SUMMARY

BACKGROUND

The University of Texas (UT) Health Intelligence Platform (UT-HIP) is a UT System-wide program sponsored by the UT System Administration Office of Health Affairs that is designed to integrate data and technology to gain insights that will improve patient care and the health of the populations served by UT institutions and reduce the overall cost of health care across the UT System.

UT-HIP provides a cloud-based application accessible to participating UT System health institutions, which is managed by UT Health Science Center at Houston in collaboration with UT Medical Branch at Galveston (UTMB) and governed by representatives from participating institutions. Due to the sensitive nature of the electronic patient health information (ePHI) processed by UT-HIP, strong data security controls must be in place. To ensure security of UT-HIP data, the UT-HIP program is applying the HITRUST Framework (HITRUST CSF) to identify data protection and data security related risks to sensitive data, guide data protection measures, and meet regulatory compliance obligations.

This engagement is part of the fiscal year (FY) 2024 Annual Audit Plan and was selected based on the risks associated with a security breach or inappropriate access to sensitive ePHI in UT-HIP.

OBJECTIVE

The objective of this engagement was to assess the design and effectiveness of data classification and data security controls for UT-HIP and evaluate compliance with any applicable Federal and State regulations and UT System policies including, but not limited to, Texas Administrative Code §202 Security Control Standards, UT Systemwide Policy 165: Information Resources Use and Security standards, and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule standards.

CONCLUSION

Overall, UT-HIP has sufficient procedures, processes, and controls in place to ensure the security and protection of sensitive data. UT-HIP has made significant efforts to implement the HITRUST CSF. An opportunity exists to further strengthen processes and controls by performing periodic testing of backup and restoration procedures. Additional opportunities that were identified and resolved by management during the audit include:

- Identification of ePHI in the asset inventory;
- Implementation of multi-factor authentication;
- Implementation of enhanced email security;
- Enhancement of change management procedures and documentation; and
- Update of audit log retention and password configurations to agree with documented policies.

OBSERVATION

1 Medium	Testing backup restoration procedures of UT-HIP at least annually will help ensure that the system can recover sufficiently and timely from disruptions that would initiate the activation of recovery plans.

Management developed an action plan to incorporate the System Audit Office recommendation to address this observation and anticipates implementation by September 30, 2024.

OBSERVATION 1
MEDIUM

Backup Testing:
Annual Restoration Testing of Information Systems

Testing backup restoration procedures of UT-HIP at least annually will help ensure that the system can recover sufficiently and timely from disruptions that would initiate the activation of recovery plans.

UT Systemwide Policy 165, Standard 6: Backup and Disaster Recovery and Texas Administrative Code (TAC) §202.76 security control standard CP-4, Contingency Plan Testing, require that backup plans must incorporate procedures for testing backup and recovery procedures. A periodic test of backup and restoration procedures is intended to provide assurance that agreed upon recovery time and recovery point objectives can be achieved in the event of a system failure, cyber-attack, or data center disruption that results in the loss of data. Restoration procedures should be tested at least annually to verify backup reliability and information integrity; and to ensure that systems can adequately recover from any type of disruption that would cause the activation of recovery plans. At the time of the audit, a test of backup and restoration procedures had not yet been performed.

ACTION PLAN

UT-HIP will conduct a restoration test and continue to perform a test of the recovery plan at least annually.

Anticipated Implementation Date: September 30, 2024

METHODOLOGY

This engagement was performed on our behalf by EisnerAmper LLP, and in accordance with the *International Standards for the Professional Practice of Internal Auditing* and generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the engagement to obtain sufficient, appropriate evidence to provide a reasonable basis for our observations and conclusions based on our objectives. We believe that the evidence obtained provides a reasonable basis for our observations and conclusions based on our objectives. The System Audit Office is independent per GAGAS requirements for internal auditors.

SCOPE AND PROCEDURES

The scope of this engagement was the UT-HIP Microsoft Azure environment and its dependencies, which are managed by the UT-HIP organization, and the policies, procedures, and practices in place at the time of the audit. The scope did not include any systems managed by other entities within UT System Administration or by UT institutions. Audit procedures included, but were not limited to, interviewing control owners and management of UT-HIP and UTMB, reviewing available documentation to confirm the design and operating effectiveness of data classification and data security, and limited testing where possible. Selected HITRUST CSF controls were evaluated to ensure that the UT-HIP program has implemented best practices to withstand common cybersecurity threats and protect the integrity and confidentiality of ePHI.

We will follow up on action plans in this report to determine their implementation status. We validate implementation of action plans for Priority- and High-level observations and review and rely on written affirmation from the responsible department to track completion of action plans for Medium- and Low-level observations. This process will help enhance accountability and ensure that timely action is taken to address the observations.

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 System Administration 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 System Administration 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 System Administration as a whole.
Low	An issue considered to have minimal probability of adverse effects to an office or business process or to System Administration as a whole.

CRITERIA

- Texas Administrative Code §202.76, Security Control Standards Catalog v. 2.1
- UT Systemwide Policy 165: Information Resources Use and Security Policy
- HITRUST Common Security Framework
- HIPAA Security Rule CFR §164.308

REPORT DATE

September 17, 2024

REPORT DISTRIBUTION

To: Zain Kazmi, Associate Vice Chancellor and Chief Digital and Analytics Officer
Cc: John Zerwas, MD, Executive Vice Chancellor for Health Affairs
Lori McElroy, Chief Information Security Officer
Dan Sherman, Chief Audit Executive, UT Health Science Center at Houston
ShuRon Green, Executive Director, UT Health Science Center at Houston
Desolyn Foy, Chief Audit Executive, UT Medical Branch at Galveston
John Flores, Associate Vice President Information Security and Chief Information Security Officer, UT Medical Branch at Galveston
UT System Administration Internal Audit Committee
External Agencies (State Auditor, Legislative Budget Board, Governor's Office)