TEXAS
The University of Texas at Austin

Health Insurance Portability and Accountability Act (HIPAA)

The University of Texas at Austin

December 2022

Office of Internal Audits
UT Austin's Agents of Change

Executive Summary

Health Insurance Portability and Accountability Act

Data Privacy and Security
Project Number: 22.005

Audit Objective

The objective of the audit was to evaluate Health Insurance Portability and Accountability Act (HIPAA) privacy processes, security controls, and breach incident practices to determine whether policies and processes provide for compliance with federal requirements.

The review included the six provider covered components designated by The University of Texas at Austin (UT Austin). Per the designation, Dell Medical School (UT Health Austin) is treated as a separate entity with its own privacy officer. As such, Dell Medical School was not included in the scope of this engagement.

Conclusion

UT Austin is partially compliant with HIPAA privacy and security requirements and has opportunities to implement policies and processes to establish full compliance.

Audit Observations[1]

Recommendation	Risk Level	Estimated Implementation Date
HIPAA Privacy and Security Officer Roles	High	May 2023
Security Risk Analysis and Management	High	May 2023
Breach Notification Procedures	High	May 2023
Business Associate Agreements	Medium	May 2023
Privacy Monitoring	Medium	May 2023
Designation of Covered Components	Medium	May 2023
HIPAA Training	Medium	May 2023

Engagement Team[2]

Mr. Jeff D. Bennett, CISA, CISSP, CCSFP, IT Audit Associate Director
Mr. Paul Douglas, CISA, CCSFP, CDPSE, IT Audit Director
Ms. Laura Walter, IT Audit Consultant

[1] Each observation has been ranked according to The University of Texas System Administration (UT System) Audit Risk Ranking guidelines. Please see the last page of the report for ranking definitions.

[2] This project was co-sourced with Postlethwaite & Netterville, APAC (P&N)

Detailed Audit Results

Observation #1 HIPAA Privacy and Security Officer Roles

Although UT Austin has designated its HIPAA Privacy and Security Officers, UT Austin does not have a cohesive approach across covered components, and specific roles, responsibilities, and resource requirements have not been defined. Without a defined approach to ensure compliance with key HIPAA security and privacy requirements, UT Austin may experience reputational loss and incur fines for non-compliance.

Recommendation: UT Austin should establish an operating model (central or hybrid) that defines key responsibilities and authority to the appropriate personnel responsible for HIPAA compliance across campus. This would include monitoring/reporting on the status of HIPAA compliance as well as providing guidance and/or assistance in the implementation of HIPAA requirements.

Management's Corrective Action Plan: To date, the University has not established a formal and cohesive HIPAA compliance program, in the true sense of the word "program". Compliance with regulatory requirements has been managed decentrally through limited resources across campus. The Chief Compliance Officer (CCO) and Chief Information Security Officer (CISO) believe that to practically implement the recommendation would necessitate the creation of a centralized HIPAA compliance program and believe implementation would be best achieved by a central operating model, but a final decision has yet to be made about the appropriate model to institute. We will provide executive leadership with additional information by December 9, 2022 to facilitate decision regarding the long-term approach to a HIPAA compliance program.

Responsible Persons: HIPAA Privacy Officer and HIPAA Security Officer

Planned Implementation Date: May 2023

Observation #2 Security Risk Analysis and Management

Covered components have not met the HIPAA Security Rule implementation specifications for performing a security risk analysis (SRA). A thorough SRA is a foundational requirement for a covered entity to ensure compliance with the Security Rule and to understand risks to electronic protected health information (ePHI). Furthermore, covered components do not have a formal risk management plan in place to manage security risks to ePHI. Because the covered components do not have appropriate risk analyses, they were not able to link security plans to the management of identified risks. Without risk management, there is no foundation upon which an entity's necessary security activities are built.

