US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

VA Needs to Strengthen Controls to Address Electronic Health Record System Major Performance Incidents

Audit | **22-03591-231** | **September 23, 2024**

BE A
VOICE FOR
VETERANS
REPORT WRONGDOING
vaoig.gov/hotline | 800.488.8244

OUR MISSION

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

CONNECT WITH US

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

PRIVACY NOTICE

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Executive Summary

VA has been working to replace its original electronic health record (EHR) information system with a more modern one that is intended to be interoperable with the one used by the Department of Defense (DOD). The goal is to provide healthcare personnel with a comprehensive medical history for veterans. In May 2018, VA awarded a 10-year contract to Cerner (now Oracle Health) for a new EHR solution.[1] The new EHR system's estimated cost has grown. It was originally $16 billion and may reach close to $50 billion.[2]

The EHR system experienced hundreds of major performance incidents affecting the five VA medical centers where the system was initially deployed.[3] A performance incident is defined as major when it causes severe system degradation, leads to an outage of services required for VA's key operations, or affects patient care and requires a response beyond routine incident management.[4] VA clinicians need timely access to patient medical records. In response to these issues, VA halted all planned EHR deployments in July 2022, with the exception of the deployment at the Captain James A. Lovell Federal Health Care Center in North Chicago, Illinois, on March 9, 2024. Since then, however, major performance incidents have continued, as recently as March 2024.[5]

The VA Office of Inspector General (OIG) conducted this audit to determine whether VA and Oracle Health had sufficient controls in place to prevent, respond to, and mitigate the impact of the EHR system's major performance incidents.

[1] The Oracle Corporation acquired Cerner Corporation, including Cerner Government Services Inc., on June 8, 2022, and assumed responsibility for the EHR contract with VA. Cerner became Oracle Cerner at that time and now goes by Oracle Health Government Services Inc. This report refers to the contractor as Oracle Health.

[2] *Hearing on VA's Electronic Health Record Modernization: An Update on Rollout, Cost, and Schedule*, *Before the Subcommittee on Military Construction and Veterans Affairs, Senate Committee on Appropriations*, 117th Cong. (September 21, 2022) (testimony of Brian Q. Rieksts, Institute for Defense Analyses). The analyst testifying at the hearing estimated the program's cost could rise to $49.8 billion, an amount that included $32.7 billion during the implementation phase and $17.1 billion for sustainment, covering the implementation phase and 15 years of operation after the system is deployed to all sites. As of June 2024, the Electronic Health Record Modernization (EHRM) Integration Office chief of staff reported VA was working on updating the program cost estimate.

[3] The five sites that initially deployed the EHR are Spokane VA Healthcare System, VA Walla Walla Health Care System, VA Central Ohio Healthcare System, Roseburg VA Health Care System, and VA Southern Oregon Rehabilitation Center and Clinics. For more information on the facilities included in these sites, see table A.1 in appendix A. VA deployed the EHR system at the Captain James A. Lovell Federal Health Care Center in North Chicago, Illinois, on March 9, 2024.

[4] This definition was incorporated into the EHR contract under a task order dated May 29, 2020. Before this task order, the EHR contract did not define a major incident.

[5] See appendix A for a chronology of these events.

What the Audit Found

The OIG found that VA and Oracle Health did not have adequate controls in place to prevent system changes from causing major incidents, to respond to those incidents when they did occur, and to mitigate their impact. The audit scope included 360 major performance incidents—outages, performance degradations, and incomplete functionality—that occurred between October 24, 2020, and August 31, 2022, and the team also reviewed incidents through March 2024.[6] The audit team obtained data on these incidents and selected a sample of 35 incidents from 2020 to 2022. An example of a major incident occurred on March 3, 2022, when the system was disrupted for 27 hours and seven minutes because a system change halted operations at the Mann-Grandstaff VA Medical Center in Spokane, Washington. Subsequently, the medical center director reported that many patients needed to have their appointments rescheduled.

Although other causes the team identified led to some of the issues identified in this report, ultimately the inadequate controls for handling major incidents originated in how the May 2018 contract was written. In May 2023, VA modified the contract to strengthen some requirements for addressing major incidents; however, incidents continued.

Major performance incidents have the potential to delay care to veterans, but they are not currently connected to patient outcomes. While VA routinely tracks patient safety events related to the EHR system as a whole, there is no formal process to link reporting of these events (which is voluntary) to specific major performance incidents.

The following sections discuss the OIG's finding regarding controls in greater detail.

Prevention Controls

Federal agencies are required to design and implement controls that facilitate risk management and compliance with applicable federal laws, policies, and standards.[7] The audit team identified weaknesses in several controls that could have prevented the major incidents in its sample—particularly *configuration management* and *assessment, authorization, and monitoring*. Lapses in these two controls resulted in VA experiencing a total of 23 incidents with 80 hours and 20 minutes of system disruption.

[6] The team only considered major performance incidents for which Oracle Health or VA was responsible—omitting any caused by other parties, such as DOD. For more information on the team's methodology, see appendix B.

[7] Throughout this report, the audit team refers to National Institute of Standards and Technology (NIST) publications as information system control guidelines. These publications provide guidance on controls to a diverse audience including agency officials with oversight responsibilities and system owners. The EHR contract performance work statement dated October 5, 2017, states that the contractor (Oracle Health) must provide the ability to host VA system components within the same locations as the primary EHR to improve user experience and response times and to support contingency and continuity situations. Further, the contract states the contractor must comply with all applicable NIST standards, including NIST Special Publication 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.

Configuration management controls provide protective measures for system components, such as hardware and software. Federal agencies must have effective general and business process application controls to achieve the appropriate confidentiality, integrity, and availability of information systems.[8] Since new components may be identified and some existing components may no longer be needed as the system matures, changes to the system's configuration should be vetted before implementation and associated activities are monitored throughout the system development life cycle.[9] This ensures that changes to configuration management do not disrupt the system and impair VA's ability to provide care to veterans.

The audit team found, however, that problems with configuration management controls caused the majority of incidents in the 35 sampled—accounting for 18 incidents lasting 65 hours and 49 minutes. For example, on March 14, 2022, the Mann-Grandstaff VA Medical Center experienced incomplete functionality for 10 hours and four minutes. This incident occurred because of an update that inadvertently corrupted some 870 user credentials and prevented those users from accessing part of the EHR system. The team concluded that this incident could have been prevented if the update and instructions had been monitored.

Similarly, problems with continuous monitoring had an impact on the system.[10] Continuous monitoring of information systems and organizations determines the ongoing effectiveness of controls, changes in information systems and environments of operation, and the state of system availability.[11] The audit team found five incidents in which Oracle Health was not continuously monitoring the EHR system, which accounted for 14 hours and 31 minutes of disruption. For example, on August 22, 2022, an incident affected all five sites for one hour and 38 minutes. Oracle Health explained its software errors created issues with data failing to populate in a separate application used by VA. Representatives from Oracle Health stated the contractor did not have monitoring in place at the time. After the incident, Oracle Health added monitoring that would alert it to the issue more quickly.

The majority of EHR system disruptions from the major incidents in the team's sample—about 77 percent of the hours—were attributable to problems with configuration management and monitoring. VA relied on Oracle Health's reporting of these incidents and did not have a formal

[8] Government Accountability Office (GAO), *Federal Information System Controls Audit Manual*, GAO-09-232G, February 2009. The EHR contract performance work statement dated October 5, 2017, notes that for configuration management, the contractor (Oracle Health) must update or change the system to ensure its effective use.

[9] NIST Special Publication 800-53. NIST Special Publication 800-34, rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, updated April 23, 2021, notes the system development life cycle encompasses the system's initiation, development and acquisition, implementation, operation, and maintenance, and ultimately its disposal.

[10] The EHR contract performance work statement dated October 5, 2017, notes that the contractor (Oracle Health) must comply with all applicable NIST standards related to information system authorization, testing, and continuous monitoring.

[11] GAO, *Federal Information System Controls Audit Manual*.

procedure for verifying contractor performance metrics and associated credits. By obtaining access to real-time EHR incident data and developing a formal procedure, VA could better prevent incidents, verify their duration, and impose penalties when warranted.

Response Controls

Response includes prioritizing incidents, notifying VA and Oracle Health stakeholders, resolving the incident, and afterward reporting on details. The team found that VA and Oracle Health did not have consistent or clear procedures, either in guidance or in the contract, for responding to major incidents.[12] According to the National Institute of Standards and Technology (NIST), the parties involved in operating a system should collaborate on developing incident response policy and procedures.[13] These controls should be applied consistently across the organization.[14] However, VA and Oracle Health responded according to who owned the incident, each following their own guidance.[15]

VA and Oracle Health had different criteria for how major incidents should be prioritized. VA's guidance shifted after the contract was signed, designating only incidents with critical impact and critical urgency as priority 1. In contrast, per the Oracle Health contract, designated incidents can qualify as priority 1 if they were critical or high in either urgency or impact.[16] This means VA's threshold for a major incident was higher, and it responded to fewer of its major incidents than Oracle Health. Without a consistent approach with Oracle Health for prioritizing incidents, VA lacks assurance that all incidents receive the necessary attention.

VA also lacked well-defined, consistent standards in its guidance for timely response and did not impose clear standards on Oracle Health in the EHR contract. For the seven incidents VA was responsible for, there were timeliness standards for responding to them. However, the OIG was only able to assess timeliness for one. Between 2019 and 2021, VA guidance specified response times for initial notification and resolution for VA-caused incidents of four priorities—critical, high, medium, and minimal. In 2021, VA revised its standards in guidance to specify *average*

[12] VA Office of Information and Technology (OIT), *Major Incident Management Process*, June 25, 2021; Oracle Health, *Major Incident Management Standard Operating Procedures*, November 18, 2021.

[13] NIST Special Publication 800-53.

[14] GAO, *Federal Information System Controls Audit Manual*. The absence of entity-wide processes may be a root cause of weak or inconsistent controls.

[15] Ownership is determined during incident response. An incident is deemed to be caused by VA when the incident is found by or reported to it, and vice versa. Neither the EHR contract nor VA and Oracle Health's major incident management guidance specifies the authority responsible for determining incident ownership.

[16] VA OIT, *Major Incident Management Process Escalation and Notification for Service Outages,* September 6, 2019; VA OIT, *Major Incident Management Process*. Incident prioritization was first referenced in the EHR contract dated May 17, 2018, as incident descriptions and prioritization categories. The prioritization process was later incorporated under an EHR task order that established standard operating procedures in November 2021. Oracle Health, *Major Incident Management Standard Operating Procedures.* Before this task order, the EHR contract did not define the prioritization process.

notification and resolution times and applied them only to critical and high-priority incidents.[17] Because these times were reportedly monthly averages, this change effectively loosened the timeliness standards for VA.[18] In contrast: For the 28 incidents Oracle Health caused during the audit scope, the contract established no clear notification time. The contract states only that Oracle Health in consultation with VA should act "immediately."[19] A senior Oracle Health manager said the goal is to start as soon as possible. Given the inconsistencies and lack of clarity in the expectations for major incident response time, the audit team could not determine whether VA or Oracle Health complied with the stated procedures in most cases.

Besides VA shifting the standards in its guidance, the audit team determined that VA's Office of Information and Technology (OIT) did not enforce them. According to an OIT director discussing the 2021 process document, the recovery times were held over from the 2019 version, were aspirational, and should have been removed. When it came to Oracle Health, since VA did not establish a clear standard for notification for its contractor, the team could not determine whether the times were appropriate for the incidents reviewed.[20]

When a major incident was resolved, neither VA nor Oracle Health consistently reported key information to minimize incident likelihood.[21] For five of the seven VA-caused incidents, the root cause sections of the reports were incomplete because VA omitted details on monitoring weaknesses, work-arounds, and individuals involved in root cause analysis. Similarly, for 20 of 28 Oracle Health–caused incidents reviewed, the contractor provided VA major incident reports that lacked elements such as incident classification, a summary of contributing factors, and irreversible correction and preventable actions. Without complete and consistent reporting on major incidents, VA cannot take adequate steps to ensure that they do not continue.

The audit team concluded that VA needs to update how it prioritizes major performance incidents to ensure that notification and resolution occur in a consistent manner; develop effective response guidance that consistently captures results for all major performance incidents; and develop a strategy to consistently collect, verify, and report the information needed in post-resolution reports.

---

[17] VA OIT, *Major Incident Management Process*.

[18] When times are listed per critical incident, as in 2019, users have some assurance that resolution will occur within 24 hours; when times are averages, as in the 2021 guidance, resolution of a given incident may occur within less or more than eight hours, and users do not know how much less or more. If all incidents in a month are included, individual times could be significantly under or over eight hours and still average to eight hours.

[19] VA contract 36C10B18D5000, Task Order 26, *VA EHRM System Performance Work Statement*, May 29, 2020.

[20] VA contract 36C10B18D5000.

[21] VA reporting requirements are outlined in VA OIT's *Problem Management Practice, Investigating and remediating the root cause of Major Incidents to prevent disruptions before they happen*, November 20, 2019. Moreover, incident reports are referenced in EHR contract documentation. For example, the EHR contract's performance work statement requires the contractor to identify; assess the impact of and report, track, escalate, and notify specialists and users about; and resolve incidents that occur within the EHR system.

Mitigation Controls

Because the EHR system is the primary means by which clinicians view information necessary to treat patients and create or amend patient records, there is immediate risk to patient care when that system is down. Federal agencies are directed to plan for downtime contingencies to mitigate risks of this type.[22] Accordingly, VA requires its offices to take actions that include identifying and assessing the risk to operations, developing and implementing strategies to mitigate this risk, and regularly training staff on these strategies.[23]

The audit team focused on the steps VA had taken to mitigate the risk to patient safety during EHR downtime. The team found that while VA had initiated two key strategies to continue patient care when the system is unavailable—procedures to follow during system downtime, and backup systems—it did not sign the procedures until May 2024, over three and a half years after launching the EHR system, and it was still implementing a strategy for its backup systems.[24]

The first of the two key mitigation strategies VA pursued but had not effectively implemented was ensuring clinicians are aware of the steps they should take in the event the system is unavailable. In May 2024, VA finalized national downtime procedures outlining the actions clinicians should take in the event the system is unavailable. While this was an important step, procedures still must be implemented and training provided. Without these additional measures, Veterans Health Administration (VHA) facilities risk staff confusion about what to do and delays that would negatively affect patient care.

VA also needs a better backup system for viewing patients' medical records when the EHR system goes down.[25] Two primary downtime viewer (DTV) options were available to clinicians when the EHR system was unavailable, yet neither option was suitable for all types of VA facilities or in the event the system was completely offline. The first option for clinicians was the Joint Longitudinal Viewer (JLV), which VA and DOD have shared since 2014 for viewing records.[26] However, when the EHR system experiences an outage, JLV does not connect with it.

---

[22] Office of Management and Budget (OMB), "Federal Agency Responsibilities for Maintaining Records About Individuals," app. I in OMB Circular A-130, *Managing Information as a Strategic Resource,* July 28, 2016; NIST Special Publication 800-34. In addition, VA requires information system contingency planning that meets NIST standards.

[23] VA Handbook 6500.8, *Information System Contingency Planning*, April 6, 2011, requires contingency planning for information systems. VA must have contingency plans in place to execute when system incidents occur. The contract specifies that Oracle Health must comply with this handbook.

[24] The audit team did not evaluate the effectiveness of the procedure because there was insufficient time within the audit scope to reasonably do so.

[25] VHA, "Oracle Health Cerner Millenium Electronic Health Record Downtime SOP" (standard operating procedure), VHA-ONS-NUR-23-01, November 14, 2023. According to this standard operating procedure, downtime is any period during which EHR resources are unavailable to users, including service degradation affecting the clinician's ability to document patient care.

