information and Technology ensure that the Office for Enterprise Operations and Field Development provide a plan that addresses VistA outages and solutions that may include a backup system with a high availability configuration at VAMCs not currently supported by a RDPC.

Recommendation 2. We recommended that the Assistant Secretary for Information and Technology ensure that the Office for Information Protection and Risk Management establish and track performance measures that monitor essential medical IT systems such as VistA.

Recommendation 3. We recommended that the Assistant Secretary for Information and Technology ensure that the Office for Information Protection and Risk Management performs and reports on risk management for essential medical IT systems.

Recommendation 4. We recommended that the Assistant Secretary for Information and Technology ensure that the Office for Enterprise Operations and Field Development provide a status report on all significant medical IT system failures or outages affecting patient safety and care to the Acting Under Secretary of Health.

Recommendation 5. We recommended that the Assistant Secretary for Information and Technology ensure that the Office for Enterprise Operations and Field Development develop a plan that addresses the aging medical IT infrastructure in Regions II and III and provide to the Acting Under Secretary of Health.

Comments

The Assistant Secretary for Information and Technology concurred with the findings and recommendations and submitted appropriate implementation plans. However, we note that at the time of submission of the plans, one completion date was yet to be determined. See Appendix A, on pages 10–15 for the full response from OI&T. We will follow up until all actions are completed.

Because the report dealt with VHA, we provided the draft to the Acting Under Secretary for Health even though there were no recommendations for their action. VHA wanted to submit comments, which are included in their entirety in Appendix B, on pages 16–20.

(original signed by:)
JOHN D. DAIGH, JR., M.D.
Assistant Inspector General for
Healthcare Inspections

Appendix A

Assistant Secretary for Information and Technology Comments

Department of Veterans Affairs **Memorandum**

Date: September 28, 2009

From: Assistant Secretary for Information and Technology (005)

Subject: **Healthcare Inspection –** VistA Outages Affecting Patient Care, Office of Risk Management and Incident Response, Falling Waters, WV

To: Assistant Inspector General for Healthcare Inspections (54)

1. The VA Office of Information and Technology (OI&T) acknowledges receipt of the Office of Inspector General's report and concurs with recommendations. OI&Ts response and target completion dates are enclosed.

2. Thank you for the opportunity to comment on your recommendations. If you have any questions, please contact Jeff Shyshka, Deputy Chief Information Officer for Enterprise Operations and Field Development at (559) 241-6408.

(original signed by:)

Roger W. Baker

Assistant Secretary for Information and Technology's Comments to Office of Inspector General's Report

The following comments are submitted in response to the recommendations in the Office of Inspector General's report:

OIG Recommendations

Recommendation 1. We recommend that the Assistant Secretary for Information and Technology ensure that the Office for Enterprise Operations and Field Development provide a plan that addresses VistA outages and solutions that may include a backup system with a high availability configuration at VAMCs not currently supported by a RDPC.

Concur **Target Completion Date:** February 2010

In May 2009, the Assistant Secretary for Information and Technology authorized EOFD to proceed as quickly as possible to implement consolidation of all VistA systems into regional Class III data centers. The data center selection process is under way for Regions 2 and 3 with the expectation that facilities will be leased and ready to begin VistA system migrations in late FY10.

The National Data Center Program (NDCP) was chartered in 2006 with the distinct goal of establishing a computing environment for the VistA system to include disaster recovery capability and high availability. There is a master project plan and communications with VHA are ongoing on the progress of this initiative. An MOU reinforcing the plan was signed in December 2008 by the AlS OI&T and the USH. OI&T is 45% complete with the transition to regionalized implementations of the VistA system that include disaster recovery capabilities and localized (medical center) implementations of the VistA Read Only (VistARO) contingency system. These systems serve VAMCs in OI&T Regions 1 and 4.

OI&T notes that VistA was not architected for 100% uptime. Provision of a second VistA system within the same data center as the original will avoid only one outage scenario, while not addressing a myriad of other issues that can also cause VistA availability outages. As it is in-line with current OI&T plans to improve VistA system availability at all hospitals, OI&T agrees that it should expedite the installation of the VistA Read Only platform at all hospitals not yet supported by an RDPC.

Recommendation 2. We recommend that the Assistant Secretary for Information and Technology ensure that the Office for Information Protection and Risk Management establish and track performance measures that monitor essential medical IT systems such as VistA.