An SRA should include all applications that create, receive, transmit and/or store ePHI. Because a comprehensive SRA has not been performed, the covered components' environments could be vulnerable to unknown security gaps and risks to ePHI data and systems. Furthermore, covered components may have difficulty defending its security posture and presenting required documentation during an Office for Civil Rights (OCR) audit or investigation. OCR could assess monetary penalties and resolution agreements if gaps are identified.

UT Austin Minimum Security Standards require covered components to identify all assets that are used to process, view, modify, store, or otherwise interact with ePHI. Currently, covered components leverage UT Austin's Information Security Office (ISO) for their security management processes. The ISO makes available a risk assessment tool, ISORA, which has the capability to populate HIPAA-related questions; however, ISORA is not configured to address HIPAA regulatory requirements. The ISO security management processes provide direction for security in place but do not fully ensure that covered components are fulfilling their regulatory responsibilities to safeguard ePHI.

Recommendation: Covered components should complete and document a formal SRA in accordance with the requirements of the HIPAA Security Rule. Based on guidance provided by the US Department of Health and Human Services (HHS) and the OCR, the risk analysis should include documentation of the following key elements:

- Scope of analysis
- Data collection
- Identify and document potential threats and vulnerabilities
- Assess current security measures
- Determine the likelihood of threat occurrence
- Determine the potential impact of threat occurrence
- Determine level of risk

The responsibility of the SRA should be defined, and each covered HIPAA component should participate in the analysis to ensure each unit understands and complies with risk analysis requirements to safeguard ePHI.

Management should develop and implement a risk management plan that outlines controls to reduce risks and vulnerabilities to an acceptable level. Controls should be a combination of policies, procedures, and technologies implemented to safeguard sensitive/critical data as identified by the risk analysis.

Finally, UT Austin should provide clear guidance to the covered components related to the implementation of HIPAA requirements (e.g., templates and/or tools utilized to successfully inventory and maintain all assets that interact with ePHI data).

Management's Corrective Action Plan: The Information Security Office Risk Assessment tool (ISORA) has the capability to include HIPAA questions for covered units. A custom HIPAA assessment for covered entities will be created in the ISORA platform and will be completed annually in addition to the standard annual campus-wide IT risk assessment. These assessments will be able to roll-up so that an overall campus HIPAA compliance score and maturity model can be reviewed. Furthermore, the Information Security Office will assess specific assets that have PHI, based on the fact that covered entities are required to account for their inventory in ISORA, and maintain a risk register for each covered component.

Responsible Person: HIPAA Security Officer

Planned Implementation Date: May 2023

Observation #3 Breach Notification Procedures

Covered entities could not demonstrate the process or procedures (i.e., breach risk assessment and related notifications) they perform following a breach of protected health information. One of the covered entities was not able to provide evidence of notification after a breach that occurred in 2019.

Recommendation: UT Austin should document procedures outlining responsibilities and actions to be performed in the event of a breach. Procedures should align with HIPAA breach notification requirements, which includes the process for performing a breach risk assessment for incidents involving PHI. One resource for consideration when documenting procedures is for covered components to utilize the breach notification plan located on the ISO's website.

Management's Corrective Action Plan: The HIPAA Privacy Officer plans to implement a University Compliance Services (UCS) HIPAA website that would include information on reporting breaches. In addition, UCS plans to formalize intakes so that the reports are reviewed, necessary action is determined and taken, and the process is monitored and documented.

Responsible Person: HIPAA Privacy Officer

Planned Implementation Date: May 2023

Observation #4 Business Associate Agreements (BAA)

One of six contracts selected for testing did not have an associated BAA. The HIPAA Security Rule mandates that a BAA is executed (between the covered component and the business associate/third party) prior to granting authorization to access PHI. Failure to execute a BAA with a business associate could limit UT Austin's options for legal recourse in the event of a breach at the third party.

Recommendation: Management should ensure a BAA is executed prior to authorizing access to PHI. The BAA should outline the PHI being disclosed, the permissible uses and disclosures of PHI, and responsibilities as it relates to the covered component and the business associate.