[26] JLV is a web-based application that provides read-only medical data from DOD, VA, and community partners in a common data viewer.

This means that clinicians at all types of facilities were unable to use JLV to view any new EHR patient record.

The second option was one Oracle Health provided, a read-only system known as the 724Access DTV.[27] The Oracle Health DTV does not show records created farther back than seven days from the date a clinician is attempting to view a patient's record. This is particularly limiting at outpatient facilities, where a patient may not have been seen within the last seven days.[28]

Since there are over a thousand of these types of outpatient facilities, making up about 90 percent of the VA clinics nationwide, the audit team concluded that the limitations of JLV and DTV during an outage at these facilities were significant.[29] Leaders of VA's Electronic Health Record Modernization (EHRM) Integration Office have recognized the need for a solution that is suitable when the system is unavailable at all facilities. However, as of May 2024, VA and Oracle Health were still working on the implementation timeline for this solution.

The audit team concluded that VA needs to make sure all clinicians are familiar with the national downtime policy, identify the appropriate backup system, and develop a training strategy to ensure clinicians can use the backup system during downtime.

Opportunities to Improve EHR Controls

Many of the issues identified in this report began with the May 2018 contract, which did not include controls to address major incidents. For example, although the May 2018 contract referenced a DTV, the system provided by the contractor was not adequate to meet VA's needs. In May 2023, VA added requirements that would rectify some of the challenges described in this report. These new requirements included a metric that outlined monthly target percentages for the system to be free of incidents other than outages (incident-free time), an increase in the target monthly uptime for the system, and strengthened requirements for financial credits when problems were not resolved within established time frames. Separate from these requirements, in August 2023, VA contracted with Oracle Health to obtain a DTV to provide an additional tool for clinicians when the system is unavailable.[30]

Still, VA has additional opportunities to make future contract changes that could help improve its management of major incidents. Real-time EHR incident data sharing by Oracle Health would

[27] The EHR contract performance work statement dated October 5, 2017, notes that the contractor must provide a 724 DTV read-only system to replace each of the over 170 instances of original EHR read-only installations. This replacement must be implemented as part of each site deployment. The DTV provided to VA by Oracle Health was available as part of the EHR's commercial product suite and was not customized for VA.

[28] In this instance, outpatient facilities may use JLV to view patient records as long as the EHR system is not experiencing an outage.

[29] According to VHA, its healthcare system provides care through about 1,300 facilities, including about 170 medical centers and about 1,100 outpatient sites.

[30] As of May 2024, VA had yet to implement the additional tool.

provide VA with greater awareness and enable quicker oversight action. Detailed incident reporting would help VA determine root causes and prevent similar incidents from occurring.

Overall, to counter the risk that major EHR incidents pose, VA needs to strengthen its incident management controls. These improved controls should help prevent the weaknesses that contribute to incidents, provide adequate guidance to respond to incidents, and establish procedures and backup systems to provide continuity and mitigate impact during downtime. Accordingly, the OIG made a series of recommendations intended to improve these controls so that VA will have the information it needs to manage major incidents such as those described in this report.

What the OIG Recommended

The OIG made the following recommendations to the acting program executive director of the EHRM Integration Office:

1. Assess electronic health record major performance incident data needs and contractually commit to real-time data sharing that will provide greater awareness of system operations.
2. Develop a formal procedure for verifying performance metrics and associated credits to ensure VA receives the remedies it is due under the contract.
3. Update the process for prioritizing major performance incidents to ensure notification and resolution occur in a consistent manner.
4. Develop effective notification and resolution metrics that consistently capture results for all major performance incidents, regardless of the owner, and enforce them.
5. Identify the information needed in post-resolution reports, such as corrective and preventative actions, and require that the contractor to consistently collect, verify, and report that information as a contract deliverable.

The OIG made the following recommendations to the under secretary for health:

6. Develop a plan to ensure all clinicians are familiar with the national downtime procedures.
7. Identify the appropriate backup system and develop a training strategy to ensure clinicians can use the system during downtime.
8. Assess facilities' patient safety reports identified during this audit to determine if additional actions need to be taken and, if so, provide an action plan.
9. Develop a mechanism to better identify major performance incidents and negative patient outcomes and provide a plan to prioritize and address their causes.

VA Management Comments and OIG Response

The EHRM Integration Office acting program executive director concurred with recommendations 1 through 5 and provided a responsive action plan. The VHA under secretary for health concurred with recommendations 6 through 9 and provided a responsive action plan.

The VHA under secretary for health reported that actions completed in July 2024 satisfy recommendations 6, 7, and 9, and the under secretary requested closure of those recommendations. Specifically, VHA developed a plan to ensure that clinicians understand downtime procedures, identified appropriate backup systems and developed an associated training strategy, and developed a mechanism to better identify major performance incidents and negative patient outcomes. However, the OIG will keep these recommendations open until VHA provides evidence that it has (1) communicated its downtime procedure to clinicians and (2) implemented its mechanism to better identify major performance incidents and negative patient outcomes and provided its assessment for communicating negative patient outcomes. The OIG will monitor the implementation of planned actions and will close recommendations when VA provides sufficient evidence demonstrating progress in addressing the intent of the recommendations and the issues identified. Appendixes C and D include the full text of VA's comments.

LARRY M. REINKEMEYER
Assistant Inspector General for
Audits and Evaluations

Contents

Abbreviations

DOD	Department of Defense
DTV	downtime viewer
EHR	electronic health record
EHRM	Electronic Health Record Modernization
IT	information technology
JLV	Joint Longitudinal Viewer
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
VHA	Veterans Health Administration

Introduction

In May 2018, VA awarded a contract to Cerner (now Oracle Health) for a new electronic health record (EHR) system.[31] As of May 2024, the department was more than halfway into its 10-year timeline to implement this system across VA facilities nationwide. The goal of the new EHR system is to give veterans and their healthcare providers a comprehensive record to improve the quality of care, as the new system is intended to be interoperable with the Department of Defense (DOD) system and community providers.

Between October 2020 and June 2022, the EHR system had been deployed at five VA medical centers and experienced hundreds of major performance incidents.[32] Major performance incidents require a response beyond routine incident management as they could cause severe system degradation, lead to an outage of services required for VA's key operations, or affect patient care.[33] VA clinicians need timely access to patient medical records to make proper diagnoses; make informed, real-time decisions; and order medications, among other tasks. EHR system availability is therefore critical to delivering quality care and preventing potential patient safety incidents.

In April 2023, the VA Secretary halted deployments of the new EHR. This reset was to address the problems experienced by staff and patients at the five deployment sites, including system performance issues and issues with the system not functioning optimally. Appendix A presents a timeline of significant EHR implementation events.

The VA Office of Inspector General (OIG) conducted this audit because system availability is essential to VA carrying out its mission and ensuring patient care and because of the system's steep cost to taxpayers. During this audit, the OIG examined whether VA and Oracle Health had sufficient controls in place to prevent, respond to, and mitigate the impact of the EHR system's major performance incidents. The scope of the incidents reviewed was from October 24, 2020, when the EHR was implemented at the first VA medical facility, through August 31, 2022.[34]

---

[31] The Oracle Corporation acquired Cerner Corporation, including Cerner Government Services Inc., on June 8, 2022, assuming responsibility for the EHR contract with VA. Cerner became Oracle Cerner at that time and now goes by Oracle Health Government Services Inc. This report refers to the contractor as Oracle Health.

[32] The five sites that initially deployed the EHR are Spokane VA Healthcare System, VA Walla Walla Health Care System, VA Central Ohio Healthcare System, Roseburg VA Health Care System, and VA Southern Oregon Rehabilitation Center and Clinics. For more information on the facilities included in these sites, see table A.1 in appendix A. VA deployed the EHR system at the Captain James A. Lovell Federal Health Care Center in North Chicago, Illinois, on March 9, 2024.

[33] This definition was incorporated in the EHR contract under a task order dated May 29, 2020. Before this task order, the EHR contract did not define a major incident. Interruptions from major performance incidents may affect one or more medical centers and, if not resolved quickly, may require continuity actions.

[34] The audit team only considered major performance incidents for which Oracle Health or VA was responsible, omitting any caused by other parties, such as DOD.

Major performance incidents occurred throughout the audit and have continued, as recently as March 2024.

EHR Contract and Costs

As part of its contract for the new EHR system, VA requires Oracle Health to ensure the system is available and functioning through continuous monitoring.[35] Additionally, Oracle Health is contractually required to manage major incidents affecting the system. The Electronic Health Record Modernization (EHRM) Integration Office is responsible for preparing VA to deploy the EHR system. This office also maintains oversight of Oracle Health's work under the contract. Oversight includes instituting sufficient information technology (IT) controls, such as testing, that keep the system running smoothly. VA and Oracle Health signed a contract modification, effective in May 2023. As part of this modification, incident-related controls were strengthened—including establishing some performance metrics and requirements for financial credits that may be applied if requirements are not met.[36]

The total estimated cost of the EHRM program was originally $16 billion, which included implementation, project management, and some infrastructure costs.[37] At a congressional hearing in September 2022, a representative of the Institute for Defense Analyses testified that total costs may reach almost $50 billion, covering the implementation phase and 15 years of operation after the system is deployed to all sites.[38] As of June 2024, the EHRM Integration Office chief of staff reported VA was working on updating the program cost estimate.

Major Performance Incidents

As described above, a major performance incident results in a significant disruption to operations. In general, when such an incident occurs, it impedes clinicians' access to patient

[35] The EHR contract performance work statement dated October 5, 2017, states that the contractor (Oracle Health) must comply with all applicable National Institute of Standards and Technology (NIST) standards related to information system authorization, testing, and continuous monitoring. In addition, Oracle Health must provide the ability to support VA system components in the same locations as the primary EHR to improve the user experience, response times, or to support contingency and continuity situations.

[36] The May 2023 modification is discussed further in the report section "VA Did Not Tailor Contract Initially but Has Made Some Improvements."

[37] The OIG previously reported that program costs are expected to exceed the estimated $16 billion. VA OIG, *Deficiencies in Reporting Reliable Physical Infrastructure Cost Estimates for the Electronic Health Record Modernization Program*, Report No. 20-03178-116, May 25, 2021.

[38] *Hearing on VA's Electronic Health Record Modernization: An Update on Rollout, Cost, and Schedule, Before the Subcommittee on Military Construction and Veterans Affairs, Senate Committee on Appropriations*, 117th Cong. (September 21, 2022) (testimony of Brian Q. Rieksts, Institute for Defense Analyses). The analyst testifying at the hearing estimated the program's cost could rise to $49.8 billion, an amount that included $32.7 billion during the implementation phase and $17.1 billion for sustainment.

records and can therefore affect the quality of care they provide. As discussed later, these incidents require specific response procedures to manage their potentially severe impacts.

The contract specifies four types of major performance incidents:[39]

- **Outages** are unscheduled periods when the entire system is unusable.[40]
- **Performance degradations** are characterized by times when the system is available, but one or more system functions are operating more slowly than expected.
- **Incomplete functionality** is when the system is available, but one or more system functions no longer operate as intended.
- **Loss of redundancy** occurs when backup data necessary for continuity in the event of a system failure are not available. Because loss of redundancy incidents have no noticeable impact on the user, the audit team did not include them in its analysis.[41]

A former VA Deputy Secretary recognized that user frustration resulting from these incidents can disrupt how clinicians use the EHR system, which in turn can put patient safety at risk.[42] This frustration can also delay users' willingness to utilize the system.

Major Performance Incident Management

Once a major performance incident occurs, the responsible entity (either VA or Oracle Health) needs to manage the impacts on its operations.[43] Major incident management is a series of actions taken with the goal of restoring services as quickly as possible to minimize adverse impacts on operations.[44] Once an incident is identified and prioritized, teams of experts from both parties, known as major incident response teams, collaborate to resolve the problem, return

[39] These types were incorporated under an EHR task order that established standard operating procedures. Oracle Health, *Major Incident Management Standard Operating Procedures,* November 18, 2021. Before this task order, the EHR contract did not specify the different types of major incidents. However, a senior Oracle Health manager reported the contractor followed these procedures since the beginning of the EHR program. A major performance incident can be classified as more than one type of service disruption.

[40] By contrast, scheduled outages can be planned by Oracle Health when necessary to perform maintenance activities. These do not constitute a performance issue.

[41] According to Oracle Health, loss of redundancy has no noticeable impact on the user, and this was confirmed by an EHRM Integration Office leader and an OIT senior official.

[42] *Hearing on VA's Electronic Health Record Modernization: An Update on Rollout, Cost, and Schedule, Before the Senate Appropriations Committee, Subcommittee on Military Construction, Veterans Affairs and Related Agencies, Senate Appropriations Committee*, 117th Cong. (September 21, 2022) (statement of Donald M. Remy, former VA Deputy Secretary).

[43] For purposes of this audit, the team only reviewed major performance incidents for which Oracle Health or VA was responsible, omitting any caused by other parties, such as DOD.

[44] VA contract 36C10B18D5000, *Performance Work Statement for the VA EHRM System*, October 5, 2017.

the EHR system to full functionality, and report on the outcomes.[45] The teams initiate a bridge (or conference) call that brings together key subject-matter experts to identify incident details and decide on a solution, all while providing status updates to key stakeholders and staff.

At some point during the call, the teams identify either VA or Oracle Health as the incident owner, and that party is responsible for resolving the incident. Neither the EHR contract nor VA and Oracle Health major incident management guidance specifies the party responsible for determining incident ownership. According to a VA Office of Information and Technology (OIT) director, the practice is that the responsible party (VA or Oracle Health) is determined once the initial root cause of the incident is identified. The incident is then managed by the responsible party until it is resolved.

Occurrence of Incidents

From October 24, 2020 (initial EHR system go-live), through March 31, 2024, there were 826 major performance incidents involving outages, performance degradations, and incomplete functionality. These incidents affected the system for 1,909 hours and 26 minutes (table 1).

Table 1. Frequency of Major Performance Incidents by Type and Responsible Party from October 24, 2020, through March 31, 2024

Incident type	VA incidents	Oracle Health incidents	All	Time the system was affected (hours: minutes)
Incomplete functionality	165	555	720	1,623:55
Performance degradation	6	63	69	134:40
Performance degradation, incomplete functionality	0	10	10	57:24
Outage, incomplete functionality	0	5	5	38:18
Outage, performance degradation, incomplete functionality	0	9	9	36:11
Outage, performance degradation	0	6	6	11:49

[45] As of October 2023, the team may include VA incident managers and coordinators who are responsible for coordination of resources and communication for all major incidents, as well as shift supervisors and leads who conduct major incident management and reporting.

Incident type	VA incidents	Oracle Health incidents	All	Time the system was affected (hours: minutes)
Outage	1	6	7	7:09
Total	**172**	**654**	**826**	**1,909:26**

Source: VA OIG analysis of all major performance incident data maintained in Oracle Health's Lights On Network from October 24, 2020, through March 31, 2024.

Note: Some incidents reviewed were categorized as more than one incident type. For example, there were 10 incidents that were categorized as both performance degradation and incomplete functionality. The incidents ranged from one minute to 27 hours and seven minutes. These totals reflect only major performance incidents for which Oracle Health or VA was responsible, omitting any caused by other parties, such as DOD. The table does not include loss of redundancy incidents because these incidents represent no impact on the user.

Figure 1 shows the trends in incidents during this time frame. Due to issues with the EHR, VA stopped all planned EHR deployments in July 2022. An exception was the system deployed at the Captain James A. Lovell Federal Health Care Center in North Chicago, Illinois, on March 9, 2024. The trend of incidents turned down as of quarter three of fiscal year 2023. However, incidents continued after this March deployment.

