UTHealth Houston

Auditing and Advisory Services

P.O. Box 20036 | Houston, TX | 713-500-3160

Epic Security Certification

#HSC25RQ0001

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 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/Scope

We conducted a risk-based analysis in order to determine general compliance with the Standards. For this engagement, our objectives were to determine whether:

- Anti-virus/anti-malware software and patches are installed for UTHealth-managed servers and devices.
- Timeouts are configured in accordance with risk assessments and regulatory requirements.
- Observed/reported deficiencies are remediated within a reasonable timeframe based on risk.
- For devices not managed by UTHealth:
    - System access is through an Epic Hosting-provided public access gateway or UTHealth-managed virtual desktop/application technology that meets patching and anti-virus/anti-malware requirements.
    - Users are unable to mount or access drives in the Epic Hosting environment or access endpoint storage.
    - Acceptable use policies are implemented.
- Access is verified, provisioned, and revoked accordingly for account provisioning, Epic access authorizations, and different environments.
- Individuals are assigned unique user accounts and instructed not to share credentials.
- Users are provided user security education and training.
- Generic accounts are restricted, monitored, configured for strong authentication, unable to access Epic-hosted environments from untrusted networks, and are not used for environments containing PHI.
- Access, access attempts, and appropriate use of Epic is monitored and suspected inappropriate access is promptly investigated.
- Two-factor authentication is used for remote access.

Epic Security Certification

- Network access to Epic environments is restricted to necessary portions of the UTHealth network and network traffic into Epic is analyzed on the firewall.
- Third-party products have appropriate support licenses/contracts, are configured, updated, and patched, and contacts and escalation points are maintained.
- Third-party connections into Epic-hosted environments are monitored and reviewed.
- Security incidents/issues around devices, infrastructure, and third-party products are identified, coordinated with Epic, and resolved.
- Third-party integration that sends/receives sensitive data to/from Epic-hosted environments are configured securely and are authorized and requested by UTHealth.
- For Epic infrastructure residing within Epic's data centers that UTHealth maintains, necessary support licenses are maintained and infrastructure is configured, updated, and patched.
- Software features that enhance/strengthen security of the Epic environment are implemented.

Scope Period
December 1, 2023 through November 30, 2024

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

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

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

OBSERVATION RATINGS

Priority	An issue that, if not addressed timely, has a high probability to directly impact achievement of a strategic or important operational objective of UTHealth or the UT System as a whole.
High	An issue considered to have a medium to high probability of adverse effects to a significant office or business process or to UTHealth as a whole.
Medium	An issue considered to have a low to medium probability of adverse effects to an office or business process or to UTHealth as a whole.
Low	An issue considered to have minimal probability of adverse effects to an office or business process or to UTHealth as a whole.

NUMBER OF PRIORITY OBSERVATIONS REPORTED TO UT SYSTEM
None

MAPPING TO A&AS FY25 RISK ASSESSMENT

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

DATA ANALYTICS UTILIZED
None

ENGAGEMENT TEAM
VP/CAO – Daniel G. Sherman, MBA, CPA, CIA
Supervisor – Brook Syers, CPA, CIA, CISA, CFE
Staff – Tammy Coble, CISA

END OF FIELDWORK DATE
March 5, 2025

ISSUE DATE
March 11, 2025

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