



UT Health

San Antonio

Internal Audit &
Consulting Services

Internal Audit & Consulting Services
7703 Floyd Curl Dr. MC#7974
San Antonio, Texas 78229-3900
210-567-2370 Fax: 210-567-2373
www.uthscsa.edu

Memorandum

Date: February 26, 2024
To: Andrea Marks
Senior Executive Vice President and Chief Operating Officer
From: John Lazarine, Chief Audit Executive
Internal Audit & Consulting
Subject: Audit Report – *Audit of Epic Hosting Information Security*

Enclosed is the Epic Hosting Information Security audit report. Please review the report and contact me to discuss any comments. If there are no comments, please acknowledge your agreement with the distribution of this report and forward it to Dr. Robert Hromas for his review.

Reviewed by Andrea Marks: _____

Reviewed by Dr. Robert Hromas, *Acting President*: _____

Enclosure

JL:sjg

Epic Hosting Information Security

As part of the Hosting Services Agreement (Agreement) with Epic for safeguarding the Epic data, the University of Texas Health San Antonio (“UTHSA”), is responsible for implementing and maintaining controls that meet or exceed the standards set by Epic (Standards) as outlined in the *Your Organization’s Responsibilities for Information Security* document attached to the Agreement. See Appendix 2.

Of the eight information security domains audited, three of the eight control objectives could not be achieved. These are “Entity Level Control”, “User Access Provisioning and Activity Monitoring” and “Physical Security”.

During this audit, Management took actions to address the findings outlined in this report. Internal Audit verified that the actions taken have mitigated the risks and considered the findings closed.

- *Background* | p.3
- *Audit Objective* | p. 3

This audit was conducted following the Texas Administrative Code Chapter 202 (TAC §202) and in accordance with generally accepted government auditing standards and the Institute of Internal Auditors’ International Standards for the Professional Practice of Internal Auditing.

HIGH
Control Domain - User Access Provisioning and Activity Monitoring.

Control - Terminated employees’ access to the application is removed in a timely manner upon termination.

Internal Audit noted that sampled terminated user accounts were not removed/disabled timely per UTHSA’s access management policy.

Summary of Results |p.4

HIGH
Control Domain – Physical Security

Control - Access to the data center is secured and reviewed periodically.

Internal Audit noted a periodic review of access to the data center is not defined and/or not in place.

Summary of Results |p.4

HIGH
Control Domain – Entity Level Control

Control - Quarterly, a self-evaluation is performed and submitted to Epic to confirm the agreed-upon security practices are in place.

The process for validating the Epic Security Self-evaluation was not formally documented. Specifically, what should be reviewed, as well as what supporting documents/evidence should be retained in support of the security attestation. was reviewed.

Summary of Results |p.5

Summary of Management's Response

Internal Audit made recommendations to address the issues identified during this audit. Those recommendations are provided at the end of each section in this report. The process owners agreed with the recommendations addressed to them.

Ratings Definitions

Internal Audit used professional judgment and rated the audit findings identified in this report. The issue ratings identified for each chapter were determined based on the degree of risk or effect of the findings with the audit objectives.

PRIORITY - An issue identified by an internal audit that, if not addressed on a timely basis, could directly impact the achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.

HIGH - A finding identified by an internal audit that is considered to have medium to high probability of adverse effects to a UT institution or the UT System as a whole.

MEDIUM - A finding identified by an internal audit that is considered to have medium to high probability of adverse effects to a UT institution or the UT System as a whole.

LOW - A finding identified by an internal audit that is considered to have medium to high probability of adverse effects to a UT institution or the UT System as a whole.

N/A - No reportable findings or observations were identified during the audit.

For more on the methodology for issue ratings, see Report Ratings in Appendix 1.

Background Information

The University of Texas Health San Antonio (“UTHSA”) and Epic Hosting, LLC (“Epic”) share the responsibility for safeguarding the Epic data. While UTHSA’s Epic-hosted environments reside on infrastructure maintained by Epic, UTHSA controls the end users’ and administrators’ access to the environments, as well as servers, appliances, and other technology that connect to or integrate with Epic-hosted environments. As a result, UTHSA’s administrative, technical, and physical security controls can impact the security of the data Epic stores and processes, as well as the Epic-hosted environments.