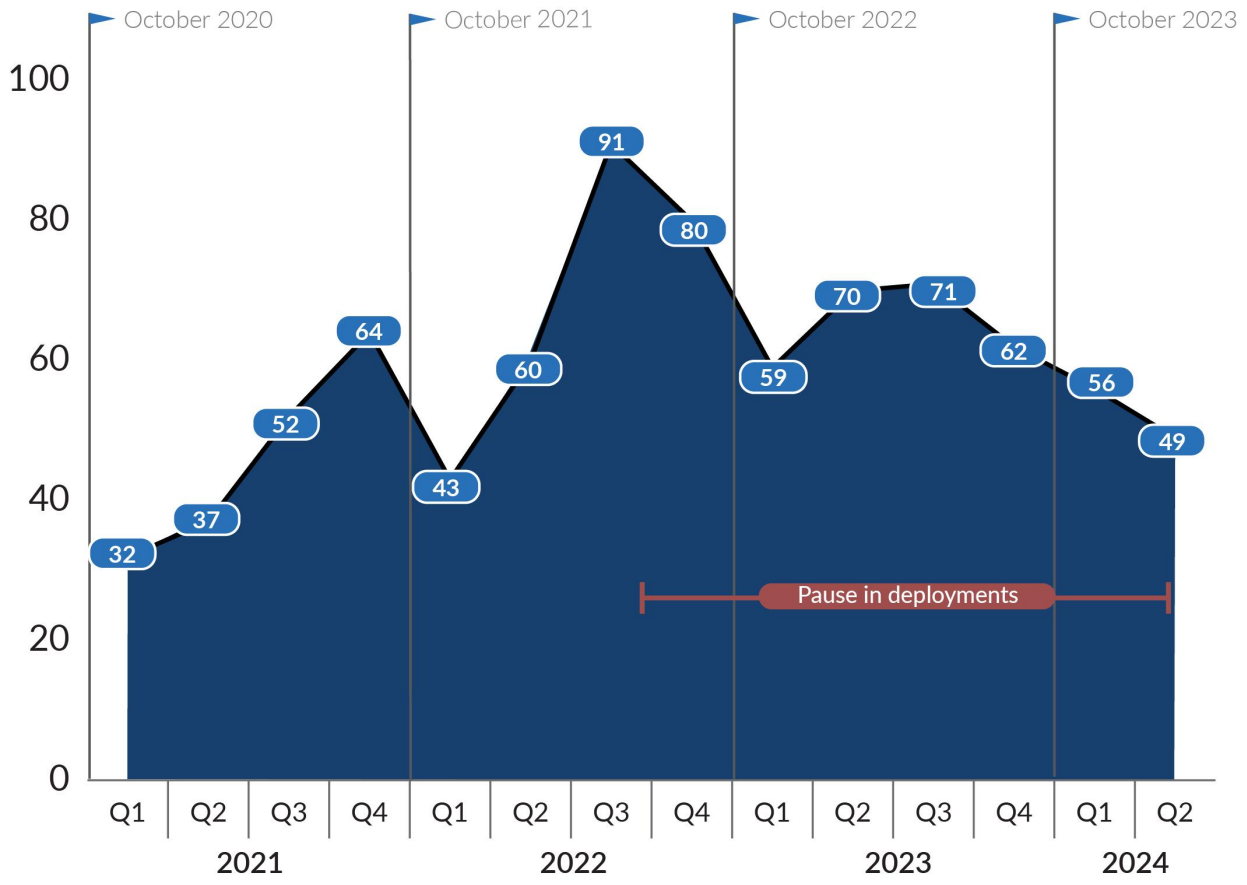

Figure 1. *Number of outages, performance degradations, and incomplete functionality incidents affecting the EHR system by fiscal quarter.*

Source: VA OIG analysis of all major performance incident data maintained in Oracle Health's Lights On Network from October 24, 2020, through March 31, 2024.

Note: These totals reflect only major performance incidents for which Oracle Health or VA was responsible, omitting any caused by other parties, such as DOD. The figure does not include loss of redundancy incidents because these incidents represent no impact on the user.

During a November 2023 congressional hearing, VA's assistant secretary for information and technology, who is also the chief information officer, said the system was still experiencing failures that affect users. He also said if system deployments had not been paused, the risk of incidents would have been greater. In addition, during the hearing, a congressman noted that about 58 percent of the employees surveyed said downtime was a problem during a two-week period.[46]

[46] *Hearing on Electronic Health Record Modernization Deep Dive: System Uptime*, *Before the Subcommittee on Technology Modernization, House Committee on Veterans' Affairs,* 118th Cong. (November 15, 2023).

Incident Priority

Incident priority is a function of impact and urgency.[47] Impact is measured by what (such as a system or application) or who (such as a VA administration) is affected, while urgency is defined by the amount of time the incident can be tolerated. All outages are considered critical, which is the highest priority. Performance degradation and incomplete functionality incidents could be assigned critical (priority 1) or high priority (priority 2), depending on impact and urgency. A critical-priority incident has an immediate impact on business functions and directly affects patient care, while a high-priority incident poses a risk to patient care.

Incidents can be identified by VA or Oracle Health IT specialists monitoring the system or by VA users who report them directly to the VA or Oracle Health service desk.[48] Once the incident is identified, service desk personnel assess the information gathered to prioritize the incident based on criteria established by VA and Oracle Health. Service desk personnel then involve the necessary VA and Oracle Health IT staff to address the incident.

Incident Control Functions

The audit team examined what controls were in place and how well they functioned to prevent, respond to, and mitigate major performance incidents that compromised the security and operational status of the EHR system. The team relied on standards formulated by the National Institute of Standards and Technology (NIST).[49] NIST standards set forth the core functions needed for major performance incidents: prevent, respond, and mitigate. These are industry standards, and the EHR contract states the contractor must comply with all applicable NIST standards, including NIST Special Publication 800-53.[50] Accordingly, the team considered VA and Oracle Health policy and procedures that implement those standards.

---

[47] VA OIT, *Major Incident Management Process Escalation and Notification for Service Outages*, September 6, 2019 (hereafter referred to as 2019 Major Incident Management Process); VA OIT, *Major Incident Management Process*, June 25, 2021 (hereafter referred to as 2021 Major Incident Management Process). The incident prioritization was first referenced in the EHR contract dated May 17, 2018, as incident descriptions and prioritization categories. The prioritization process was later incorporated under an EHR task order that established standard operating procedures in November 2021. Oracle Health, *Major Incident Management Standard Operating Procedures.* Before this task order, the EHR contract did not define the prioritization process.

[48] Incidents are logged as tickets through the VA and Oracle Health ticketing system. Tickets are submitted by users who encounter problems with the EHR system.

[49] Throughout this report, the audit team refers to NIST publications as information system control guidelines. These publications provide guidance on controls to a diverse audience including agency officials with oversight responsibilities and system owners.

[50] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, April 16, 2018; NIST Special Publication 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020; NIST Special Publication 800-12, rev. 1, *An Introduction to Information Security*, June 2017.

Prevent

According to NIST, an important part of incident prevention is configuration management. It provides assurance that a system has been configured to meet the needs and standards of an agency and that any changes to the system are reviewed and approved before implementation.[51] Another aspect of prevention is monitoring. Ongoing monitoring of controls ensures a system's performance within an acceptable level of risk despite any changes that occur.[52]

Respond

NIST standards stress the importance of a fast response to incidents. Therefore, it is important that parties collaborate on the development of incident response policy and procedures. NIST also recommends policies and procedures at the organization level. Procedures can be documented in plans that clearly establish roles and responsibilities. NIST standards note that simply restating controls does not constitute an organizational policy or procedure.[53]

The four steps in the response process are as follows:

- **Prioritization.** The party (VA or Oracle Health) that first became aware of the incident assesses the information reported and assigns a priority. Depending on its priority, an incident could be determined to be major.
- **Notification.** When a user experiences issues or when system monitoring identifies an incident, either VA or Oracle Health will be notified and will inform the other party.[54]
- **Resolution.** Using the bridge call to communicate status updates, key personnel resolve the incident and facilitate the complete restoration of service.
- **Post-resolution analysis.** The party (VA or Oracle Health) that caused the incident is responsible for analyzing and documenting incident details, including root cause.[55]

[51] NIST Special Publication 800-53. According to NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011, configuration management is defined as a collection of activities focused on establishing and maintaining the integrity of a system through controls of the processes for initializing, changing, and monitoring the system's configurations.

[52] NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011.

[53] NIST Special Publication 800-53; NIST Special Publication 800-128; NIST Special Publication 800-61, rev. 2, *Computer Security Incident Handling Guide*, August 2012.

[54] VA is responsible for notifying and updating all VA stakeholders, including any affected VA sites.

[55] Oracle Health, *Major Incident Management Standard Operating Procedures.*

Mitigate

Mitigation encompasses the actions taken to minimize the impact major performance incidents have on patient care. NIST guidance outlines the need for a contingency plan that details how an organization's mission and business processes will be sustained during and after a significant disruption. For VA, downtime procedures are actions staff should take to continue caring for veterans when the EHR system, or part of the system, is not available for use.[56]

[56] VA Handbook 6500.8, *Information System Contingency Planning*, April 6, 2011; NIST Special Publication 800-34, rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, updated April 23, 2021.

Results and Recommendations

Finding: VA Needs to Improve System Controls for Better Management of Major Performance Incidents

Hundreds of hours of partial or complete inaccessibility of the EHR system at the five sites where it first went live show VA lacks sufficient controls to prevent, respond to, and mitigate the impact of major incidents. For example, during one major incident that occurred on March 3, 2022, the system was disrupted for 27 hours and seven minutes because a system change halted operations at the Mann-Grandstaff VA Medical Center in Spokane, Washington. Subsequently, the medical center director reported that many patients needed to have their appointments rescheduled. The OIG found that VA and Oracle Health did not have adequate controls in place to prevent system changes from causing major incidents, respond to those incidents when they occurred, or mitigate their impact. The OIG also determined that while VA routinely tracks patient safety events related to the EHR system as a whole, there is no formal process to link reports of these events to specific major performance incidents.

Ultimately, limited EHR controls for handling major incidents originated in how the May 2018 contract was written. VA's EHR contract did not include specific terms that comprehensively required Oracle Health to take necessary actions to address major incidents, and performance metrics were difficult to find. In May 2023, about two and a half years after initial go-live and after a number of incidents had occurred at the sites that were live, VA added requirements that strengthened performance metrics such as increasing the monthly uptime goal for the EHR system. However, the OIG maintains that VA has the opportunity to further improve its management of major incidents and thereby reduce potential risk to patient safety. It is imperative that VA and Oracle Health take steps to better prevent, respond to, and mitigate the impact of major incidents so that VA can deliver the highest standards of patient care.

What the OIG Did

The audit scope included 360 major performance incidents—outages, performance degradations, and incomplete functionality—that occurred between October 24, 2020, and August 31, 2022. The number of these incidents is consolidated and presented in figure 2 by fiscal quarters spanning this period.[57] In total, these incidents affected the system for 892 hours and 39 minutes. The audit team obtained data on these incidents and selected a sample of 35 incidents from this

[57] For more on the scope and methodology and the sampling methodology, see appendix B.

period. The team notes that major performance incidents continue, as recently as March 2024 (figure 1).[58]

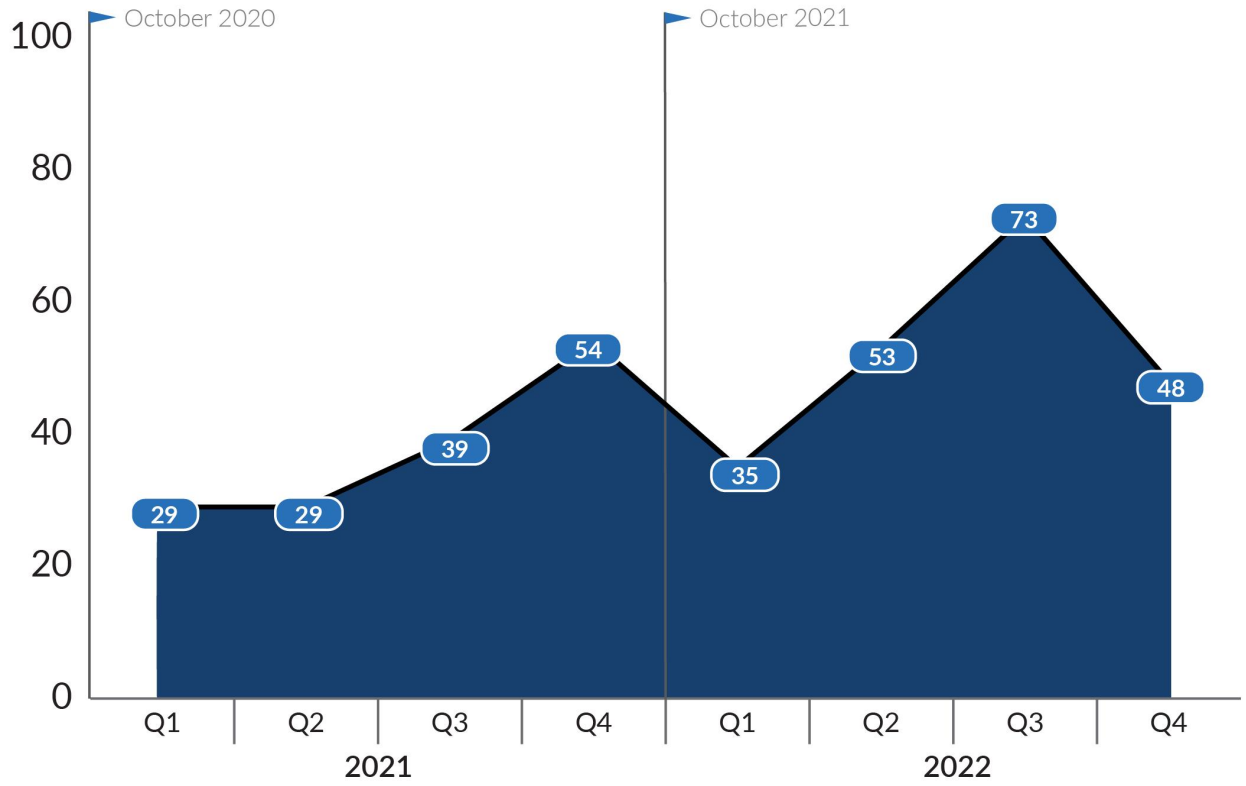

Figure 2. *Number of outages, performance degradations, and incomplete functionality incidents affecting the EHR system by fiscal quarter.*

Source: VA OIG analysis of major performance incident data maintained in Oracle Health's Lights On Network from October 24, 2020, through August 31, 2022.

Note: These totals reflect only major performance incidents for which Oracle Health or VA was responsible, omitting any caused by other parties, such as DOD. The figure does not include loss of redundancy incidents because these incidents represent no impact on the user.

VA was the responsible party for 91 of the incidents that the team reviewed; Oracle Health was the responsible party for 269. The team conducted testing on a sample of 35 incidents, one of which was selected judgmentally and 34 of which were selected statistically.[59] Of these 35 incidents, VA was responsible for seven and Oracle Health was responsible for 28. The team reviewed the details of these incidents and discussed them with VA and Oracle Health personnel to determine what measures were taken to address them. During the audit, the team updated its

[58] The team identified these incidents by excluding ones that were less than 30 minutes in duration. For more information on the team's methodology, see appendix B.

[59] The audit team judgmentally selected one incident it considered to be high risk—system disruptions that lasted 27 hours and seven minutes.

assessment of EHR controls by considering ongoing incidents, system developments, and contract modifications.

The following determinations support the OIG's finding:

- VA should improve system performance by strengthening prevention controls.
- VA should standardize response procedures and ensure complete and consistent incident reporting.
- VA finalized its national downtime procedure late and needs to effectively assess its backup options to mitigate the effects of major performance incidents.
- VA did not tailor the contract initially but has made some improvements.
- Informal reporting of major performance incidents may misrepresent patient safety risk.