Management's Corrective Action Plan: Management agrees this needs to be implemented. Implementation will require cooperation with Business Contracts. Full implementation would require review of all units' business processes to determine whether there are other contracting methods, e.g., PO's, that would need to be captured and brought into compliance. Management will explore the possibility of using ISORA to track and monitor need for and use of BAAs.

Responsible Person: HIPAA Privacy Officer working with Business Contracts

Planned Implementation Date: May 2023

Observation #5 Privacy Monitoring

Covered components are not proactively monitoring (e.g., defined regular reviews) access logs for unauthorized access to patient records and/or other ePHI. Therefore, covered components may not be able to determine whether ePHI is used or disclosed in an inappropriate manner. In addition, covered components may not be able to identify information security system activity for indicators of a breach.

Recommendation: UT Austin should establish a policy that indicates what reviews should be conducted and any procedures to specify how reviews will be performed. Furthermore, management should consider leveraging the Patient-Privacy-Monitoring (PPM) module of Splunk for monitoring logs since this practice is already implemented for Dell Medical School.

Management's Corrective Action Plan: Procedures will be put in place to specify what reviews will be done by the covered components and establish a schedule for doing so. Splunk will be used for monitoring.

Responsible Person: HIPAA Privacy Officer and HIPAA Security Officer

Planned Implementation Date: May 2023

Observation #6 Designation of Covered Components

UT Austin's list of covered components is not up-to-date and does not account for the closing of the pharmacy and the addition of the Stress and Anxiety clinic. As outlined in observation #1, the lack of a cohesive approach impacts compliance with key HIPAA security and privacy requirements. Without a complete understanding of the HIPAA covered components, UT Austin may incur fines for non-compliance, experience reputational loss, and negatively impact the patient experience.

Recommendation: Management should implement a process that ensures HIPAA-related requirements have been met and relevant documentation is updated in a timely manner.

Management's Corrective Action Plan: Management will implement a process to ensure the ISO has an updated list of units (by department code) to ensure the appropriate security tools and services are utilized.

Responsible Person: HIPAA Privacy Officer and HIPAA Security Officer

Planned Implementation Date: May 2023

Observation #7 HIPAA Training

UT Austin processes do not ensure that covered components monitor that individuals granted access to PHI complete the required HIPAA training. Furthermore, covered components have no process to monitor and document those individuals interacting with PHI.

Because UT Austin is a hybrid entity, the HIPAA training regulations and requirements only apply to the covered components on campus. Therefore, without defining the individuals interacting with PHI, the covered components cannot ensure that required HIPAA training is completed.

Recommendation: UT Austin should implement a monitoring process for HIPAA training requirements. Management should also consider defining and documenting which individuals are interacting with PHI.

Management's Corrective Action Plan: Procedures will be implemented to ensure that the covered units identify all personnel that need HIPAA training and provide University Compliance Services with the lists and update them annually.

Responsible Person: HIPAA Privacy Officer

Planned Implementation Date: May 2023

Conclusion

UT Austin is partially compliant with HIPAA privacy and security requirements and has opportunities to implement policies and processes to establish full compliance. The following table provides a summary of the audit results.

Table: Controls Assessment

Audit Objective	Controls Assessment
Evaluate privacy processes to determine compliance with federal and state requirements.	Limited effectiveness with compliance opportunities.
Evaluate security controls to determine compliance with federal and state requirements.	Limited effectiveness with compliance opportunities.
Evaluate breach incident practices to determine compliance with federal and state requirements.	Limited effectiveness with compliance opportunities.

A sample of HIPAA Security, Privacy, and Breach Notification requirements were selected as part of the audit. Detailed compliance results were provided to each covered component and the HIPAA Privacy Officer and HIPAA Security Officer during the engagement.

Background

HIPAA is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. UT Austin is a hybrid entity under the HIPAA Privacy Regulations and has covered components that provide covered healthcare services. The University also has other offices that provide business support to the covered healthcare providers, and these business support offices have or may have access to protected medical and health information.