As part of the Hosting Services Agreement (Agreement), UTHSA is responsible for implementing and maintaining controls that meet or exceed the standards set by Epic (Standards) as outlined in the *Your Organization’s Responsibilities for Information Security document* attached to the Agreement. See *Appendix 2*

Quarterly, the Chief Information Security Officer (CISO) is required to perform, and submit to Epic, a self-evaluation and attest to meeting the Standards. In addition to the quarterly self-evaluation, Epic requires a yearly audit of compliance with the Standards.

Objective & Scope

The primary objective of this audit is to evaluate the security posture of Epic to help ensure that electronic patient health records and billing data are effectively safeguarded, with access being restricted to those whose primary responsibilities require that access and are not unnecessarily vulnerable to inside or outside threats.

The scope included an assessment of the following Information Security Domains taking a risk-based approach.

- Entity Level Control - Control provides reasonable assurance that information security controls are maintained.
- End Point Security - Control provides reasonable assurance that there is protection and maintenance for endpoints such as physical or virtual workstations used by end users to connect to Epic-hosted environments.
- User Access Provisioning and Activity Monitoring - Control provides reasonable assurance that user's access and attempts are monitored, and appropriate use of Epic applications by users and promptly investigating any suspected inappropriate access.
- Network Access - Control provides reasonable assurance that users securely connect to the network before connecting to the Epic-hosted environment.
- Third-Party Integrations - Control provides reasonable assurance that third-party integration is configured per request and authorization from the customer.
- Incident Reporting - Control provides reasonable assurance that identified incidents in the Epic-hosted environment are reported in a timely manner.
- Physical Security - Control provides reasonable assurance that the physical security of devices and infrastructures that connect users to Epic-hosted environments are secured.
- Infrastructure Security - Control provides reasonable assurance that the infrastructure residing within Epic’s data centers is maintained.

Summary of Results

HIGH**User Access Provisioning and Activity Monitoring**

Control Description: Terminated employees' access to the application is removed in a timely manner upon termination.

Observation: 20 of 25 sampled terminated users' Active Directory access was not disabled timely per the institution's access management policy that states "terminated user accounts should be disabled immediately". The authentication path to the Epic system is with an authorized individual's Active Directory credentials (username and password). IA noted the termination period range for removal of access was between 6 and 108 days.

Therefore, the delayed removal of access can result in terminated employees retaining access to sensitive systems and data, increasing the risk of data breaches or unauthorized actions, legal consequences, and reputational damage.

Recommendation:

(a1) Management to determine a formal process to ensure terminated users are deactivated immediately from the AD layer per the standard defined in the UTHSA access management policy and given the authentication path to the Epic system is through network credentials.

(a2) A retroactive analysis and review of terminated users should be performed by ensuring the Network credentials are deprovisioned on the effective termination date or within 3 business days.

(b1) Automating the termination process - The initiation of the process would start with HR inputting the information of the terminated user in the HR system. A scheduled job picks up the termination job to disable access to the Network and respective applications wherein the configuration integration is applicable. If not possible at the application layer, periodic removal of terminated users at the application layer should be completed.

OR

(b2) Alternatively, HR sends out a daily list of terminated users to the Application owner or Application System Administrator with effective termination dates for terminated users. This would ensure the terminated users can be disabled immediately upon receipt.

Management's Response: Accounts terminated from the Active Directory layer, AD, do not have access to the Epic system. Therefore, a process to ensure all terminated accounts at the AD layer are inactivated in the Epic system timely was put in place. This process includes –

- 1) When users are terminated in the HRIS system, HR sends the Epic security team an email notification of the termination date and the Epic account is inactivated the same day upon receipt of the notification.
- 2) Weekly, the Epic Security team runs a script that searches for any account that has not logged in 90 days or more in the Epic system and inactivates them proactively.

Responsible for Implementation: The Epic Security Team, is responsible for implementation with an estimated completion date of 01/25/24.

Remediation Status: Control deficiency was remediated and verified by Internal Audit.

HIGH

Physical Security

Control Description: Access to the data center is secured and reviewed periodically.

Observation: A periodic review of access to the data center is not defined and/or not in place. Therefore, unauthorized access or security breaches can disrupt data center operations, affecting business continuity and services.

Recommendation:

- (a) Management to determine the frequency of review. Monthly preferred
- (b) Reviewer(s) to obtain a system-generated report of users with access to the data center on the defined frequency period.
- (c) Reviewer(s) to ensure evidence to validate the completeness of data is included and retained in the review completed.
- (d) Reviewer(s) to confirm the appropriateness of authorized individuals with access to the data center from the report provided.
- (e) If inappropriate access was identified, a lookback analysis should be performed. Reviewer(s) should determine as of when this identified individual was inappropriate, review the audit log to determine if his/her access was used after the time considered inappropriate, retain supporting evidence, and request removal of access. Please ensure all documentation is retained and stored.