Preventing Major Performance Incidents: VA Should Strengthen Controls to Improve System Performance

Federal agencies are required to implement controls that facilitate risk management and compliance with applicable federal laws, policies, and standards. These controls provide protective measures for systems, organizations, and users.[60] Changes to the system's configuration are vetted before implementation, and associated activities are monitored throughout the system development life cycle.[61] This ensures that changes to configuration management do not disrupt the system and impair VA's ability to provide care to veterans. It is important that these controls be implemented and effective to protect the system's availability.

Most of the 35 incidents reviewed by the audit team could be traced to two controls in the NIST guidance.[62] Weaknesses in these two controls—(1) configuration management and (2) assessment, authorization, and monitoring—accounted for 23 incidents and 80 hours and 20 minutes of system disruption, as shown in table 2.[63] The team also identified weaknesses in other controls, but none of them were as frequent or as long-lasting as these two.[64] Weaknesses

[60] NIST Special Publication 800-53.

[61] NIST Special Publication 800-53. NIST Special Publication 800-34 notes the system development life cycle encompasses the system's initiation, development and acquisition, implementation, operation, and maintenance, and ultimately its disposal.

[62] For more information on the team's methodology, see appendix B.

[63] For purposes of the audit, the team considered assessment, authorization, and monitoring to be continuous monitoring. During the audit, the team also identified weaknesses in other controls but decided not to report on them as none of them were significant in number or duration.

[64] These included weaknesses in controls relating to access, contingency planning, and system and services acquisition.

in the other controls accounted for a combined 12 incidents and 23 hours and 24 minutes of disruption.

Table 2. Top Two Control Weaknesses Associated with Major Performance Incidents

Controls	Number VA was responsible for	Number Oracle Health was responsible for	Time the system was affected (hours: minutes)
Configuration management	3	15	65:49
Assessment, authorization, and monitoring	0	5	14:31
Total	**3**	**20**	**80:20**

Source: VA OIG analysis of performance data for sampled major incidents maintained in Oracle Health's Lights On Network for the team's audit sample from October 24, 2020, through August 31, 2022.

Note: These major performance incidents reflect only those for which Oracle Health or VA was responsible, omitting any caused by other parties, such as DOD.

The following sections detail the control weaknesses in configuration management and continuous monitoring that were responsible for all the downtime and performance degradation, as well as some of the incomplete functionality, associated with the major incidents in the OIG's sample.

Inadequate Configuration Management Controls

The audit team found that problems with configuration management controls accounted for 18 incidents lasting 65 hours and 49 minutes. Configuration management controls protect system components such as hardware and software. Federal agencies must have effective general and business process application controls to achieve the appropriate confidentiality, integrity, and availability of information systems. These controls provide reasonable assurance that changes to information system resources are authorized, and systems are configured and operated securely and as intended. For example, the entity's configuration management should reasonably ensure that all changes to systems are fully tested and authorized. Without effective configuration management, users do not have adequate assurance that the system will perform as intended and to the extent needed to support their missions.[65] As the EHR system matures, new components may be identified, and some existing components may no longer be needed.

[65] NIST Special Publication 800-53; Government Accountability Office (GAO), *Federal Information System Controls Audit Manual*, GAO-09-232G, February 2009. The EHR contract performance work statement dated October 5, 2017, notes that for configuration management, the contractor (Oracle Health) must update or change the system to ensure its effective use.

In the following examples, the lack of configuration management controls caused major performance incidents.

Example 1

On March 14, 2022, Mann-Grandstaff VA Medical Center experienced incomplete functionality for 10 hours and four minutes. This incident occurred because of an update that inadvertently included a special character that corrupted the credentials of 872 users. Those users then could not access part of the EHR system. The audit team concluded that this incident could have been prevented if the update and instructions had been monitored. To resolve the incident, Oracle Health modified the update and manually resolved each affected user credential. EHRM Integration Office personnel stated that test data need to replicate the information in the system. To prevent future occurrences, Oracle Health should perform quality checks on updates before they are implemented.

Example 2

On August 24, 2022, Mann-Grandstaff VA Medical Center experienced incomplete functionality. VA was responsible for this incident, which was caused by a protection feature in an update to the Microsoft Edge browser. This prevented users from launching a dental application in the EHR system. Although the EHRM Integration Office personnel stated that this was a known issue, it nonetheless affected users for one hour and 27 minutes. To resolve the incident and prevent future occurrences, VA developed, tested, and deployed a fix to the new protection feature. The audit team concluded that this incident was the result of ineffective configuration management of updates.

Inadequate Assessment, Authorization, and Monitoring Controls

The audit team found that problems with assessment, authorization, and monitoring controls caused five of the 35 incidents reviewed and accounted for 14 hours and 31 minutes of disruption. The continuous monitoring controls determine the ongoing effectiveness of controls, changes in information systems and environments of operation, and the state of system availability.[66] The following examples detail major performance incidents caused by the lack of continuous monitoring controls.

[66] For ease of use in the control selection process, NIST organized the controls into 20 families, or groups, each containing controls related to the specific topic. Of the 20 control families organized in NIST Special Publication 800-53, the assessment, authorization, and monitoring family addresses continuous monitoring controls. Continuous monitoring at the system level facilitates ongoing awareness of the system's availability to support organizational risk management decisions.

Example 3

On May 10, 2022, all three sites where the EHR system had been deployed experienced incomplete functionality for five hours and four minutes. The incident occurred because of an expired certificate that disrupted some applications. The certificate in question was not listed in Oracle Health's monitoring tool that tracks certificates and therefore was not identified automatically and flagged for renewal before it expired. To resolve the incident, Oracle Health added this certificate to the monitoring tool. The audit team concluded that this incident was not detected promptly because Oracle Health did not effectively use the monitoring tool so that it could send notifications before certificates expired. An EHRM Integration Office official agreed that notifications should be sent before certificates expire. To prevent future occurrences, Oracle Health updated its associate notification protocols and expanded automatic audits of certificates that come due.

Example 4

Another incomplete functionality incident occurred on August 22, 2022, and affected all five sites for one hour and 38 minutes. Oracle Health explained its software errors created issues with data failing to populate in a separate application used by VA. Representatives from Oracle Health stated the company did not have monitoring in place at the time. After the incident, Oracle Health added monitoring that would alert it to the software errors more quickly.

All of the EHR downtime and most of the system disruption from the major incidents in the team's sample—about 77 percent of the hours—was attributable to problems with configuration management and continuous monitoring. By addressing these two control issues, VA could better prevent incidents.

Overreliance on Oracle Health for Oversight Information

As the agency responsible for modernizing the EHR, VA should implement policies and procedures to prevent or minimize damage and interruption to critical systems, but it may delegate the responsibility for tasks such as developing controls and monitoring them.[67] Although the contract specifies that Oracle Health takes responsibility for the technical system, including monitoring, VA is still ultimately responsible for maintaining situational awareness of the system to make effective, timely, and informed risk management decisions.[68]

[67] GAO, *Federal Information System Controls Audit Manual*; NIST Special Publication 800-53.

[68] NIST Special Publication 800-37, rev. 2, *Risk Management Framework for Information Systems and Organizations,* December 2018.

The audit team found that VA has limited access to the data Oracle Health uses to monitor the EHR system and the supporting environment. As Oracle Health is contractually required to perform monitoring of the EHR system, VA does not currently perform any continuous monitoring, according to the EHRM Integration Office deputy chief information officer, and it does not have access to all the underlying data that feed the Lights On dashboard system. VA personnel use the dashboard to view selected performance metrics.[69] VA relies on Oracle Health's incident reporting and does not have a formal procedure for verifying contractor performance metrics and associated credits according to the contract. Because of this, VA relies on Oracle Health's reporting to determine financial credits in line with the contract, resulting from major performance incidents caused by the contractor.[70]

To ensure that VA has access to the data it needs, VA plans to require Oracle Health to share the underlying information it has. Still, the assistant deputy chief information officer for the EHRM Integration Office told the audit team that before the exchange of real-time data can occur, additional processes must be completed, and VA is far from being able to perform proactive monitoring on its own. The same official did not give the OIG an estimate of when sharing could occur. As system deployments increase, continuous system monitoring is important to identify potential issues before they arise and ensure optimum EHR system performance across all deployed sites. Although the OIG recognizes that VA has contracted Oracle Health to monitor the EHR, performance incidents are ongoing, and it would be prudent for VA to enhance its oversight of the system. Therefore, VA needs to take action to assess and define the type of data and reporting it needs and how this information will be shared to determine how the system is performing.

To improve how VA prevents major incidents from occurring, the OIG's first recommendation is to assess its EHR incident data needs and contractually commit to real-time data sharing that will provide VA with greater awareness of system operations. The OIG's second recommendation is to develop a formal procedure for verifying contractor performance metrics and associated credits to ensure VA receives the remedies it is due under the contract.

Responding to Major Performance Incidents: VA Should Improve Its Controls

According to NIST, it is important for the parties involved in operating an information technology (IT) system to collaborate on developing incident response policy and procedures.[71]

[69] A dashboard is made up of images with titles and descriptions that present information in a visual format.

[70] Through the May 2018 contract, VA and Oracle Health agreed to the government's sole and exclusive remedy for Oracle Health's failure to meet the system availability commitment of 99.9 percent.

[71] NIST Special Publication 800-53.

These controls should be applied consistently across the organization, meaning enterprise-wide.[72] The audit team found that incident controls for the EHR program are ineffective because VA and Oracle Health each had their own incident response procedures. VA's were internal, while Oracle Health's were dictated by contract requirements. In both cases, notification time frames were not well defined. In addition, over time, VA's guidance for evaluating response time changed and became less rigorous. Due to the vagueness of these procedures, the team could not determine whether VA or Oracle Health complied with the stated time frames in most cases. As a result, VA does not have all the information needed to effectively manage responses.

VA and Oracle Health Lack Strong Procedures for Responding to Incidents

Incident response includes identifying, prioritizing, resolving, and reporting.[73] The following sections detail the inadequacies in those processes.

Approaches to Prioritizing

When a service disruption occurs, a single VA user or a group of VA users may report it to the VA or the Oracle Health service desk.[74] Service desk personnel review the incident to gather information and prioritize it based on its impact and urgency.[75]

For VA, the guidance regarding the prioritization process changed in 2021, from initiating major incident response procedures for all four priorities to initiating them only for critical and high. Since then, when a major incident is validated as priority 1 or 2, it is raised to the VA major incident management team for immediate notification and resolution. However, when validated by VA as priority 3 or 4, the incident is downgraded and resolved by their technology groups. As shown in figure 3, only incidents that are critical in both urgency and impact are assigned priority 1 in VA's incident priority matrix.

[72] GAO, *Federal Information System Controls Audit Manual*. The absence of entity-wide processes may be a root cause of weak or inconsistent controls.

[73] Oracle Health, *Major Incident Management Standard Operating Procedures.*

[74] Disruptions may also be identified through monitoring.

[75] VA OIT, 2019 Major Incident Management Process; VA OIT, 2021 Major Incident Management Process; Oracle Health, *Major Incident Management Standard Operating Procedures.*

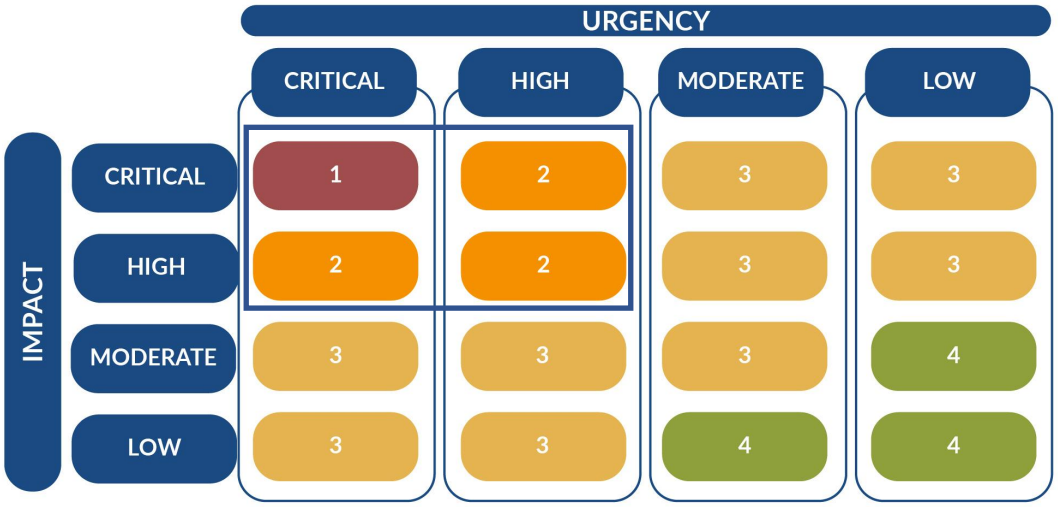

Figure 3. *VA's incident priority matrix.*

Source: VA, 2019 Major Incident Management Process, and VA, 2021 Major Incident Management Process.

Note: Colors and numbers in the figure represent incident priority as reported by VA. The rectangle around 1 and 2 in the figure above indicates the incidents considered major after the 2021 guidance update.

Oracle Health's prioritization matrix, which is part of the contract, includes more detail, as seen in figure 4.

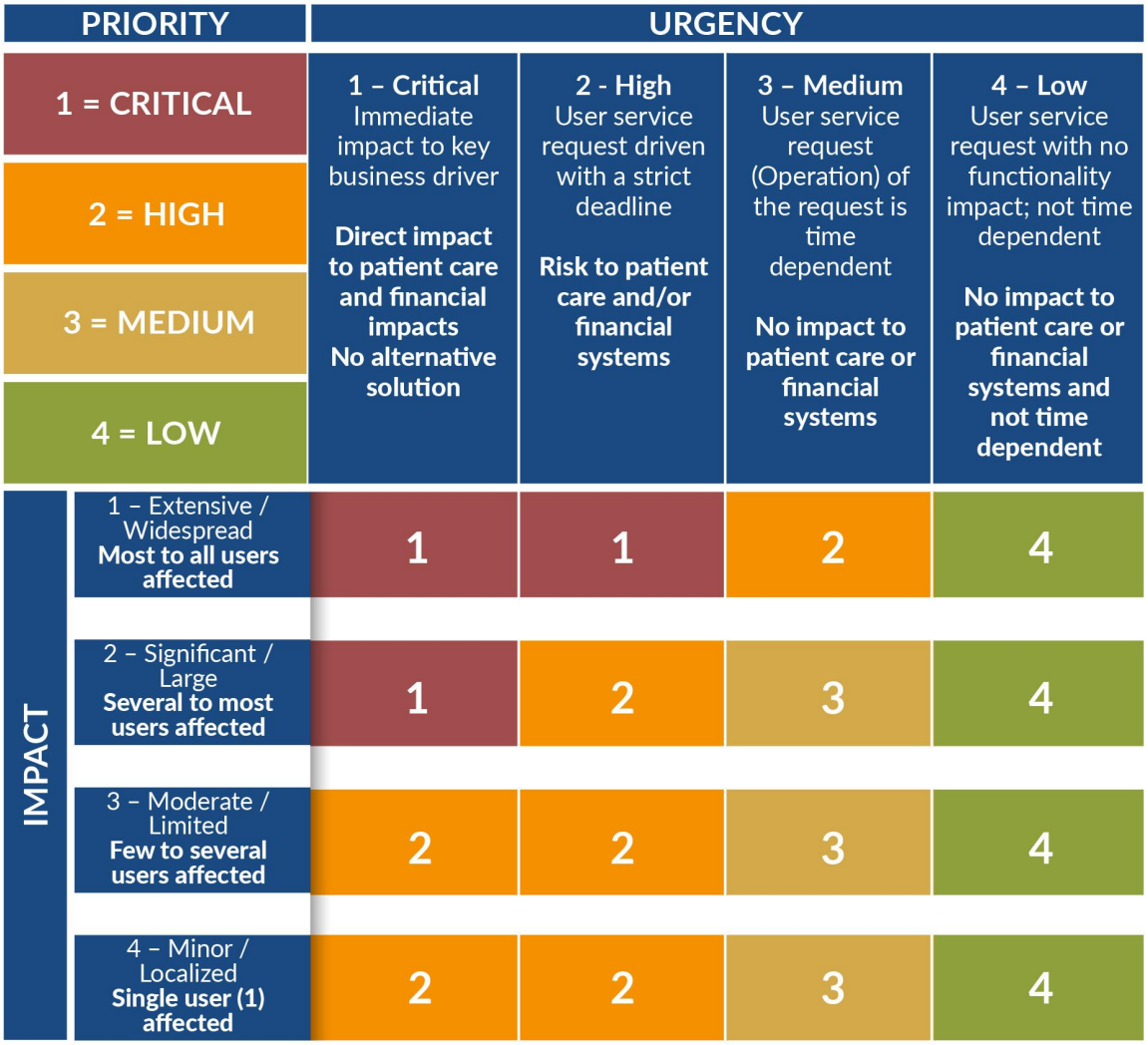

Figure 4. *Oracle Health's incident priority matrix.*

Source: Oracle Health, Major Incident Management Standard Operating Procedures*, November 18, 2021.*

Note: Colors and numbers in the figure represent incident priority as reported by Oracle Health.

