
Date: June 16, 2023

To: Dr. Robert Hromas, Dean, Long School of Medicine
Dr. Robert Leverence, Exec Vice Dean-Clinical Affairs -UTHP ADM CMO


From: John Lazarine, Chief Audit Executive
Internal Audit & Consulting

Subject: *Audit Report – Audit of Epic Application - Access Provisioning
(Providers & Nurse Practitioners)*

As part of our FY23 Audit Plan, we completed an audit of *Epic Application - Access Provisioning (Providers & Nurse Practitioners)*. This audit identified no audit issues, and the conclusion is summarized in the “Summary of Results” section of the report.

We appreciate the cooperation and assistance we received from UTHP Health-IT management throughout the review.

Respectfully,



John Lazarine, CIA, CISA, CRISC
Chief Audit Executive
Internal Audit & Consulting Services

Distribution:

cc: Dr. William Henrich, President
Andrea Marks, Senior Executive Vice President, and Chief Operating Officer
Ginny Gomez-Leon, Vice President, and Chief Financial Officer
Yeman Collier, Vice President, and Chief Information Officer
Todd Holling, Deputy Chief Information Officer
Dr. Edward Sankary, Chief Health Information & Value Officer
Julie Wingate, Asst. VP, Clinical Systems
Wayne Laskie, Director, Clinical System Technical Infrastructure
Sarah Cook, Director, Clinical Information Systems
J. Michael Peppers, Chief Audit Executive, UT System

External Audit Committee Members:

Randy Cain
Carol Severyn
Ed Garza

Audit Report (23-09)
Audit of Epic Application – Access Provisioning
(Providers & Nurse Practitioners)
June 12, 2023

Executive Summary

Background

Epic is a leading provider of electronic health records software utilized by UT Health Physicians (UTHP). The system is an integrated platform for most areas of care with numerous developed modules.

The original audit title and objectives communicated in the audit plan were updated due to the ongoing Epic projects. These are Epic application upgrades, Epic hosting migration, and Hyperdrive migration. The control domain was assessed to determine areas for process improvement, existing control enhancement, and addressing identified IT risks. The data at risk includes but is not limited to, patient health records and billing information.

Objective & Scope

An audit of the Epic Application access provisioning process was completed, focusing on Providers and Nurse Practitioners (NP) at UTHP. The primary objective of this audit was to determine whether logical access to Epic Application programs and data is restricted to properly authorized individuals.

The scope of this audit focused on Epic access provisioning for “Providers” and “NP” during FY 2023¹.

Methodology

The audit was conducted by reviewing the access provisioning process for Providers and NPs. Policies, procedures, and controls related to the access provisioning process were reviewed. In addition, key stakeholders responsible for the access provisioning process, including Epic Security IT staff, and Cadence Team were interviewed.

Sample testing of the access provisioning process was completed to assess its effectiveness.

This audit was conducted in accordance with the Institute of Internal Auditors’ *International Standards for the Professional Practice of Internal Auditing*. In addition, this audit satisfies the TAC 202² requirement of the biennial review, as set forth by the State of Texas and UT System Administration.

Summary of Results

Overall, we determined the access provisioning control was suitably designed and operated effectively throughout the period from September 1, 2022, to January 31, 2023, thereby achieving the access provisioning control objective, “Controls provide reasonable assurance that logical access to Epic Application programs and data is restricted to properly authorized individuals.”

During the course of this engagement, the following opportunities to further enhance the access provisioning process for Providers and NPs were identified and shared with management:

¹ Fiscal Year 2023 (September 1, 2022 – August 31, 2023)

² Texas Administrative Code Chapter 202 (TAC §202), RULE §202.76 (c) A review of the institution's information security program for compliance with these standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the institution of higher education head or his or her designated representative(s).

- Ensure that all required documentation is completed and includes the justification for access and the level of access required.
- Ensure consistency and centralization of the access provisioning process from the initiation of the access to granting the access.
- Ensure consistency in the design of linkable templates assigned to requested access to address the risk of segregation of duties in the logical access environment.

By implementing the recommended improvements, the organization can reduce the risk of unauthorized access to patient information and ensure that only authorized individuals have access to the Epic application.

Management has agreed with the results of this audit. We would like to thank UTHP Health-IT management and staff for the support and assistance provided during this audit.

AUDIT TEAM

Samuel Babajide, IT Audit Director, MSEM, CISA, CIPT, CPSP, ITIL

APPROVED FOR RELEASE



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

DISTRIBUTION

Dr. William Henrich, President
Andrea Marks, Senior Executive Vice President, and Chief Operating Officer
Ginny Gomez-Leon, Vice President and Chief Financial Officer
Yeman Collier, Vice President, and Chief Information Officer
Todd Holling, Deputy Chief Information Officer
Dr. Edward Sankary, Chief Health Information & Value Officer
Julie Wingate, Asst. VP, Clinical Systems
Wayne Laskie, Director, Clinical System Technical Infrastructure
Sarah Cook, Director, Clinical Information Systems
J. Michael Peppers, Chief Audit Executive, UT System

Criteria

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, and the Control Objectives for Information and Related Technologies (COBIT). Using a centrally managed controls catalog effectively ensures that all agencies and institutions use common language and minimum standards when implementing security measures.

Testing Methodology and Results

Internal Audit utilized TAC §202 SCSC as part of the validation testing to determine control was suitably designed and operated effectively. The results of the test work are summarized above:

- **(*) Risk and Risk Ranking** *(as to its impact on UTHP Operations in the absence of adequate controls)*
 - **Red** = High Risk
 - **Yellow** = Medium Risk
 - **Green** = Low Risk
- **Mitigating Control** *(as defined in TAC §202 Security Controls Standards Catalog)*
- **Control Status**
 - **Red** = Control is not in place and/or not working
 - **Yellow** = Control is in place and is not reliable
 - **Green** = Control is in place and operating effectively

**Summary of the Audit of Epic ITGCs Testing Results:
IT Processes Evaluation**

#	Risk	Risk Ranking *	Mitigating Control	Control Status
1	Users of the IT environment are not authorized because (i) requests for removal of unneeded access of IT personnel are not made timely, and (ii) access action requests are fulfilled inaccurately or untimely.		New/Modified User Set-up <i>TAC 202, SCSC AC-2, AC-3 & AC-5 COBIT, APO13</i>	