Management's Response:

1. GRC@uthscsa.edu will receive a quarterly report (every January, April, July, and October) from the University of Texas Police Department, UTPD, containing the list of individuals with access to the ADC.
2. Governance Risk & Compliance (GRC)/Manager Information Security & Assurance/CISO will review and make necessary revisions to the list before forwarding it to the Chief Information Officer, CIO.
3. The CIO will review and respond to the emailed list as attestation, including any further changes.
4. GRC will submit any access changes to UTPD via the Access Requests Service Request.
5. If necessary, GRC will communicate any updates to Data Center Operations staff via eso-dcsiteam@uthscsa.edu.

Responsible for Implementation: GRC/ CISO/ CIO is responsible for implementation with an estimated completion date of 11/9/2023.

Remediation Status: Control deficiency was remediated and verified by Internal Audit.

HIGH

Entity Level Control

Control Description: Quarterly, a self-evaluation is performed to confirm that the agreed-upon security practices are in place.

Observation: The process for validating the Epic Security Self-evaluation was not formally documented. Specifically, what should be reviewed, as well as what supporting documents/evidence should be retained in support of the security attestation.

Recommendation: Management should formally document the process to validate the Epic quarterly self-evaluation. This should include what information should be reviewed, as well as what evidence should be retained to support the conclusion of the security self-assessment.

Management's Response:

1. Management will develop a formal, documented, process for completing the quarterly security self-evaluation.

2. GRC will be responsible for requesting and reviewing the evidence needed for the completion of the quarterly security self-evaluation.
3. GRC will support the CISO and be responsible for the completion of the quarterly Epic security self-evaluation and the annual Epic security compliance audit.
4. The CISO is responsible for completing the quarterly security self-evaluation checklist upon review of the attestation completed by the control domain owners, sign-off on the document and send to Epic.

Responsible for Implementation: The Chief Information Security Officer, CISO, is responsible for implementation with an estimated completion date of 01/31/2024.

Remediation Status: Control deficiency was remediated and verified by Internal Audit.

N/A

User Access Provisioning and Activity Monitoring

Control provides reasonable assurance that user's access and attempts are monitored, and appropriate use of Epic applications by users and promptly investigating any suspected inappropriate access.

Control provides reasonable assurance that users who have access to the Epic-hosted environments have unique accounts assigned and password adheres to defined standards.

Control provides reasonable assurance that generic account use is restricted and monitored.

Control provides reasonable assurance that users who have access to the Epic-hosted environments were authorized and provisioned appropriately and reviewed periodically.

N/A

End Point Security

Control provides reasonable assurance that there is protection and maintenance for endpoints such as physical or virtual workstations used by end users to connect to Epic-hosted environments.

N/A

Network Access

Control provides reasonable assurance that users securely connect to the network before connecting to the Epic-hosted environment.

N/A

Third-Party Integrations

Control provides reasonable assurance that third-party integration is configured per request and authorization from the customer.

N/A

Incident Reporting

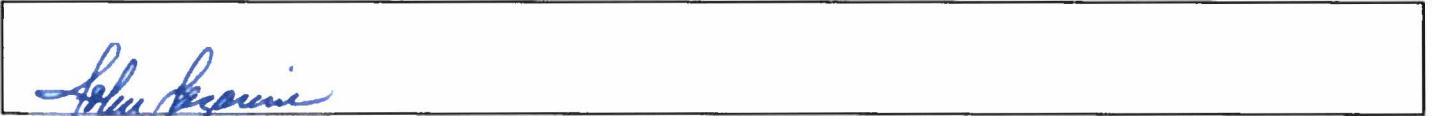
Control provides reasonable assurance that identified incidents in the Epic-hosted environment are reported in a timely manner.

N/A

Infrastructure Security

Control provides reasonable assurance that the infrastructure residing within Epic's data centers is maintained.

APPROVED FOR RELEASE

A rectangular box containing a handwritten signature in blue ink. The signature appears to be "John Lazarine".

John Lazarine, Chief Audit Executive, Internal Audit & Consulting Services

APPENDICES

Appendix 1

Criteria

The audit was intended to meet the TAC 202 biennial review, as required by the State of Texas and UT System Administration.