The figure makes clear that incidents can qualify as priority 1 if they are critical or high in either urgency or impact.[76] That conflicts with VA's guidance, which designates priority 1 only to incidents with both critical impact and critical urgency. A senior manager for Oracle Health acknowledged VA's revised guidance does not align with Oracle Health's priority matrix and said its threshold for major incidents is lower. As a result, incidents are prioritized differently, and Oracle Health may respond to an incident considered either moderate or medium by VA.

[76] According to an EHR task order dated May 29, 2020, major incidents are defined as the subcategory of incidents having significant impact or urgency, requiring engagement and response processes beyond those of routine incidents. Major incident response is handled jointly by VA and the contractor.

The audit team determined Oracle Health prioritized for action all sampled incidents that it caused, while VA took priority action only on the critical or high incidents it caused. Without a consistent approach to prioritization, the same incident could be given a greater or lesser priority and responded to differently depending on the party involved.

Standards for Incident Notification and Resolution Times

VA lacked well-defined, consistent expectations for timely response in its guidance and has not imposed clear standards on Oracle Health in its contract. When an incident is prioritized as major, a twofold response process begins: (1) notification is sent to VA and Oracle Health IT specialists, who join a bridge call; and (2) the team works until the incident is resolved.[77] VA's guidance differs from Oracle Health's regarding how quickly these two steps must be completed, and in 2021, the process became less rigorous for VA. Therefore, the text that follows shows weaknesses in the guidance they follow when responding to an incident.

Between 2019 and 2021, VA guidance specified response times for initial notification and resolution for each of the four priorities (table 3).

Table 3. VA 2019 Guidance

Priority	Description	Notification time	Resolution time
1	Critical	30 minutes	24 hours
2	High	30 minutes	Two business days
3	Medium	12 hours	Four business days
4	Minimal	24 hours	10 business days

Source: VA OIT, 2019 Major Incident Management Process.

In 2021, however, VA revised its standards in guidance to specify *average* notification and resolution times and apply them only to critical- and high-priority incidents (table 4).[78] The times appear more restrictive, but they do not give the frequency with which to evaluate incidents—for example, whether the average is calculated monthly, quarterly, or annually. OIT leaders reported to the team that OIT considers the frequency to be monthly, which effectively loosens the timeliness standards for VA.[79]

[77] VA OIT, 2019 Major Incident Management Process; VA OIT, 2021 Major Incident Management Process; Oracle Health, *Major Incident Management Standard Operating Procedures*. Response time includes initial notification to either VA or Oracle Health information technology (IT) specialists and resolution when service is restored.

[78] VA OIT, 2021 Major Incident Management Process. In October 2023, OIT issued new major incident management guidance. The notification and resolution procedures remain the same.

[79] When times are listed per critical incident, as in 2019, users have some assurance that resolution will occur within 24 hours; when times are averages, as shown in the 2021 guidance, resolution of a given incident may occur within less or more than eight hours, and users do not know how much less or more. If all incidents in a month are included, individual times could be significantly under or over eight hours and still average to eight hours.

Table 4. VA 2021 Guidance

Priority	Description	Average notification time	Average resolution time
1	Critical	≤ 20 minutes	< 8 hours
2	High	≤ 20 minutes	< 24 hours

Source: VA OIT, 2021 Major Incident Management Process.

In contrast, for the 28 Oracle Health–caused incidents the team reviewed, no clear notification time was specified in the contract. The contract refers to time for notification and states only that Oracle Health in consultation with VA should act "immediately."[80] When asked about this, EHRM Integration Office's chief architect reported the office did not have a formal definition but focused on the time to resolution. A senior Oracle Health manager said the goal is to start the bridge call as soon as the priority is confirmed. For resolution, the contract states that Oracle Health is to resolve incident tickets within the times specified in table 5.[81]

Table 5. Oracle Health's Contract Requirements

Priority	Percent of tickets resolved or mitigated	Resolved or mitigated within	VA time for confirming resolution cannot exceed
Critical	100	Five hours	24 hours
High	90	16 hours	64 hours
Moderate	80	Four business days	60 calendar days
Minor	80	Six business days	60 calendar days

Source: VA contract no. 36C10B18D5000.

Note: A ticket is considered resolved when Oracle Health places it in a status for the client to approve or confirm the issue is addressed. Once VA confirms that the ticket has been completely resolved, Oracle Health is responsible for closing the ticket.

Considering how VA and Oracle Health evaluate notification and resolution of major incidents, VA will have difficulty determining whether it and the contractor have adequately responded.

Response Time Performance

Because of the inconsistencies and lack of clarity outlined above, the audit team could not determine whether VA or Oracle Health responded to most incidents reviewed in a timely manner.

[80] Oracle Health, *Major Incident Management Standard Operating Procedures.*

[81] Before September 2023, there was no financial credit for not resolving incidents within the stated time frames.

For VA, the shift from 2019 to 2021 guidance made its standards more ambiguous and less rigorous. According to an OIT director, OIT made this change because it was reducing its target notification times. With the change in guidance, the audit team could not evaluate the timeliness of response for all seven of the incidents VA caused.[82] The seven incidents consisted of two critical- and three high-priority incidents. The remaining two, assigned medium priority, were not reported on by VA under its updated guidance. The team was able to evaluate only one critical incident, which occurred in 2020 before VA adopted the less rigorous standards. For that incident, notification and resolution occurred within the standard times.[83] For the remaining four incidents that VA reported on, the standards in VA's 2021 guidance had shifted to averages, making comparison impossible without knowing the frequency of the averages.[84] Nonetheless, the team calculated that for these four incidents, VA took between two minutes and 44 minutes to notify VA major incident management staff and between one hour and 13 minutes and 211 hours and 40 minutes (nearly nine days) to resolve them.

The audit team determined that, besides shifting the standards in guidance, VA OIT did not enforce meeting them. According to an OIT director discussing the 2021 process document, the recovery times were held over from the 2019 version, were aspirational, and should have been removed. He said there are simply too many variables affecting restoration times, most beyond the control of the major incident management process. "Bottom line," he said, "we do our best to facilitate the repair of services as quickly as possible."

When it came to Oracle Health, since VA did not establish a clear standard for notification for its contractor, the audit team could not determine whether the times were appropriate for the incidents reviewed.[85] Still, the team calculated that notifications from Oracle Health for the 28 incidents ranged from five minutes to two hours and 20 minutes.

Similarly, in evaluating the times for resolution, the team could not determine whether Oracle Health met requirements for all 28 incidents. Oracle Health reported its incidents monthly based on the time it took to resolve them, without indicating their priority.[86] This prevents VA from easily determining whether Oracle Health met contract requirements for all incidents.

Also complicating the OIG's analysis is that the priority level of an incident can be elevated as more information about its impact is discovered.[87] The audit team cross-checked the 28 incidents

[82] Appendix B includes information on the audit team's sample.

[83] VA OIT, 2019 Major Incident Management Process. At the time, the initial incident response goal was 30 minutes, while the resolution goal was under 24 hours. To determine the timeliness of the notification and resolution of this incident, the audit team combined the time taken for initial email notification to VA and the incident's duration.

[84] VA OIT, 2019 Major Incident Management Process; VA OIT, 2021 Major Incident Management Process.

[85] VA contract 36C10B18D5000.

[86] Four of the 28 incidents had only a date and did not include a specific time.

[87] Six incidents included multiple priorities.

and was able to determine that 20 (which remained the same priority throughout the response process) were resolved as required.[88] In the following example, a major performance incident that was initially prioritized as low eventually rose to critical and caused 27 hours and seven minutes of system outage and incomplete functionality.[89]

Example 5

On March 3, 2022, an incident ticket was entered after patient charts at the Mann-Grandstaff VA Medical Center were found to include another patient's sensitive health information, including notes and lab results. Oracle Health assigned the ticket a low priority.[90] The same day, three more tickets regarding incorrect patient names and demographics appearing in the system were submitted from the facility and another facility. According to VA, Oracle Health took 21 hours and 29 minutes to raise the priority.[91] Oracle Health representatives said the incident, which resulted from a system change, was not escalated until the next morning because it did not come in as a high-priority ticket. After this event, the Mann-Grandstaff medical center director told facility personnel to stop using the EHR system and consider all electronic patient data corrupted or inaccurate. He also noted many veterans' appointments had to be rescheduled.

Without adequate procedures for prioritization, notification, and resolution, VA cannot manage EHR incident response effectively.

VA Did Not Ensure Post-resolution Reporting Was Complete and Consistent

After resolution, VA and Oracle Health did not consistently report key analysis to minimize the likelihood of incidents continuing. Because the two entities had different reporting requirements during the audit period, the text below addresses them separately.[92]

[88] Two of the incidents that remained one priority throughout the response process included only a date.

[89] Incidents can also involve numerous tickets, and response times are not always cumulative.

[90] This was the priority according to information in ServiceNow, VA's system for tracking incident tickets. The priority of the incident conflicts with information in Oracle Health's ticketing system, where it was assigned as medium. Tickets are submitted by users who encounter problems with the EHR system.

[91] The audit team found the duration of this incident in ServiceNow. The amount of time conflicts with Oracle Health information related to this incident, which showed the incident's priority was escalated in about 40 minutes.

[92] VA OIT, 2019 Major Incident Management Process; VA OIT, 2021 Major Incident Management Process; Oracle Health, *Major Incident Management Standard Operating Procedures.*

VA

After critical and high-priority incidents, VA guidance calls for a report that includes impact, duration, root cause, and corresponding recommendations.[93] For five of the seven VA-caused incidents, the root cause sections of the reports were incomplete.[94] VA included a reason-for-outage statement but did not always include details on root cause, monitoring weaknesses, work-arounds, and individuals involved in root cause analysis.[95]

Oracle Health

For the 28 incidents it caused, Oracle Health provided VA 20 incomplete major incident reports.[96] As part of the reporting process, an Oracle Health team creates a major incident report for every incident they own for VA's record. This report contains information including event overview, total incident duration, summary of cause, total incident duration, and irreversible correction and preventative actions.[97] The audit team determined that the reports received were missing some of these elements. Of the 28 Oracle Health–caused incidents, five had reports that did not include or lacked information on actions taken to prevent the incidents. Three reports included a working theory on cause, which according to EHRM Integration Office leaders is not necessarily sufficient as root cause for incidents. This office's assistant deputy chief information officer told the team that incident reports are used to validate incidents and should acknowledge whether details are unknown.

Oracle Health staff explained to the audit team that in August 2022 the contractor implemented a process for reporting on critical and high-priority performance incidents it is responsible for. This process includes conducting root cause investigations and documenting actions taken to prevent future occurrences. However, because the team determined that the process was not contractually required and internal to Oracle Health, the team did not evaluate it.

Incomplete and inconsistent reporting on major incidents limits VA's ability to address them. Without identifying the root cause of an incident, VA or Oracle Health would not know what steps to take to resolve it. Further, documenting the causes and resolutions of an incident would be useful if a similar incident occurs.

---

[93] VA OIT, *Problem Management Practice, Investigating and remediating the root cause of Major Incidents to prevent disruptions before they happen*, November 20, 2019.

[94] According to an OIT associate director, the information missing from these reports was maintained in the incident record in ServiceNow. The other two incidents did not merit reports because they were of medium priority.

[95] A root cause statement is a description recorded once the underlying cause of the problem is determined.

[96] Incident reports were referenced in EHR contract documentation. For example, the EHR contract's performance work statement requires the contractor to identify; assess the impact of and report, track, escalate, notify specialists and users about; and resolve incidents that occur within the EHR system. An incident is deemed to be caused by Oracle Health when the incident is found by or reported to it.

[97] Oracle Health, *Major Incident Management Standard Operating Procedures.*

Planning Deficiencies Weakened Response Controls

Ineffective incident response procedures resulted from not having an entity-wide response plan.[98] VA created a response plan, which did not take effect until 2020, but did not apply it to all parties.[99] According to an OIT director, Oracle Health was included in this plan's development, but contractor representatives reported to the team that they were unaware of the plan. The response plan was reissued in 2023.[100] However, the same director reported that Oracle Health was not directly involved in creating that version. Although the plan stated that each party had the same indicators for notification and resolution, it allowed the two to maintain their own processes regarding prioritization. Further, the plan cover page had a disclaimer that those involved in running the EHR system did not have to follow it.

Moreover, VA did not hold Oracle Health accountable for post-resolution reporting. Oracle Health is required to identify a root cause, perform an analysis of every major incident, and issue a report to VA for every major incident it owns.[101] VA contracting personnel confirmed this to the team. However, EHRM Integration Office officials reported that the contract does not explicitly require Oracle Health to formally provide the results to VA as a deliverable.[102] VA was slow to address weaknesses in Oracle Health's incident reporting, with EHRM Integration Office officials acknowledging in July 2023 that this reporting was still insufficient.[103] As a result of poor planning and not taking a more active role in contracting for the EHR system, VA did not establish effective controls for responding to major incidents. Therefore, the controls cannot be relied on to accurately assess Oracle Health's performance.

To improve VA's response to major incidents when they do occur, the OIG's third recommendation is for VA to update how it prioritizes major performance incidents to ensure that notification and resolution occur in a consistent manner. Recommendation 4 is to develop effective metrics that consistently capture results for all major performance incidents, regardless of the owner, and enforce them. In the fifth recommendation, the OIG recommends that VA identify the information needed in post-resolution reports and require the contractor to consistently collect, verify, and report that information as a contract deliverable.

---

[98] GAO, *Federal Information System Controls Audit Manual*. The absence of entity-wide processes may be a root cause of weak or inconsistent controls.

[99] Federal Electronic Health Record Inter-Agency Operations Working Group, Major Incident Management, *Federal Electronic Health Record*, July 2020.

[100] Federal Electronic Health Record Inter-Agency Operations Working Group, Federal Major Incident Management, *Federal Electronic Health Record*, August 2023.

[101] VA contract 36C10B18D5000. The contract specifies that Oracle Health is required to identify incident root cause and corrective or preventative action.

[102] VA contract 36C10B18D5000.

[103] The EHR system contract is discussed more in the section of the report titled "VA Did Not Tailor Contract Initially but Has Made Some Improvements."