Concur **Target Completion Date:** Completed

In early June, EOFD began reporting available system performance metrics for VistA and other systems within the VA enterprise to the Assistant Secretary for Information and Technology (ASIT). In July, access to the daily metrics report was provided to VHA management interested. Currently, performance metrics for all VistA systems located within RDPCs are reported on a daily basis. Performance measures related to the Computerized Patient Record System (CPRS) and other key health applications have been reported for all VAMCs on a weekly and monthly basis for several years. The aggregate of these performance measures will also be added to the daily report to the ASIT within 90 days. This information has been briefed to the Secretary of Veterans Affairs during his daily 8:00 AM operational review meeting. At this meeting, the Secretary is also briefed on all system outages reported for the last 24 hours. Until August 1, 2009, this report was prepared by Risk Management and Incident Response (RMIR). It is now prepared by the Integrated Operations Center (IOC), with RMIR assistance.

Recommendation 3. We recommend that the Assistant Secretary for Information and Technology ensure that the Office for Information Protection and Risk Management performs and reports on risk management for essential medical IT systems.

Concur **Target Completion Date: TBD**

OI&T Risk Management and Incident Response (RMIR) agrees that a proactive, independent OI&T Risk Management Program is needed to address Information Technology (IT) risks, to include medical IT systems. This approach must be in coordination with our customers and partners at the VHA.

RMIR has worked actively to implement a comprehensive, proactive IT Risk Management program to assist in identifying and mitigating risk to IT

systems. As a result of the major west coast VA Medical Center service disruptions resulting from the Sacramento Regional Data Processing Center failure on August 31, 2007, and the subsequent program management review (PMR) of the Regional Data Processing Center (RDPC) Program, RMIR performed an analysis of the risks associated with that program. The contract through which this analysis was conducted will lapse this year, and RMIR has been unable to contract for additional support due to contracting resource constraints within the department.

Recommendation 4. We recommend that the Assistant Secretary for Information and Technology ensure that the Office for Enterprise Operations and Field Development provide a status report on all significant medical IT system failures or outages affecting patient safety and care to the Under Secretary of Health.

Concur **Target Completion Date:** Completed

In January 2008, the Office of Risk Management and Incident Response (RMIR) began producing an incident report on a daily basis, reporting significant major IT system outages and information breaches. It is distributed to staff in all administrations and major program offices throughout VA, and briefed to the Secretary by the Assistant Secretary for Information and Technology at the daily 8:00 a.m. operational status meeting. The distribution list is extensive, and includes the Acting Under Secretary for Health and members of the VHA management team. In addition, the new Assistant Secretary for Information and Technology frequently communicates with VHA senior management via phone, email, or in person, regarding ongoing outages as they are occurring.

The March 17 and 18, 2009 versions of the Daily Incident Report included the incident mentioned in this OIG report regarding the VistA outage at the North Texas Healthcare System. Emergency reports and updates, called Incident Response Alerts (IRAs), are also sent throughout the day, as necessary.

In August 2009, RMIR transitioned the responsibility of producing the electronic Daily Incident Report and service disruption IRAs to the Integrated Operations Center.

In Service Level Requirement 2.2 of the Service Level Agreement (SLA) for IT Services between OI& T and VHA, the requirement to provide an After Action Report (AAR) following any significant service disruption has been defined. When events occur that adversely impact operations at VHA VAMCs, an AAR is generated. The AAR summarizes the event timeline, causal factors, critical findings and remediation actions (both accomplished and planned). The AAR for the subject outage was completed on March 18, 2009. There is no evidence that any AARs have been deliberately withheld from anyone with a need to know within VHA. However, OI&T will emphasize a proactive approach to communication of AARs to appropriate VHA staff whenever an AAR is created. At a minimum, the monthly VHA OHI Service Coordination meeting is an appropriate forum to share documents such as an AAR.

Recommendation 5. We recommend that the Assistant Secretary for Information and Technology ensure that the Office for Enterprise Operations and Field Development develop a plan that addresses the aging medical IT infrastructure in Regions II and II and provide to the Under Secretary of Health.

Concur **Target Completion Date:** December 2009

In the spring of 2009, the Facility Infrastructure Standards and Improvement (FISI) assessment was completed. The purpose of FISI was specifically to identify aging physical infrastructure that supports IT systems at VA facilities. The results of this assessment indicate that an investment of over $100 million is required to remediate serious, long-standing infrastructure vulnerabilities at VAMCs. The collocation of VistA systems at national data centers is in large part due to the infrastructure vulnerabilities that exist at VAMCs. As VistA systems in Regions 2 and 3 are migrated to the NDCP environment, the VAMC-based system will be replaced with the VistARO contingency system.