Texas Administrative Code Chapter 202 (TAC §202) outlines the minimum information security and cybersecurity responsibilities and roles at state agencies and institutions of higher education. TAC §202 requires agencies and institutions of higher education to use the TAC §202 Security Controls Standards Catalog (SCSC). The security controls catalog is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, R5. Other frameworks used are the Control Objectives for Information and Related Technologies (COBIT) and the Center of Internet Security (CIS – IT related). Using a centrally managed controls catalog effectively ensures that all agencies and institutions use common language and minimum standards when implementing security measures.

Methodology

We conducted this performance audit from July 1, 2023, through December 31, 2023, in accordance with generally accepted government auditing standards and the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Report Ratings

In determining the ratings of audit findings, auditors considered factors such as financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Internal Audit also identified and considered other factors when appropriate.

The following members of the Internal Audit & Consulting Service's staff performed the audit:

- Sam Babajide, MSEM, CISA, CIPT, CPSP, ITIL (IT Audit Director)
- Wumi Awotoye, MBA, CPA (IT Audit Senior)

Appendix 2

Exhibit 10

Last revised: 02/11/2021

Your Organization's Responsibilities for Information Security

Overview

Your organization and Epic Hosting, LLC ("Epic") share responsibility for the overall security of your data. While your Epic-hosted environments reside on infrastructure maintained by Epic, you control your end users' and administrators' access to your environments, as well as servers, appliances, and other technology which connect to or integrate with your Epic-hosted environments. As a result, your organization's administrative, technical, and physical security controls can impact the security of your Epic-hosted environments. Epic expects that your controls meet or exceed the following standards. If you extend your Epic-hosted environments via Community Connect, you are responsible for ensuring these controls are in place for these affiliated sites and users.

Information Security Domains

End Point Security

You are responsible for protecting and maintaining end points, such as physical or virtual workstations, used by your end users to connect to your Epic-hosted environments.

- For devices that you or a Community Connect affiliate manage, you will at a minimum:
 - Ensure that anti-virus/anti-malware software is installed and kept up-to-date.
 - Patch end points regularly and apply critical security patches in a timely fashion.
 - Configure end point timeouts in accordance with risk assessments and regulatory requirements.
- For devices that it is not practical for you to manage (such as a physician's personal laptop used for incidental access), you will at a minimum have acceptable use policies that specify the same requirements as for your managed devices.

You are responsible for monitoring the security of your end points and remediating any observed or reported deficiencies within a reasonable timeframe based on risk.

User Provisioning and Activity Monitoring

You are responsible for verifying, provisioning, monitoring, and revoking access for your users who have access to your Epic-hosted environments. This includes both account provisioning, such as via Active Directory, and provisioning of access within the Epic applications, such as administrative and user-level security classes. At a minimum, you will:

- Assign user accounts to individuals and instruct individuals not to share credentials for any reason.
- Require reasonable password length, complexity, and rotation practices, following industry standards.

You are responsible for restricting and monitoring generic account use, such as accounts used to run automated services or emergency access accounts. For generic accounts accessing web services, additional information for configuration of strong authentication is available on Galaxy.

- Generic accounts should not be able to access the Epic-hosted environments from untrusted networks. This excludes shared clinical workstations that use generic accounts to access the operating system or application deployment environment prior to an end user authenticating with their personal credentials to the Epic application.
- For environments containing PHI, individual users should avoid using generic accounts whenever possible.
- For environments that don't contain PHI, such as training environments, you will require access to your network or a network you trust first, or require authentication with a named user account prior to use of a generic account.

You are also responsible for monitoring access, access attempts, and appropriate use of Epic applications by users and for promptly investigating any suspected inappropriate access. This includes monitoring behavior in both production and non-production environments, such as:

- Access or viewing of patient records.
- Export of patient records and other clinical or financial information in support of patient services.
- Failed login attempts and successful logins from your end points, including workstations and mobile devices, and lockout of users after no more than 10 failed attempts.

Epic provisions access to different environments, such as Production, Test, and Training environments, and network locations, such as those used to store files, via Active Directory groups or individual accounts upon your request. You are responsible for provisioning, reviewing, and revoking membership in these groups and coordinating with Epic to provision the necessary assets to the relevant users.

