UTHealth Houston
Auditing and Advisory Services
P.O. Box 20036 | Houston, TX | 713-500-3160

Epic Security Certification

#HSC26RQ0932

EXECUTIVE SUMMARY

Auditing & Advisory Services (A&AS) has completed an assurance engagement of the Epic Security Certification. This engagement was performed at the request of the UTHealth Houston (UTHealth) Audit Committee and was conducted in accordance with the Global Internal Audit Standards.

Background

The Epic environment is hosted on infrastructure maintained by Epic. As part of the Hosting Services Agreement (Agreement), UTHealth 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 (Document) attached to the Agreement.

On a quarterly basis, the Chief Information Security Officer (CISO) is required to perform 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.

Objectives

Our objective was to verify compliance with the security practices included in the Document provided by Epic. We performed the following procedures:

Access Security

For UTHealth-managed end point devices that can access Epic (including affiliate-managed devices), verified:

a) Observed or reported deficiencies during the audit period were remediated within a reasonable timeframe based on risk.
b) Antivirus/antimalware software is installed and kept up to date.
c) Patches are applied regularly and critical security patches are applied in a timely fashion according to risk.
d) End-of-life plans for vendor notification channels are monitored and remediation plans for outdated technologies are created.
e) Session timeouts are configured according to risk assessments and regulatory requirements.

For devices where it is not practical for you (or your affiliates if applicable) to manage (such as a physician's personal device used for occasional home use), verified:

a) Users are not allowed to mount or access drives in the Epic-hosted environment nor access/mount endpoint storage from the virtual desktop infrastructure or published application (such as fixed drives or Universal Serial Bus storage passthrough).
b) Users acknowledged and accepted acceptable device use policies which specify substantially the same requirements as for your managed endpoints.

Verified network traffic is restricted/monitored to ensure only those parts of the network that need access to the Epic-hosted environments have access.

Verified multi-factor authentication (MFA) is enabled for:
*MyChart (required)
*EpicCare Link (required)
*Physician Mobile Apps (e.g., Haiku/Canto) (recommended)

Verified MFA is enabled for remote access to Epic-hosted environments including the internet.

Verified compensating controls when remote access is allowed without MFA:
a) Perimeter authentication is used to verify for both client registration and user authentication where applicable.
b) For limited-time perioding outages, compensating controls are implemented as feasible, and single factor remote access is disabled after precipitating issues are resolved.

User Provisioning and User Activity Monitoring
Verified:
a) Access is properly authorized and provisioned for all Epic-hosted environments (e.g., Production, Test, Training).
b) Provisioning includes both account provisioning, such as via Active Directory, and provisioning of access within the Epic applications, such as Epic application administrative (including generic accounts) and user-level security classes (assets).
c) Periodic access reviews are conducted for both Epic user and administrative accounts.

Verified Epic users:
a) Are assigned unique user accounts.
b) Instructed not to share credentials.
c) Follow password requirements (i.e., length, complexity, expiration, rotation) for standard and generic accounts and configured according to industry standards.
d) Are provided user security education and training, including recognizing phishing attacks and how to report potential security incidents.

Verified generic accounts:
a) Are authorized and reviewed for specific use such as automated services or emergency access.
b) Are configured with strong authentication according to Epic security standards.
c) Used only from trusted network or authorized domains, except for clinical workstation or application deployment prior to end user authentication with Epic personal credential.
d) Are not used in the environment containing PHI unless authorized.
e) For non-PHI environment such as Training environments, users log in from trusted network first, or authenticate with a name user account prior to using generic account.
f) Follow password requirements (i.e., length, complexity, expiration, rotation) for standard and generic accounts are configured according to industry standards.

Verified monitoring of access, access attempts, and appropriate use of Epic applications by users, and prompt investigation of any suspected inappropriate access.

Third-Party Integrations
Verified third-party integrations that send or receive sensitive data to and from Epic-hosted environments are configured securely:
a) Written authorization for configurations that do not conform to Epic's data protection standards.

b) Documentation of risk acceptance for non-standard configurations.
c) Communication and approval of cost estimates for additional services related to integration.

Obtained the list of Epic installed third-party products or integrations during the audit period and verified:
a) Necessary support licenses/contracts are maintained.
b) Coordination with Epic to configure, update, and patch third-party products installed in Epic-hosted environments.
c) Vendor contacts and escalation points with third parties are maintained.
d) Third-party connections into the Epic-hosted environment are monitored and reviewed.
e) Known critical security issues with third-party products during the audit period were escalated, investigated, and addressed with Epic's involvement within a reasonable timeframe based on risk.

Incident Reporting
Verified all security incidents during the audit period that were detected by UTHealth and could impact the Epic hosted environment or infrastructure were reported to Epic.

Obtained a list of all security incidents reported by Epic during the audit period and verified coordination with Epic throughout the entire incident lifecycle.

Physical Security
Verified devices and infrastructure that connect users to Epic-hosted environments are physically secured.

Verified all security incidents during the audit period that were detected by UTHealth and could impact the Epic hosted environment or infrastructure were reported to Epic.

Infrastructure Security
For UTHealth infrastructure residing within Epic's data centers that UTHealth maintains, verified:
a) Necessary support licenses are maintained.
b) Infrastructure is configured, updated, and patched with Epic's involvement.

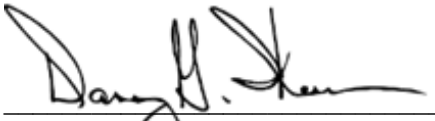
Verified all security incidents during the audit period that were detected by UTHealth and could impact the Epic hosted environment or infrastructure were reported to Epic.

Epic Application and Infrastructure Configuration
Verified security-enhancing software featuring cybersecurity initiatives are reviewed, prioritized, and implemented, or that alternate Epic-recommended best practice security configurations are applied.

Scope Period
December 1, 2024, through November 30, 2025

Conclusion
Based on the procedures performed, UTHealth complies with the Standards.

We would like to thank the Healthcare IT and IT Security staff and management who assisted us during the engagement.



Daniel G. Sherman, MBA, CPA, CIA
Vice President & Chief Audit Officer

NUMBER OF PRIORITY OBSERVATIONS REPORTED TO UT SYSTEM
None

MAPPING TO A&AS FY26 RISK ASSESSMENT

Reference	Risk
None	Not applicable – This is a required annual compliance audit.

DATA ANALYTICS UTILIZED
Not Applicable

ENGAGEMENT TEAM
VP/CAO – Daniel G. Sherman, MBA, CPA, CIA
Supervisor – Brook Syers, CPA, CIA, CISA
Staff – Lieu Tran, CISA

END OF FIELDWORK DATE
February 11, 2026

ISSUE DATE
February 16, 2026

REPORT DISTRIBUTION
Audit Committee
Dr. Olasunkanmi Adeyinka
Richard Anselme
Bassel Choucair
Mary Dickerson
Kevin Dillon
Dr. Babatope Fatuyi
Dr. James Griffiths
Tariq Khan
Tony Murry
Ana Touchstone
Amar Yousif