Mitigation of Major Performance Incidents: Implementation of Effective Controls Was Delayed

When the EHR system is unavailable, there can be immediate risk to patient care because the system is the primary means by which clinicians access information necessary to treat patients and create or amend patient records. To mitigate downtime, federal agencies are directed to have an information system contingency plan.[104] Accordingly, VA requires its offices to take actions such as identifying and assessing the risk to operations, developing and implementing strategies to mitigate this risk, and regularly training staff on these strategies.[105]

The audit team focused on the steps VA has taken to mitigate the risk to patient safety during EHR downtime. The team found that while VA had initiated two key strategies to continue patient care when the system is unavailable—procedures to follow during system downtime and backup systems—it did not sign the procedures until May 2024, over three and a half years after launching the EHR system, and it was still implementing a strategy for its backup systems.[106] According to Veterans Health Administration (VHA) personnel involved with developing VA's strategies, this delay happened because they did not assess the adequacy of contingency actions until after a significant number of incidents occurred. Furthermore, without having effective mitigation strategies, VA was unable to thoroughly train clinicians on them as required.[107]

National Downtime Procedure Finalized Late

In May 2024, VA finalized a national downtime procedure outlining the actions clinicians should take in the event the system is unavailable.[108] Although this is an important step, more needs to be done. Specifically, procedures must be implemented and training provided. Ensuring the standardization and awareness of approved procedures is an important control that promotes

[104] Office of Management and Budget (OMB), "Federal Agency Responsibilities for Maintaining Records About Individuals," app. I in OMB Circular A-130; NIST Special Publication 800-34. In addition, VA requires information system contingency planning that meets NIST standards.

[105] VA Handbook 6500.8 requires contingency planning for information systems. VA must have contingency plans in place to execute when system incidents occur. The contract specifies that Oracle Health must comply with this handbook.

[106] The audit team did not evaluate the effectiveness of the procedure because there was insufficient time within the audit to reasonably do so.

[107] VA Handbook 6500.8.

[108] Veterans Health Administration (VHA), "Oracle Health Cerner Millenium Electronic Health Record Downtime SOP" (standard operating procedure), VHA-ONS-NUR-23-01, November 14, 2023.

patient safety.[109] Without these additional measures, VHA facilities risk staff confusion about what to do and delays that would negatively affect patient care.

Before the procedures were finalized, the five VA medical centers that had gone live with the EHR each had to implement their own procedures. Of the five, the OIG team received draft downtime procedures from three and final downtime procedures from two during the audit.[110] The following examples illustrate the inefficiencies facility personnel experienced because they did not have consolidated, approved procedures.

The audit team found that the downtime procedures established at the Mann-Grandstaff Medical Center directed staff to scan forms created during system unavailability, while the procedures at the Chalmers P. Wylie Veterans Outpatient Clinic in Columbus, Ohio, required staff to manually enter specific information (such as vital signs, clinical assessments, and medications administered and prescribed) into the EHR system when it came back online. In addition, according to the chief of health information management at the medical center in Roseburg, Oregon, each department was responsible for tailoring procedures in its area of care. Furthermore, the chief of clinical operations at Columbus provided the team 10 forms for carrying out downtime procedures—including charting, physician orders, and medication administration. Different local procedures could complicate how clinicians document patient records and make decisions about a patient's treatment.

The audit team notes that finalizing national downtime procedures is just the first step toward ensuring the standardization of actions clinicians take when the system is unavailable. Procedures are generally considered guidance that should be followed by employees but are not mandatory; however, VHA leaders agreed that consistent downtime actions should be required of clinicians and stated there is a plan to make actions mandatory once more sites deploy the EHR.

As with any change, effective implementation requires training. In May 2024, before the finalization of the procedures, VHA personnel reported that they would be scheduling a presentation for VHA field leadership at all the EHR live sites and setting deadlines for implementation of the procedures following publication. For future EHR sites, they would ask

[109] The Institute for Safe Medicine Practices noted that without an organized downtime plan, facilities tend to respond to unanticipated EHR downtime in silos, with poor interdepartmental communication and collaboration. "Emergency Preparedness: Be Ready for Unanticipated Electronic Health Record (EHR) Downtime" (web page), Institute for Safe Medication Practices, August 25, 2022, accessed June 8, 2023, https://www.ismp.org/resources/emergency-preparedness-be-ready-unanticipated-electronic-health-record-ehr-downtime.

[110] The three that provided draft downtime policies were Jonathan M. Wainwright Memorial VA Medical Center in Walla Walla, Washington; Roseburg VA Medical Center in Roseburg, Oregon; and VA Southern Oregon Rehabilitation Center and Clinics in White City, Oregon. The Mann-Grandstaff VA Medical Center in Spokane, Washington, and the Chalmers P. Wylie Veterans Outpatient Clinic in Columbus, Ohio, provided final downtime procedures. Procedures were provided between April 11, 2022, and January 9, 2023.

for an implementation plan for the procedures at least nine months before system initiation. The OIG believes that VHA should continue its plans to train clinicians on the procedures. Medical studies have shown the importance of having consistency during a downtime event to ensure patient safety. A study from the National Library of Medicine showed downtime introduces unique and significant demands on hospital staff and resources; therefore, to manage the allocation of the resources as well as maintain safe and effective patient care, better and more detailed downtime contingency plans with a focus on communications, resource allocation, and training are necessary.[111] To address the ongoing demand for healthcare workers, VA continues to bring on new staff throughout its facilities, making training on national downtime procedures all the more important.[112]

Lack of Effective Backup Systems

The second of two key actions to mitigate the risk of the EHR system experiencing downtime is providing clinicians with a backup system that would allow them read-only access to important patient record information.[113] Two primary downtime viewer (DTV) options were available to clinicians when the EHR system was unavailable, but neither option was suitable for all types of VA facilities or during complete system outages. The first option for clinicians was the Joint Longitudinal Viewer (JLV), which VA and DOD have shared since 2014 for viewing records.[114] The second option was one Oracle Health provided to access EHR medical records during periods of downtime through a read-only system known as the 724Access DTV.[115] Both systems have limitations that vary based on the type of facility and the significance of the incident.

Turning first to JLV, when the EHR experiences an outage, JLV will not connect with the system. This means clinicians at all types of facilities are unable to use JLV to access any new

[111] Ethan Larsen, et al., "Continuing Patient Care during Electronic Health Record Downtime – PMC" (web page), National Institutes of Health, July 10, 2019, accessed June 8, 2023, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6620179/. Further, a study from the Agency of Healthcare Research and Quality emphasized that the lack of downtime procedures may delay care, increase medical errors, and disrupt communication. "Evidence-based Contingency Planning for Electronic Health Record Downtime" (web page), Agency for Healthcare Research and Quality, accessed December 12, 2023, https://digital.ahrq.gov/ahrq-funded-projects/evidence-based-contingency-planning-electronic-health-record-downtime.

[112] In July 2023, VHA announced its hiring and onboarding process improvement plan, stating that VA needs to hire more than 50,000 employees per year over the next five years to keep pace with expanding needs for veterans' care and to maintain a healthy, vibrant workforce.

[113] According to VHA's "Oracle Health Cerner Millennium Electronic Health Record Downtime SOP," downtime is any period during which EHR resources are unavailable to users, including service degradation impacting the clinician's ability to document patient care.

[114] JLV is a web-based application that provides read-only medical data from DOD, VA, and community partners in a common data viewer.

[115] The EHR contract performance work statement dated October 5, 2017, notes that the contractor must provide a 724 DTV read-only system to replace each of the over 170 instances of original EHR read-only installations. This replacement must be implemented as part of each site deployment. The DTV provided to VA by Oracle Health was available as part of the EHR's commercial product suite and was not customized for VA.

EHR patient record. Other limitations were reported by clinicians to the team during site visits, existing outside the use of JLV in an outage. Some clinicians at the five sites stated JLV is not user-friendly, indicating that navigation was slow and image searches were difficult.

The Oracle Health DTV also has a limitation in that it does not show records created farther back than seven days from the date a clinician is attempting to view a patient's record. This is particularly limiting at outpatient facilities, where a patient may not have been seen within the last seven days.[116] The team confirmed issues with the suitability of the DTV during site visits. Staff at all five facilities stated that viewers are ill-suited to facilities that provide predominantly outpatient care, as these five facilities do, because the DTV only displays limited patient information, most not useful to clinicians.

The team observed another potential issue with the DTV when an informatics officer in Columbus tried to log in to demonstrate the viewer and was unable to do so. The officer stated this likely was because the DTV had not been updated and informed the team that DTVs need routine, manual updates. The same officer reported because updates are time-consuming and the viewers are of limited use to the facility, the amount of work is not worth the benefit. According to VHA personnel involved with using the DTV, Columbus personnel do not use it, as the viewer is for downtime in inpatient settings and does not meet the facility's downtime clinical information needs.

The audit team concluded that the limitations of JLV and DTV during an outage affect VHA outpatient sites the most. These limitations are significant considering that there are over 1,000 of these types of facilities, making up about 90 percent of VA clinics nationwide.[117] If the EHR system is offline, medical facility personnel reported they may tell veterans, particularly at a lab, that there may be a delay, so the veterans can choose to stay or go. Medical center personnel also reported taking notes during downtime either by pen and paper or typing it offline on their computers only to later enter it in the system or scan it, which may be time consuming. There is also a potential for patient information to be lost and the likelihood for patients not to recall key parts of their record, which could jeopardize their care.

EHRM Integration Office leaders have recognized the need for a solution that is suitable when the system is unavailable at all facilities, and the office is working on deploying another system intended to be used at outpatient facilities. This system was developed by Oracle Health to mitigate risk to patient safety and is intended to make 24 months of data available for all patients

[116] In this instance, outpatient facilities may use JLV to view patient records as long as the EHR system is not experiencing an outage.

[117] According to VHA, its healthcare system provides care through about 1,300 facilities, including about 170 medical centers and about 1,100 outpatient sites.

with scheduled appointments.[118] However, as of May 2024, VA and Oracle Health were still working on the implementation timeline for this solution.

No Effective Assessment of Downtime Viewer Needs

During EHR contracting, VA did not consider other system backup options besides the viewer provided by Oracle Health. VA's EHRM Integration Office; VA's Office of Acquisition, Logistics, and Construction; and VHA officials reported that there was no consideration of other options. As of May 2024, over three years after launching the EHR system, VA was still working on acquiring another option for a DTV. Although the OIG recognizes this effort, VA did not have a full backup solution for its outpatient activities because it had not assessed the risks associated with using the DTVs. Meanwhile, VA is maintaining JLV for clinicians' use during downtime to view certain patient information, such as appointments, consults, and medications.

Having multiple systems available to clinicians during downtime is not ideal. According to federal guidance, fragmentation, overlap, and duplication can affect program implementation, outcomes and impact, and cost-effectiveness.[119] In the case of EHR DTVs, having different options may cause confusion among users about which to use and when. In addition, it will increase the training burden on staff and raise maintenance costs. Without comprehensive actions and suitable systems to facilitate clinical care during downtime, VA will run the risk of disruptions in patient care.

To better mitigate the harm caused by EHR system outages, the OIG's sixth recommendation is for VA to ensure that all clinicians are familiar with the national downtime procedures. VA should also identify the appropriate backup system and develop a training strategy to make certain that clinicians can use the system during downtime, as indicated in the OIG's seventh recommendation.

VA Did Not Tailor the Contract Initially but Has Made Some Improvements

Many of the issues identified in this report originate with the May 2018 contract, which did not include terms that comprehensively required Oracle Health to take necessary actions to address major incidents. For example, although the May 2018 contract referenced a DTV, the system provided by the contractor was not adequate to meet VA's needs. Separate from these provisions, in August 2023, VA contracted with Oracle Health to obtain a viewer to provide an additional tool for clinicians when the system is unavailable.[120]

---

[118] VHA, *EHRM Sprint Report*, version 1, March 2023.

[119] GAO, *Fragmentation, Overlap, and Duplication: An Evaluation and Management Guide*, GAO-15-49SP, April 14, 2015.

[120] As of May 2024, VA had yet to implement the additional tool.

In May 2023, VA exercised its first option for the contract and added requirements that relate to some of the issues in this report. VA also improved its contract terms and instituted five one-year option periods as opposed to one five-year option period. The EHRM Integration Office's chief of staff stated that this approach allows for the annual review of its progress and renegotiations with Oracle Health as needed. The following requirements are either new—VA did not include them in the initial contract—or strengthened.[121] These changes are relevant to the findings presented in this report, as they refer to incident-free time, outage-free time, and ticket management, but they address the audit work generally and are not focused on refining the process of managing major incidents.[122] These requirements include the following:

- **New.** The incident-free time metric outlines monthly target percentages for the system to be free of incidents other than outages. This metric targets the occurrence of performance degradation and incomplete functionality incidents. Before the May 2023 modification, the only incident-related metric in the contract was related to outages.
- **Strengthened.** VA increased the target monthly system uptime by 0.05 percent. This took the target uptime from 99.9 percent to 99.95 percent.[123]
- **Strengthened.** Although a trouble ticket resolution metric was included in the initial contract, requirements for financial credits were included for the first time in May 2023. Under these terms, VA will receive a credit from Oracle Health when a percentage of tickets are not resolved within a certain time. The time varies depending on how severe the ticket is.

The audit team did not evaluate the effectiveness of these changes partly because some of them did not take full effect until months after the May 2023 contract modification; thus, there was insufficient time in the audit to reasonably do so.[124] Also, despite these changes, major performance incidents continued. Between the signing of this agreement and March 2024, there were 193 major performance incidents that ranged in duration from one minute to 18 hours and 22 minutes.[125] As discussed in the next section, VA could consider building other requirements

[121] VA contract 36C10B18D5000, modification no. P00002, May 16, 2023. These metrics bind the contractor throughout the life of the contract, including any task orders that may extend beyond the contract's ordering period, and identify the respective amounts to which the contractor will be liable to the government, in the form of an invoice credit (offset) for every metric the contractor fails to meet.

[122] Incorporated into the contract in May 2023, the incident-free time metric is a percentage of time the system was free of unplanned events such as incomplete functionality and performance degradation, excluding outages.

[123] Uptime is the time the system is not experiencing an outage. In the May 2023 contract modification, the uptime metric name was changed to outage-free time.

[124] For example, one change involved metrics for tickets and associated financial credits, which were effective in September 2023.

[125] This assessment includes all major performance incidents considered during the audit.

into the contract and enhancing oversight controls, which may help alleviate these control weaknesses.

Opportunities to Improve Information Sharing

In April 2023, VA announced an EHRM program reset and took steps to improve the EHR system. Some of VA's planned work with Oracle Health during the reset would include improving system performance, such as addressing uptime and incident-free time and updating the incident management resolution process. However, continued improvements are still needed to enhance its management of major incidents. An EHRM Integration Office leader mentioned that he would like to change some contract terms, including requiring Oracle Health to provide real-time system data and enhancing incident reporting requirements to include corrective and preventive actions.

Specifically, based on the work conducted during the audit, the OIG determined that the following information could enhance VA oversight and help address existing EHR control weaknesses:

- Real-time data from Oracle Health that provides information on the performance of the EHR system would enable quicker oversight actions by VA.
- Detailed reporting on incidents the contractor is responsible for would help address EHR control weaknesses—specifically, a requirement for Oracle Health to provide reports on all major incidents that include a root cause analysis and distinct actions to prevent incidents from occurring.