Scope, Objectives, and Methodology

This audit was conducted in conformance with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. Additionally, we conducted the audit in accordance with Generally Accepted Government Auditing Standards and meet the independence requirements for internal auditors. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions on our audit objectives.

The scope of this review included the following healthcare provider covered components designated [3]by UT Austin:

1. University Health Services
2. Counseling and Mental Health Center
3. The College of Communication's Speech and Hearing Center
4. The School of Nursing's Children's Wellness Clinic
5. The School of Nursing's Family Wellness Clinic
6. Intercollegiate Athletics' Sports Medicine Department

Specific audit objectives and the methodology to achieve the objectives are outlined in the table below.

Table: Objectives and Methodology

Audit Objective	Methodology
Evaluate privacy processes to determine compliance with federal and state requirements.	• Reviewed policy and procedure documents specific to privacy monitoring, electronic medical record system certifications, and right to access requests. • Completed UT Learn HIPAA training. • Reviewed HIPAA training logs for completion. • Conducted client interviews.
Evaluate security controls to determine compliance with federal and state requirements.	• Tested a sample of user security reports, configuration/authentication parameters, multi-factor authorization. • Tested a sample of contracts for BAA.
Evaluate breach incident practices to determine compliance with federal and state requirements.	• Interviewed the University's Chief Compliance Officer and covered components. • Reviewed existing breach notification procedures and documents.

[3] Per the designation, Dell Medical School (UT Health Austin) is treated as a separate entity with its own privacy officer. As such, Dell Medical School is not included in the scope of this engagement.

Criteria

45 CFR Part 164 – Security and Privacy
Subpart A – General Provisions
Subpart C – Security Standards for the Protection of Electronic Health Information
Subpart D – Notification in the Case of Breach of Unsecured Protected Health Information
Subpart E – Privacy of Individually Identifiable Health Information

Excerpts:

45 CFR § 164.530 Administrative Requirements (a)

(a) (1) Standard: Personnel designations.

(i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.
(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(a) (2) Implementation specification: Personnel designations. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

45 CFR § 164.308(a)(2) Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

45 CFR § 164.308 Administrative safeguards. (a) A covered entity or business associate must, in accordance with § 164.306:

(1)
(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.
(ii) Implementation specifications:

(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

45 CFR §164.308(a)(1)(ii)(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

45 CFR §164.306(a) General requirements. Covered entities and business associates must do the following:

> (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

45 CFR § 164.404 Notification to individuals. (a) Standard (1) General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

45 CFR § 164.414 Administrative requirements and burden of proof.

> (a) Administrative requirements. A covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.
>
> (b) Burden of proof. In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.

Observation Risk Ranking

Audit observations are ranked according to the following definitions, consistent with UT System Audit Office guidance.

Risk Level	Definition
Priority	If not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of The University of Texas at Austin (UT Austin) or the UT System as a whole.
High	Considered to have a medium to high probability of adverse effects to UT Austin either as a whole or to a significant college/school/unit level.
Medium	Considered to have a low to medium probability of adverse effects to UT Austin either as a whole or to a college/school/unit level.
Low	Considered to have minimal probability of adverse effects to UT Austin either as a whole or to a college/school/unit level.

In accordance with directives from UT System Board of Regents, Internal Audits will perform follow-up procedures to confirm that audit recommendations have been implemented.

Report Submission and Distribution

We appreciate the courtesies and cooperation extended throughout the audit.

Respectfully Submitted,

Sandy Sutton Jansen

Sandy Jansen, CIA, CCSA, CRMA, Chief Audit Executive

Dr. Jay C. Hartzell, President
Mr. Darrell Bazzell, Senior Vice President and Chief Financial Officer
Mr. Cam Beasley, Chief Information Security Officer
Mr. Jeff Graves, Chief Compliance Officer and Privacy Officer
Ms. Monica Horvat, Director of Presidential Priorities
Ms. Melissa Loe, Chief of Staff, Financial and Administrative Services

The University of Texas at Austin Institutional Audit Committee
The University of Texas System Audit Office
Legislative Budget Board
Governor's Office
State Auditor's Office