Network Access

You are responsible for securing access to Epic-hosted environments via your network, including how users connect to your network before connecting to the Epic-hosted environment. At a minimum, you will:

- Require at least one form of authentication when devices connect to your network (e.g., a user or system account authenticating to your domain).
- Require multifactor authentication for remote access to the Epic-hosted environments, such as access over an untrusted network like the Internet. For example, you can require multifactor authentication for remote users connecting to your network via Virtual Private Network (VPN) and then to the Epic-hosted environments, or require multifactor authentication on a publicly accessible gateway to the Epic-hosted environments. This requirement does not apply to applications designed to be publicly accessible, such as MyChart, EpicCare Link, or Haiku.
- In the event that remote access must be made available without multifactor for a limited time period, such as during an unexpected outage of the network connection between your and Epic's data centers, you will work with Epic to implement compensating controls as is feasible and disable single-factor remote access once the precipitating issues are resolved.

Review and restrict network traffic through your firewalls entering Epic-hosted environments such that only those parts of your network that need access to the Epic-hosted environments have access. If you extend your network to Community Connect sites, you will ensure they have firewalls protecting their network.

Third-Party Integrations

Upon your written request, Epic will configure the Epic Hosting side of clinical or financial third-party integrations that directly send or receive your sensitive data to or from infrastructure hosted by Epic. For example:

- If your requested integrations require Epic to configure data storage or transmission that does not conform to Epic's data protection standards, you will authorize such configuration and accept the associated risk to Epic in writing.
- Depending on technical requirements and any additional required professional services or infrastructure, such integrations may increase your Hosting Services fees. Upon your request, Epic will provide a cost estimate for such services.

If, upon your written request, Epic installs your third-party products or integrations, you are responsible for coordinating with Epic and the third party as necessary to install and maintain the integration. At a minimum, you will:

- Maintain necessary support licenses and coordinate with Epic to configure, update, and patch third-party products installed in Epic-hosted environments.
- Maintain vendor contacts and escalation points with any third party.
- Monitor and review use of third-party connections, such as web service calls, into the Epic-hosted environment.
- Escalate and work with Epic to investigate and address any known, critical security issues with third party products or integrations within a reasonable timeframe based on risk.

Incident Reporting

- An incident that impacts your environment might also impact the Epic-hosted environment. When you become aware of a potential security incident that might impact Epic-hosted environments, you are responsible for reporting it to Epic.
- If Epic notifies you of any potential security incidents, you are responsible for coordinating with us throughout the incident's life cycle.

Physical Security

- You are responsible for the physical security of devices and infrastructure that connect your users to your Epic-hosted environments.
- If Epic infrastructure resides at your facility or a facility contracted by you, you are responsible for the physical security of such infrastructure and agree to notify Epic of any security incidents impacting the security of that infrastructure.

Infrastructure Security

For infrastructure residing within Epic's data centers that you maintain, at a minimum, you will:

- Maintain necessary support licenses and coordinate with Epic to configure, update, and patch said infrastructure.

- Monitor, escalate, and work with Epic to investigate and address any known security issues with this infrastructure within a reasonable timeframe based on risk.

Epic Application and Infrastructure Configuration

Epic continues to develop software features and identify new cybersecurity initiatives to enhance and strengthen the security of the Epic application and its associated infrastructure. You will coordinate with Epic to review, prioritize, and implement these capabilities, or identify alternate secure configurations, when they are made available or identified by Epic as a best practice for your Epic environments.

Audits

You agree to audit your organization's compliance and your users' compliance, including those of your Community Connect partners, with the responsibilities in this document at least once per year and promptly remediate any identified deficiencies. Upon Epic's request, you will share a summary of your audit findings with Epic.

Distribution List

Copies of this report have been distributed to the following:

- Dr. Robert Hromas, Acting President and Dean of Medical School
- Andrea Marks, Chief Operating Officer
- Dr. Robert Leverence, Exec Vice Dean-Clinical Affairs
- Dr. Edward Sankary, Chief Health Information and Value Officer
- Yeman Collier, VP & Chief Information Officer
- Todd Holling, Deputy Chief Information Officer
- Michael Schnabel, Assistant VP, Info Sec & Ops
- Julie Wingate, Assistant VP, Clinical Systems
- Michael Walter, Chief Technology Officer
- Wayne Laski, Director of Clinical Systems Technical Infrastructure
- Sarah Cook, Director of Clinical Information Systems
- Jay Villarreal, Senior Director of Information Security & Operations
- June Cox, Manager, Access Control
- Michelle Pham, Clinical Cache DBA-Senior
- J. Michael Peppers, Chief Audit Executive, UT System