VA's Initial Contract Oversight Was Limited

The audit team noted that VA has been relatively slow to improve the EHR contract.[126] VA's EHR contract did not include the controls needed.[127] The EHRM Integration Office knew some revisions to the contract language were needed well before the May 2023 contract modification. For example, the deputy chief information officer told the OIG team the contract terms were very broad. The metrics that measure contractor performance were difficult to find in the contract. In addition, the deputy stated the contractor would only describe incidents for VA and not provide the root cause. As previously noted, the team found that no definition of "major incidents" and no guidance for prioritizing them were included in the contract until 2020. In addition, contract language did not clearly define what "immediately" meant for response time.

[126] VA reviewed, acknowledged, and accepted all the DOD EHR functional requirements as its base set of requirements.

[127] For example, VA's EHR contract only established an uptime target percentage and associated financial credits.

According to the deputy chief information officer, the contractor was not meeting contract requirements. Oracle Health failed to meet the system uptime goal in November 2020, July 2021, November and December 2021, and March 2022. Although VA received a credit for those months, it did not issue any formal notice of concern to the contractor on system performance until April 2022, nearly 18 months after the first site went live with the EHR.[128] The delay in issuing a letter of concern illustrates VA's conservative approach to addressing major incidents. While incorporating the additional language in the May 2023 modification was a positive step, this occurred about two and a half years after initial go-live and after a significant number of incidents had occurred at the sites that were live.

The OIG maintains that VA should improve its processes to more quickly identify when action should be taken to enhance controls and reduce major performance incidents. For example, VA has a dashboard for each site before go-live that provides limited real-time system performance information. This dashboard is used to monitor system performance before and during the site's go-live event. However, VA could consider using this dashboard beyond go-live events to monitor real-time site performance data throughout EHR system implementation at all sites. Continued use of this dashboard would enable VA to better understand system incidents in real time and facilitate timely response.

Informal Reporting of Major Performance Incidents May Misrepresent Patient Safety Risk

Major performance incidents have the potential to delay care to veterans, but they are not currently connected to patient outcomes. Although VA routinely tracks patient safety events related to the EHR system as a whole—for example, system disruptions potentially contributing to errors in patient data and delays in care—there is no formal process to link reporting of these events in the Joint Patient Safety Reporting System (which is voluntary) to specific major performance incidents.

At the request of the audit team, four of the five VA medical centers using the EHR system identified patient safety reports they attributed to major performance incidents during the period reviewed. However, these reports may not reflect all patient safety events because facility staff must manually search the reports for keywords that might suggest a connection to a major performance incident. Consequently, the team could not validate the number of patient safety incidents. Because of this, there is a risk that events associated with the EHR may not be identified with a negative patient outcome, and their causes may not be prioritized appropriately.

[128] In April and August 2022, VA determined Oracle Health violated aspects of the EHR contract, and a VA contracting officer issued letters of concern and asked the contractor to respond with corrective action plans to address the situations. Inclusive of all incidents reviewed, between October 2020 and April 2022, there were 307 major performance incidents that ranged in duration from one minute to 27 hours and seven minutes.

Further, VA does not have comprehensive insight into how significantly these incidents could be affecting patient care.

The OIG's eighth recommendation is VA should reassess facilities' patient safety reports identified during this audit to determine whether additional actions need to be taken and provide a plan to do so. Finally, VA should develop a mechanism to better identify major performance incidents and negative patient outcomes and provide a plan to prioritize and address their causes.

Conclusion

An EHR system that reliably provides access to patient information is critical to delivering quality health care. However, since VA began implementing the system, many major performance incidents have occurred, hindering clinicians' access to patient records and increasing risk to patient safety. To counter that risk, VA needs better controls to improve incident management. These include an awareness to prevent the weaknesses that contribute to incidents, adequate procedures to respond to and resolve incidents according to the contract and guidance, and training and backup systems to maintain continuity and mitigate impact during downtime.

Ultimately, major performance incidents occurred because VA's initial contract requirements were limited. Although the EHR contract was modified in May 2023, VA should consider additional controls to help prevent further incidents from occurring and strengthen the department and contractor's response to them. If actions are not taken to improve EHR operations, major performance incidents will continue to occur, leading to further delays in EHR system implementation while putting patient safety at risk.

Recommendations 1–9

The OIG made the following recommendations to the acting program executive director of the EHRM Integration Office:

1. Assess electronic health record major performance incident data needs and contractually commit to real-time data sharing that will provide greater awareness of system operations.
2. Develop a formal procedure for verifying performance metrics and associated credits to ensure the department receives the remedies it is due under the contract.
3. Update the process for prioritizing major performance incidents to ensure that notification and resolution occur in a consistent manner.
4. Develop effective notification and resolution metrics that consistently capture results for all major performance incidents, regardless of the owner, and enforce them.

5. Identify the information needed in post-resolution reports, such as corrective and preventative actions, and require the contractor to consistently collect, verify, and report that information as a contract deliverable.

The OIG made the following recommendations to the under secretary for health:

6. Develop a plan to ensure all clinicians are familiar with the national downtime procedures.
7. Identify the appropriate backup system and develop a training strategy to ensure clinicians can use the system during downtime.
8. Assess facilities' patient safety reports identified during this audit to determine if additional actions need to be taken and, if so, provide an action plan.
9. Develop a mechanism to better identify major performance incidents and negative patient outcomes and provide a plan to prioritize and address their causes.

VA Management Comments

The EHRM Integration Office acting program executive director concurred with recommendations 1 through 5 and provided action plans for each:

- **Recommendation 1**. The acting program executive director reported that sharing real-time system operations data between VA and DOD will enhance the efficacy of the federal EHR. VA currently has access to real-time incident data through the VA ServiceNow Remedy Bidirectional Help Desk Interface but will evaluate additional opportunities such as data feeds from Lights On Network incident data. The target completion date is December 2024.
- **Recommendation 2**. The acting program executive director indicated that VA will formalize the existing process for reviewing and confirming credits in a documented standard operating procedure. The target completion date is December 2024.
- **Recommendation 3**. The acting program executive director stated that since 2022, VA has used "mean time to resolve" and "total time to repair" metrics to assess the efficacy of incident resolution. The acting director reported that these metrics have been trending positively and further stated that although processes and procedures have been improved to manage the differences between DOD and VA prioritization matrixes, VA will review existing processes to ensure that notifications and resolutions occur in a consistent manner. The target completion date is December 2024.
- **Recommendation 4**. The acting program executive director reported VA has notifications in place that display these metrics, which have been enhanced since the

audit period. VA will continue to work to align EHRM resolution metrics to OIT's resiliency scorecard to facilitate better capture and enforcement. The target completion date is December 2024.

- **Recommendation 5**. The acting program executive director wrote that VA will continue to require the contractor to collect, verify, and report such information as a part of existing contract deliverables and will do the same for any additional contract deliverables as necessary. The target completion date is May 2025.

The VHA under secretary for health concurred with recommendations 6 through 9 and reported actions specific to recommendations 6, 7, and 9 were completed in July 2024.

- **Recommendation 6**. VHA program offices developed a plan to ensure that clinicians understand downtime procedures, which the under secretary for health stated was documented in the *Millennium EHR Downtime Standard Operating Procedure* and was provided to sites that use the new EHR. The under secretary indicated the procedure assigns responsibility to medical center leaders to monitor compliance with associated procedures and ensure employees understand their responsibilities during and after any EHR downtime. In addition, the procedure contains information on training staff.
- **Recommendation 7**. The under secretary for health stated that VHA program offices, in coordination with OIT and the EHRM Integration Office, identified appropriate backup systems and developed an associated training strategy. According to the under secretary, the *Millennium EHR Downtime Standard Operating Procedure* provides guidance on using the 724Access DTV and the VA JLV during downtime and holds medical center leaders responsible for ensuring that staff review the training resources within the procedure and comply with the downtime procedure.
- **Recommendation 8**. The under secretary for health wrote that the appropriate VHA program offices will review the patient safety reports identified during the audit and assess whether any corrective actions are needed. The target completion date is January 2025.
- **Recommendation 9**. The under secretary for health indicated that the appropriate VHA program office, in coordination with EHRM Integration Office, developed a mechanism to identify major performance incidents. These offices will assess the current process for communicating negative patient outcomes and develop a plan to address their causes as needed, according to the under secretary.

OIG Response

The EHRM Integration Office acting program executive director provided a responsive action plan with target completion dates for recommendations 1 through 5. The OIG will monitor implementation of the planned actions and will consider the recommendations open until VA has provided sufficient evidence to demonstrate the cited corrective actions have been implemented.

The under secretary for health concurred with recommendations 6 through 9 and provided a responsive action plan. The under secretary for health reported that the following actions completed in July 2024 satisfy recommendations 6, 7, and 9 and requested closure of those recommendations: VHA developed a plan to ensure that clinicians understand downtime procedures, identified appropriate backup systems and developed an associated training strategy, and developed a mechanism to better identify major performance incidents and negative patient outcomes. However, the OIG will monitor the implementation of VHA's planned actions and will close these recommendations when VHA provides sufficient evidence demonstrating progress in addressing the intent of the recommendations and the issues identified. Specifically, VHA needs to demonstrate that its downtime procedure was communicated to clinicians, that the mechanism for tracking incidents and outcomes is operating, and that the assessment of its process for communicating negative patient outcomes is completed. Appendixes C and D include the full text of VA's comments.

Appendix A: Electronic Health Record (EHR) Implementation Timeline

In May 2018, VA awarded a 10-year contract to Cerner, now Oracle Health, to replace its EHR system. As of May 2024, VA was over halfway into the timeline; however, the system has only been implemented at six VA sites (the five in table A.1 and the one in North Chicago).

Table A.1. Five Sites Where EHR System Was Initially Deployed

VA site	Selected facility/facilities	Location
VA Spokane Healthcare System	Mann-Grandstaff VA Medical Center	Spokane, Washington
VA Walla Walla Health Care System	Jonathan M. Wainwright Memorial VA Medical Center	Walla Walla, Washington
VA Central Ohio Healthcare System	Chalmers P. Wylie Veterans Outpatient Clinic	Columbus, Ohio
Roseburg VA Health Care System	Roseburg VA Medical Center	Roseburg, Oregon
VA Southern Oregon Healthcare System	VA Southern Oregon Rehabilitation Center and Clinics	White City, Oregon

Source: VA OIG analysis of VA deployment information and VA websites.

Note: VA deployed the EHR system at the Captain James A. Lovell Federal Health Care Center in North Chicago, Illinois, on March 9, 2024.

Figure A.1 on the next page provides a timeline of significant developments involving the EHR.

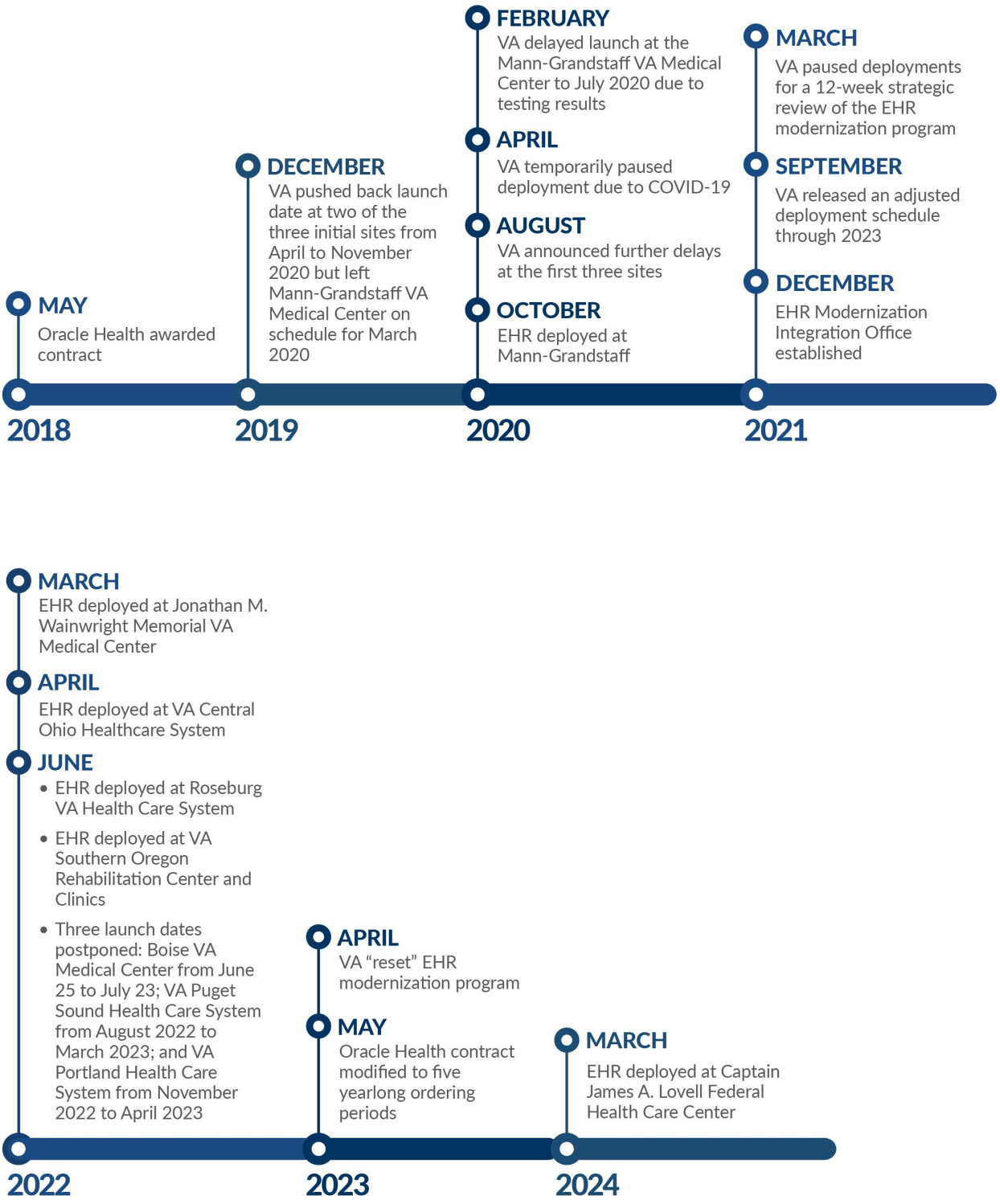

Figure A.1. *Chronology of EHR implementation.*

Source: VA OIG analysis of VA contract documentation, VA deployment schedules, and VA communication.

Appendix B: Scope and Methodology

Scope

The audit team conducted its work from September 2022 through July 2024. The team reviewed the controls VA and Oracle Health had in place to prevent, respond to, and mitigate the impact of major performance incidents involving the electronic health record (EHR) system. Specifically, these incidents included outages, performance degradations, and incomplete functionality since the go-live at the first VA medical facility—from October 24, 2020, through August 31, 2022. The scope includes the five VA sites that went live during that period. The team also conducted analysis of the number and duration of VA and Oracle Health major performance incidents from September 1, 2022, through March 31, 2024.

Statistical Sampling

To assess whether VA and Oracle Health had sufficient controls in place to prevent, respond to, and mitigate the impact of EHR system major performance incidents, the team coordinated with an audit statistician to develop the methodology for testing major performance incidents. The team reviewed a sample of major performance incidents and corresponding documentation within the audit period.

Population

The population included 681 records of major performance incidents occurring from October 24, 2020, through August 31, 2022. For the purposes of the audit, the team excluded from the population records of incidents with duplicate record numbers; loss of redundancy (incidents that did not affect users); a responsible party other than VA or Oracle Health, such as the Department of Defense (DOD); or duration less than a total of 30 minutes. These restrictions resulted in a final population of 360 unique major performance incidents.

Sampling Design

The team judgmentally selected one and statistically selected 34 major performance incidents from the population of major performance incident records.[129] Although some incidents passed through more than one category before resolution, the team counted each incident only once.[130]

[129] The audit team judgmentally selected one incident it considered to be high risk—system disruptions that lasted 27 hours and seven minutes.