EOFD will maintain a Configuration Management (CM) program for the VistA platform. This program is executed in a partnership with the contractors mentioned in this report. VA VistA CM includes enterprise level testing of software and firmware as well as compliance monitoring with changes to the VistA platform at VAMCs or data centers that have been deemed critical to the availability and performance of the VistA

system. As VistA systems reach thresholds for capacity and performance, EOFD recommends and implements platform modifications to maintain system stability.

EOFD is currently performing an analysis, as it has in the past, based on historical trends in system utilization and performance using SPEC rate and M commands per second. The analysis determines the sites that are in need of a hardware refresh as well as projecting trend lines to determine when other sites will begin to be at risk for performance degrades. This analysis will highlight which sites require attention between now and when they are migrated to a National Data Center. In the meantime, and in parallel, all sites in Regions 2 and 3 are being migrated to Cache v5.2 and a client-server architecture. These changes serve to improve performance, improve stability, and add somewhat more fault tolerance. In the course of these upgrades, some sites have already received additional hardware as well. The output of the aforementioned analysis will furnish the plan that will bridge the gap between the present and when all sites will have been migrated to a National Data Center.

Appendix B

Department of Veterans Affairs **Memorandum**

Date: September 28, 2009
From: Acting Under Secretary for Health (10)
Subject: OIG Draft Report, *Healthcare Inspection, VistA Outages Affecting Patient Care Office of Risk Management and Incident Response Falling Waters, WV,* Project No. 2009-01849-HI0112 (WebCIMS 439138)
To: Assistant Inspector General for Healthcare Inspections (54)

1. I have reviewed the draft report, and I concur with the findings and recommendations. The concerns outlined in the report coincide with issues that VHA has had previously. It has been VHA's observation that the VA Office for Information Protection and Risk Management (IPRM) does not perform actual risk management activities for medical information technology (IT) systems. Rather, their demonstrated focus has been on privacy and data loss issues, not IT operations and systems. VA agrees with OIG that in order to maintain an effective incident response capability, and efficiently mitigate system disruptions affecting patient care, it is essential that IPRM's Office of Risk Management and Incident Response perform and report on risk management for Veterans Health Information Systems and Technology Architecture (VistA) and other essential medical IT systems.

2. To provide context for VHA's comments included on the attachment, it is important to describe impacts to patient care as a result of a VistA outage. These impacts are typical to any VA medical center experiencing an extended loss of this critical system. The report does describe patient care impacts, but other effects and costs due to VistA outages also need to be understood and addressed. These include indirect costs such as the loss of medical center staff (including clinical care providers) who are redirected to other tasks dealing with the outage, decreased productivity due to the use of manual procedures, backfilling of the database from paper forms collected during the outage, and the loss of data that were unable to be captured manually during the outage. Such evidence suggests an extended outage of this critical system, has far-reaching implications for immediate patient care and safety as well as long-term effective medical center operations.

3. Attached are VHA comments and concerns related to each of the Office of Inspector General recommendations.

4. One other issue of concern is the need for more frequent opportunities to practice what actions need to be taken during computer outages. This could take the form of having VHA facilities and OI&T personnel to conduct regular outage drills to ensure all staff has the training and experience needed to prepare for extended

computer outages. This could be incorporated into existing emergency management procedures and programs. One other issue of concern is the need for more frequent opportunities to practice what actions need to be taken during computer outages. This could take the form of having VHA facilities and OI&T personnel to conduct regular outage drills to ensure all staff has the training and experience needed to prepare for extended computer outages.

5. Thank you for the opportunity to review the report and provide comments. I would be pleased to discuss any concerns or comments you may have about this response. If you have any questions, please have a member of your staff contact Margaret Seleski, Director, Management Review Service (1085) at (202) 461-7245.

Gerald M. Cross, MD, FAAFP

Attachment

Appendix B

VETERANS HEALTH ADMINISTRATION
Additional Comments Related to Recommendations in OIG Draft Report,
Healthcare Inspection, VistA Outages Affecting Patient Care Office of Risk Management and Incident Response Falling Waters, WV
Project No. 2009-01849-HI-0112 (WebCIMS 439138)

Recommended Actions	Status	Completion Date

Recommended Improvement Action(s) 1: Ensure that the Office for Enterprise Operations and Field Development provide a plan that addresses VistA outages and solutions that may include a backup system with a high availability configuration at VAMCs not currently supported by a RDPC.

