21-118 Epic Security Certification

We have completed our audit of the Epic Security Certification. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

BACKGROUND

Once implemented at UTHealth, the Epic environment will be 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. As Epic has not been fully implemented, A&AS reviewed current policies and procedures to verify compliance with the Standards ahead of the May 2021 go-live date.

OBJECTIVES

The objective of this audit was to verify current policies and procedures are in compliance with the Standards outlined in the Agreement.

SCOPE PERIOD

The scope period was as of September 30, 2020.

METHODOLOGY

The following procedures were performed:

- For UTHealth-managed end point devices, verified current policies and procedures require anti-virus/anti-malware software to be installed and kept up-to-date, end points to be patched regularly and critical security patches applied in a timely fashion, and end point timeouts to be configured in accordance to risk assessments and regulatory requirements.
- For devices that UTHealth cannot fully manage, verified acceptable use policies are in place that state the same requirements as UTHealth-managed devices.
- Verified policies and procedures regarding incident reporting between Epic and UTHealth have been established.
- Verified current policies and procedures require:
    - Updates to the host configuration environment and address physical security.
    - User accounts to be assigned to individuals and individuals are instructed not to share credentials for any reason.
    - Passwords to be of a specific and reasonable length, complexity, and rotated, following industry standards.

  - Access to be verified, provisioned, and revoked accordingly, for both account provisioning and access authorization within applications.
  - Generic accounts to be restricted, monitored, configured for strong authentication, and access restricted through untrusted networks.
  - Unique credentials to access the UTHealth network and multifactor authentication for remote access to hosted environments containing PHI over untrusted networks.
  - Third-party products to have appropriate support licenses and contacts, and be configured, updated, and patched per the vendor's or UTHealth's requirements.
  - Vendor contracts and escalation points with any third party be maintained.
  - Use of third-party connections into environments containing PHI to be monitored and reviewed.
- For environments containing PHI, verified policies and procedures:
  - Restrict the usage of generic accounts.
  - Address access, access attempts, monitoring of appropriate use, and investigation of suspected inappropriate access.
  - Address access to different environments (Production, Test, Training, etc.) is provisioned, reviewed, and revoked.
  - Restrict network access to only necessary portions of the UTHealth network, and network traffic is reviewed and restricted through firewalls.
  - Require secure configuration of third-party integrations such as web services that send or receive sensitive data to or from hosted environments.
  - Require use of third-party connections into environments containing PHI to be monitored and reviewed.

AUDIT RESULTS

Based on our procedures, UTHealth's current policies and procedures are in compliance with the Standards outlined in the Agreement. Once Epic has gone live, we will verify those policies and procedures are implemented for the Epic environment.

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

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

NUMBER OF PRIORITY FINDINGS REPORTED TO UT SYSTEM

None.

MAPPING TO FY 2021 RISK ASSESSMENT

Risk (Rating)	Not applicable.

DATA ANALYTICS UTILIZED

Data Analytic #1	Not applicable.

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

AVP/CAO	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook Syers, CPA, CIA, CISA, CFE
Auditor Assigned	Tammy Coble, CISA
End of Fieldwork Date	October 27, 2020
Issue Date	November 4, 2020

Copies to:
Audit Committee
Amar Yousif
Dr. Babatope Fatuyi
Beverly Moore