[130] Major performance incident categories include outages, incomplete functionality, performance degradation, and loss of redundancy.

The population was stratified based on timing and incident type and categorized in the four strata seen in table B.1.

Table B.1. Sample Summary

Stratum	Definition	Incident count	Sample size
1	Judgmental: high risk, March 3, 2022, major performance incident	1	1
2	Statistical: configuration updates	94	14
3	Statistical: configuration	155	10
4	Statistical: non-configuration related	113	10
Total		**360***	**35**

Source: VA OIG stratified population of Lights On Network data were obtained from October 24, 2020, through August 31, 2022.

Note: Stratum 2, or configuration updates, includes changes such as system updates and upgrades. Stratum 3, or configuration, includes modifications to components and password changes. Stratum 4, or non-configuration related, includes application of networks and applications or programs running on a system.

** The audit team did not include the three incidents that the Lights On Network categorized as cyber incidents. The team excluded these incidents because Oracle Health personnel reported they were the responsibility of DOD.*

Because of the small sample size, the team did not report projections to the population.

Methodology

The team identified and reviewed applicable laws, regulations, policies, local procedures, and Government Accountability Office and industry practices pertaining to preventing, responding to, and mitigating major performance incidents. In addition, the team reviewed documentation from various VA offices and Oracle Health pertaining to the management of incidents. The team also reviewed prior audit work and recommendations related to VA's EHR. The team determined some previous audit reports had relevance to its objective, but the recommendations for these reports were either closed or their implementation was delayed during the audit. Furthermore, the team obtained contractual documentation from VA's Electronic Contract Management System pertaining to VA's EHR system. The team coordinated with the Office of the Counselor to the Inspector General for legal guidance during the audit.

To learn more about how major incidents are managed, the team interviewed VA officials from the Technology Acquisition Center in the Office of Acquisition, Logistics, and Construction; Electronic Health Record Modernization (EHRM) Integration Office; Office of Enterprise Integration; National Center for Patient Safety; Enterprise Command Operations in the Office of

Information and Technology (OIT); and the offices of Health Informatics and Nursing Services in the Veterans Health Administration (VHA). In addition, the team conducted site visits to the Mann-Grandstaff VA Medical Center (Spokane, Washington), the Jonathan M. Wainwright Memorial VA Medical Center (Walla Walla, Washington), the Chalmers P. Wylie Veterans Outpatient Clinic (Columbus, Ohio), and VA Central Office in Washington, DC. Furthermore, the team interviewed VA personnel at Roseburg VA Health Care System (Oregon) and VA Southern Oregon Healthcare System (White City). The team also obtained evidence from and interviewed VA contractor staff at Oracle Health (Kansas City, Missouri).

To obtain information on major performance incidents, the team evaluated data and reports from Oracle Health's Lights On Network dashboard. Furthermore, the team assessed VA and Oracle Health incident reporting to determine the frequency and duration of major performance incidents, why they occurred, and how they were resolved. In addition, the team reviewed documentation related to the management of these incidents, including incident tickets, incident reports, and root cause analyses. The team also used this information to confirm Oracle Health's compliance with VA contract performance metrics. When appropriate, the team consulted with OIG IT specialists about the results of its assessments of system controls.

To determine whether VA effectively mitigated the impact of major system incidents, the team evaluated VA enterprise and medical facility procedures for when a system downtime event occurred. The team also determined what backup systems were available to medical facilities and how these systems were used when an event occurred. In addition, the team reviewed patient safety summary information to determine whether adverse health events may have resulted from incidents. The team also attempted to confirm whether patient safety events could be linked to specific incidents, but the safety reports did not include the detail necessary to do so.

Internal Controls

The team assessed the internal controls significant to the audit objective.[131] The team identified the following four components and five principles as significant to the objective.[132] The team identified internal control weaknesses during this audit and proposed recommendations to address the following control deficiencies:

- Component: Control Environment
    - Principle 3: Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

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

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

- Component: Risk Assessment
    - Principle 7: Management should identify, analyze, and respond to risks related to achieving the defined objectives.
- Component: Control Activities
    - Principle 12: Management should implement control activities through policies.
- Component: Information and Communication
    - Principle 13: Management should use quality information to achieve the entity's objectives.
    - Principle 14: Management should internally communicate the necessary quality information to achieve the entity's objectives.

Data Reliability

The team obtained data on major incidents from Oracle Health's Lights On Network and VA's ServiceNow system to identify performance information, including the start date, the site(s) affected, the responsible party, and the incident description. The team researched these systems and data by reviewing VA documentation, including contract documents. This documentation provided information on the data tracked in the Lights On Network and ServiceNow system. In addition, the team contacted EHRM Integration Office, OIT, and Oracle Health personnel to discuss Lights On and ServiceNow data.

To ensure the reliability of computer-processed data, the team conducted multiple reasonableness tests of Lights On Network data, including checking the completeness for the time frame. The team also compared selected Lights On data from the period reviewed to selected data fields in Lights On at different times during the audit. In addition, the team validated the Lights On data for the period by assessing it against Oracle Health service outage analysis information. The team also verified the reliability of ServiceNow data by cross-referencing selected system data against VA root cause analysis reports. Based on this data reliability assessment, the team concluded the Lights On and ServiceNow data used during the audit were appropriate and sufficient.

Furthermore, the team obtained EHR system contract documentation from VA's Electronic Contract Management System as well as invoice data from VA's invoice payment processing system. The team confirmed the availability of contract documentation with VA. To assess the reliability of invoices gathered, the team compared invoices to accounting records pulled from VA's financial management system. The team identified no discrepancies in the invoice credits applied for the associated contract metrics and verified the receipt by VA. The team determined

the documentation maintained in VA's Electronic Contract Management System and invoice payment processing system was sufficiently reliable for the purposes of this audit.

Government Standards

The OIG conducted this performance audit in accordance with generally accepted government auditing standards. 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.

Appendix C: VA Management Comments, Acting Program Executive Director, Electronic Health Record Modernization Integration Office

Department of Veterans Affairs Memorandum

Date: August 9, 2024

From: Acting Program Executive Director, Electronic Health Record Modernization Integration Office (00EHRM)

Subj: Audit—VA Needs to Strengthen Controls to Address Electronic Health Record System Major Performance Incidents (VIEWS 12003219)

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

1. Thank you for the opportunity to review the Department of Veterans Affairs (VA) Office of Inspector General (OIG) draft report "VA Needs to Strengthen Controls to Address Electronic Health Record System Major Performance Incidents." The report contains five recommendations (Recommendations 1-5) for the Electronic Health Record Modernization Integration Office (EHRM-IO), and I concur with all five recommendations.

2. VA's Electronic Health Record Modernization (EHRM) effort is, at its core, a large system transformation. The Federal EHR system is a highly complex environment composed of the core medical records system and several other connected systems that together deliver the overall EHR experience to clinical providers and patients. Improving overall system reliability, resiliency and availability remains critical for VA. While the draft report documents known system and process issues that occurred during the initial set of deployments between October 2020 and August 2022, since then VA has realized significant improvements to system performance and implemented more effective contractual controls.

3. As a result of VA's systematic approach to achieving sustained high performance and high reliability, the core Federal EHR has increasingly stabilized over time, resulting in improvements to the user experience. Since August 2022, there have been only three months in which the Service Level Agreement (SLA) threshold for Outage-Free Time (OFT) has not been met. The Incident-Free Time (IFT) rate has dramatically improved since August 2022: Oracle Health has achieved a 30% reduction in hangs and crashes experienced by the 1% of system users experiencing the worst performance among their peers. While IFT was not included as a contractual requirement until May 2023, since then there have only been four months in which the SLA for IFT has not been met. In addition to the incorporation of IFT, as part of the contract renegotiation in May 2023, VA increased the number SLAs with concrete financial consequences related to technical performance and user experience. There are now 22 SLAs and 6 service-level obligations in place and VA has seen improvement across all metrics.

4. While the core Federal EHR has stabilized, VA recognizes that the frequency of performance incidents and outages is still a challenge and accordingly, will continue expend maximal effort to reduce any preventable events. Even with this effort, there will likely still be some level of system disruption, partly due to the number of changes still being introduced to the Federal EHR environment by both VA and the Department of Defense (DoD). It is a well-established axiom of software development that systems stabilize when the rate of changes made to the system decreases. The rate of change is still high for the Federal EHR, likely contributing to more incidents. Accordingly, combined with current engineering,

testing, and management efforts, VA anticipates that the system's performance will improve even further when the change velocity decreases, and enough time has passed to address unanticipated defects.

5. VA is continuing to move forward with implementing a modern, commercial EHR solution in close coordination with our Federal partners, including DoD and the Federal EHRM Program Office, but we know from listening to VA clinicians that the system reliability of the Federal EHR is not yet meeting expectations. While our current progress in the program Reset is reassuring, we still have important work ahead, and we expect to see continued improvements in technical performance at our current and future live sites.

The OIG removed point of contact information prior to publication.

(Original signed by)

Neil C. Evans, M.D.

Attachment

Attachment

ACTION PLAN

Recommendation 1

The EHRM-IO Acting Program Executive Director assesses electronic health record major performance incident data needs and contractually commit to real-time data sharing that will provide greater awareness of system operations.

VA Response: Concur

Target Date for Completion: December 2024

Comments

The Department of Veterans Affairs (VA) concurs with the recommendation to enhance real-time data sharing to provide greater awareness of system operations. Sharing real-time system operations data between VA and the Department of Defense (DoD) will enhance the efficacy of the Federal Electronic Health Record (EHR). VA currently has access to real-time incident data through the VA ServiceNow (SNOW) Remedy Bidirectional Help Desk Interface (BDHDI) but will evaluate additional opportunities such as data feeds from Lights On Network (LON) incident data.

Recommendation 2

The EHRM-IO Acting Program Executive Director develops a formal procedure for verifying performance metrics and associated credits to ensure the department receives the remedies it is due under the contract.

VA Response: Concur

Target Date for Completion: December 2024

Comments

VA will formalize the existing process for reviewing and confirming credits in a documented Standard Operating Procedure (SOP).

Recommendation 3

The EHRM-IO Acting Program Executive Director updates the process for prioritizing major performance incidents to ensure that notification and resolution occur in a consistent manner.

VA Response: Concur

Target Date for Completion: December 2024

Comments

Since 2022, VA has utilized Mean Time to Resolve (MToR) and Total Time to Repair (TToR) to assess the efficacy of incident resolution. These metrics have been trending positively. Processes and procedures have been improved to manage the required differences between DoD and VA prioritization matrixes, but VA will review existing processes to ensure that notifications and resolutions occur in a consistent manner.

Recommendation 4

The EHRM-IO Acting Program Executive Director develops effective notification and resolution metrics that consistently capture results for all major performance incidents, regardless of the owner, and enforce them.

VA Response: Concur

Target Date for Completion: December 2024

Comments

VA has notification metrics in place and both the LON and SNOW interfaces that display these metrics have been enhanced since the audit period contemplated by OIG. VA will continue to work to align EHRM resolution metrics to the Office of Information and Technology (OIT) Resiliency Scorecard to facilitate better capture and enforcement.

Recommendation 5

The EHRM-IO Acting Program Executive Director identifies the information needed in post-resolution reports, such as corrective and preventative actions, and require the contractor to consistently collect, verify, and report that information as a contract deliverable.

VA Response: Concur

Target Date for Completion: May 2025

Comments

VA will continue to require the contractor to collect, verify, and report such information as a part of existing contract deliverables, and will do the same for any additional contract deliverables that are deemed necessary.

Recommendation 6

The Under Secretary for Health develops a plan to ensure all clinicians are familiar with the national downtime procedures.

VA Response: Concur; request closure

Completion Date: July 2024

Comments

The Veterans Health Administration (VHA) program offices developed a plan to ensure that clinicians understand downtime procedures. It was documented in the Millennium EHR Downtime SOP and provided to sites that use the new EHR. The SOP assigns responsibility to Medical Center leadership for developing a local Downtime Workgroup to monitor compliance with associated procedures and ensure employees understand their responsibilities during and after any EHR downtime. In addition, the SOP contains information on training staff and offers further appendices and external resources. The VHA Digital Health Office, along with other VHA program offices, will assist Medical Center leadership as necessary in implementing EHR downtime procedures. VHA respectfully requests closure in the published report based on the supporting evidence provided.

Recommendation 7

The Under Secretary for Health identifies the appropriate backup system and develop a training strategy to ensure clinicians can use the system during downtime.

VA Response: Concur, request closure

Completion Date: July 2024

Comments

VHA program offices, in coordination with OIT and EHRM-IO, identified appropriate backup systems and developed an associated training strategy. The 724Access Downtime Viewer product provides current inpatient clinical encounter information and the VA Joint Legacy Viewer is the primary source of clinical information for outpatient care. The Millennium EHR Downtime SOP provides guidance on using these solutions when a user is seeking inpatient or outpatient clinical information during downtime. The procedural section of the SOP provides backup system instructions and specific use cases. The appendices provide training resources for both backup clinical information systems. Medical Center leadership is responsible for ensuring that the appropriate staff review the training resources within the SOP and comply with the downtime procedures. VHA respectfully requests closure in the published report based on the supporting evidence provided.

Recommendation 8

The Under Secretary for Health assesses facilities' patient safety reports identified during this audit to determine if additional actions need to be taken and, if so, provide an action plan.

VA Response: Concur

Target Date for Completion: January 2025

Comments

The Quality and Patient Safety (QPS) and Informatics Patient Safety program offices will review the patient safety reports identified during the audit and assess if any corrective actions are needed.

Recommendation 9

The Under Secretary for Health develops a mechanism to better identify major performance incidents and negative patient outcomes and provide a plan to prioritize and address their causes.

VA Response: Concur, request closure

Completion Date: July 2024

Comments

The QPS program office, in coordination with EHRM-IO, developed a mechanism to identify major performance incidents. When a major performance incident occurs, a notification is sent to all technical and functional leads for action. Technical and functional leads with equity in the incident participate in a resolution call and Medical Center users receive an alert via the EHR alert messaging system. When the major performance incident is resolved, a corrective action/preventive action review is completed. The QPS program office, in coordination with EHRM-IO, will assess the current process for communicating negative patient outcomes and develop a plan to address their causes as needed. VHA respectfully requests closure in the published report based on the supporting evidence provided.

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 D: VA Management Comments, Under Secretary for Health

Department of Veterans Affairs Memorandum

Date: July 29, 2024

From: Under Secretary for Health (10)

Subj: OIG Draft Report, Audit of VA's Measures Taken for Major Performance Incidents Impacting the Electronic Health Record System (VIEWS 11989198)

To: Executive Director, Electronic Health Record Modernization Integration Office (00EHRM)

1. Thank you for the opportunity to review and comment on the OIG draft report regarding major performance incidents affecting the electronic health record (EHR) system. The Electronic Health Record Modernization Integration Office will provide responses to recommendations one through five. The Veterans Health Administration (VHA) concurs with the recommendations made to the Under Secretary for Health (6-9). VHA's action plan to address these recommendations is attached.

2. VHA appreciates the work performed by the OIG. VHA will continue the development of rapid and reliable processes for quickly identifying and resolving issues within the new EHR. Collectively, VA and VHA embrace OIG's recommendations as renewed opportunities to strengthen EHR controls related to major performance incidents.

The OIG removed point of contact information prior to publication.

(Original signed by)

Shereef Elnahal, M.D., MBA

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.

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	Jessica Blake, Director Quentien Brewington Cynthia Christian Angela Ferguson Benjamin Howe Ryan Mols Cecilia Shim Nancy Soto
Other Contributors	Laurence Adair Michael Martin Charlma Quarles Allison Tarmann

Report Distribution

VA Distribution

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

Non-VA Distribution

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

OIG reports are available at www.vaoig.gov.