VHA Comments

Concur

If this is approved as a final OIG recommendation, VHA is available to review any VHA Office of Information and Technology (OI&T) plan for impact on VHA operations (e.g., resources and cost) as well as discuss with OI&T how the proposed plan would overlap with and effect similar activities currently underway in OI&T, such as:

(a) Veterans Health Information Systems and Technology Architecture (VistA), VistA Read-Only (VistA-RO) Project: Scheduled to complete VistA-RO deployments across Region Two (R2) and Region Three (R3) by January 2010.

(b) R2 and R3 consolidations into Regional Data Processing (RDP) facilities: slated to commence in April 2010 (per latest information from the Ol&T RDP Project Manager)

According to VHA OHI's recent assessment, Ol&T's High Availability (HA) architecture for R1 through R4 remains in flux at this point though it is estimated to cost $60M and take until 2012 for full deployment. Deployment of a VAMC-based HA solution across R2 and R3 may incur similar or even greater costs and take as long.

Recommended Improvement Action(s) 2: Ensure that the Office for Information Protection and Risk Management establish and track performance measures that monitor essential medical IT systems such as VistA.

VHA Comments

Concur

VHA advocates that the premise for establishment of Enterprise Service Level Agreements should be to define performance metrics for critical IT systems such as VistA.

Recommended Improvement Action(s) 3: Ensure that the Office for Information Protection and Risk Management performs and reports on risk management for essential medical IT systems.

VHA Comments

Concur

VHA is concerned that opportunities for failure could continue unless there is an emphasis on increasing the role of pre-action assessments by OI&T. Additional duties aspects of these pre-action assessments conducted by the Office of Risk Management and Incident Response (RMIR) could include requirement to proactively conduct assessments of the condition and stability of hardware and software deployed, to evaluate recommendations for implementation from vendors for risk mitigation, and to actively track the status of these risks assessments and risk mitigation strategies for deployment to affected systems.

Recommended Improvement Action(s) 4: Ensure that the Office for Enterprise Operations and Field Development provide a status report on all significant medical IT system failures or outages affecting patient safety and care to the Under Secretary of Health.

VHA Comments

Concur in part

While VHA agrees with this recommendation in part, and suggests that VHA should work closely with the Office for Enterprise Operations and Field Development about assessments on all significant medical IT system failures or outages affecting patient safety and care. Such collaboration would help to ensure more accurate assessments.

VHA suggests the recommendation be reworded to require collaborations between VHA and the appropriate office in VA OI&T.

Recommended Improvement Action(s) 5: Ensure that the Office for Enterprise Operations and Field Development develop a plan that addresses the aging medical IT infrastructure in Regions II and III and provide to the Under Secretary of Health.

VHA Comments

Concur

This recommendation is a positive step towards addressing the compendium of issues noted in the OIG report related to patient safety and continuity of operations (i.e., the aging hardware, software upgrades, and implementations). VHA provides the following insights in regards to specific issues:

(c) For the short term, VA recommends that expected measures to be taken to remediate possible risks at other VA medical centers (VAMCs) through the use of Hewlett Packard Storage Works Enterprise Virtual Array 5000 disk devices still operating with identified faulty firmware needs attention.

(d) For the mid-term, Ol&T should define what should be done to ensure redundancy in operations in R2 and R3 while in a transition stage between decentralized and consolidated Regional Data Processing (RDP) environments needs to be defined.

(e) For the long term, it would be advantageous for VHA and other administrations to work with VA OI&T to assess OI&T plans for RDP consolidation to reduce the associated risk for future implementations as well as other potential risks inherent in the proposed model.

(f) Lastly, VHA suggests this recommendation be expanded to cover all four regions R1 through R4 and collaborate about the development of the plan with appropriate VHA program office prior to delivery of the plan to the Under Secretary for Health.

Veterans Health Administration
September 2009

Appendix C

OIG Contact and Staff Acknowledgments

OIG Contact	Anthony M. Leigh Director, Healthcare Financial Analysis Division 410-637-4721
Acknowledgments	Michael Shepherd, M.D. Thomas Seluzicki Annette Robinson Derek Montgomery

Appendix D

Report Distribution

VA Distribution

Office of the Secretary
Assistant Secretary for Information and Technology
Veterans Health Administration
Assistant Secretaries
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

This report is available at http://www.va.gov/oig/publications/reports-list.asp.