UT Health
San Antonio
Internal Audit &
Consulting Services

Internal Audit & Consulting Services
7703 Floyd Curl Dr. MC#7974
San Antonio, Texas 78229-3900
210-567-2370 Fax: 210-567-2373
www.uthscsa.edu

Date: April 25, 2019

To: Dr. Peter Loomer, Dean, School of Dentistry

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

Subject: Audit Report – Axium Application Review (Backup and Recovery)

As part of our FY 2018 Audit Plan, we recently completed the Axium Application Review Backup and Recovery. Attached is the report detailing the results of this review. Management's Action Plans are included in the report.

We appreciate the cooperation and assistance we received from the School of Dentistry throughout the review.

Respectfully,

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

Distribution:

cc: Dr. William Henrich, President
Michael Black, Sr. EVP & COO
Andrea Marks, VP & CFO
Yeman Collier, VP & CIO
Jessica Saldivar, Chief Compliance Officer
Jack Park, Chief Legal Officer
Dr. Gary Guest, Associate Dean, School of Dentistry
Carol Nava, Senior Manager, Information Systems Operations
Janet Rivera, Manager, Patient Mgmt. & Business Office

External Audit Committee Members:
Pat Frost
Regina Conklin
Ed Garza
Brian Kelly

Axium Application Review (Backup and Recovery) (Project # 18-06)

April 25, 2019

John Lazarine, CIA, CISA, CRISC
Chief Audit Executive

Internal Audit Staff:

Robert Morgan, IT Audit Director, CISA, CISSP, GSNA, OCP

Executive Summary

As part of our approved annual Audit Plan, we conducted an audit of the School of Dentistry's Axium application. The School of Dentistry utilizes Axium as its comprehensive electronic health records (EHR) system, and both employees and students use the system for clinical operations and academic support. The audit objectives, conclusions and recommendations follow:

Audit Objective

The objectives of this audit were to review the processes and controls associated with Axium's backup and recovery and to evaluate whether these controls are adequate and operating effectively.

Conclusion and Corrective Actions

Overall, the adequacy of the processes and controls associated with Axium information systems backup and recovery within the School of Dentistry could be improved. While the School of Dentistry currently has processes and procedures in place to ensure Axium backups are occurring regularly and secured in a secondary location, it does not routinely test the recovery of Axium data using existing backups and has not performed an exercise of its Axium system contingency plan within the last three years. Routinely testing backups to ensure their viability and conducting functional tests of contingency plans are critical elements in protecting the availability and integrity of electronic protected health information (ePHI) data during unexpected adverse events, and are foundational requirements within the HIPAA Security Rule.

Internal Audit identified several opportunities for the School of Dentistry to strengthen its controls by creating processes and procedures designed to routinely test the recovery of Axium backups and to perform an annual test of the Axium system contingency plans. The School of Dentistry also identified gaps in its contingency planning during 2018 IT risk assessment activities, and it is currently revising both its Axium data recovery and systems contingency plans as well as, the larger School of Dentistry Business Continuity plans. Additionally, while automated Axium backup process notifications were operational, the sheer volume of daily emails associated with the backups made it very difficult for IT staff within the School of Dentistry to identify areas of concern and action. Internal Audit identified opportunities to strengthen controls by revising the automated backup notifications and enhancing their operational utility.

Acknowledgement

We appreciate the courtesy and cooperation we received from staff within the School of Dentistry, IMS, and the UT Police Department throughout the audit.

BACKGROUND

The School of Dentistry at UT Health San Antonio was founded in 1970 and has been accredited since 1978. The School has 195 dedicated faculty members in 8 fields of study and graduates over 90 dentists annually.

As an integral part of the academic program, dental students have hands-on training in clinical settings. The School of Dentistry utilizes Axium as its comprehensive electronic health records (EHR) system, and both employees and students use the system for clinical operations and academic support. Axium is designed for use in dental schools and its functions include patient registration, appointment scheduling, billing, reporting, and treatment planning.

The loss or unavailability of the Axium EHR could represent both a significant potential patient safety hazard and a major disruption to UT Health San Antonio School of Dentistry academic and clinical operations.

Contingency plans are a critical part of mitigating the risks associated with this loss or unavailability. As a formal recognition of this criticality, CCFR Part 160 and Part 164, Subparts A and C, "Security Standards for the Protection of Electronic Protected Health Information" (commonly known as the HIPAA Security Rule) establish a Contingency Plan standard that includes five implementation specifications. UT Health San Antonio, as a covered entity, is subject to the standards established within the Security Rule.

SCOPE & METHODOLOGY

The scope of this review included current operational activities associated with Axium backup and recovery processes within the School of Dentistry. Our audit testing focused on assessing expected processes and controls established to mitigate risks related to the protection and availability of Axium system data. Our review included, but was not limited to, discussions with both School of Dentistry and IMS Information Systems Operations staff, as well as personnel within the UT Health San Antonio Police Department. Additionally, as part of our assessment of the processes and controls associated with the physical safeguards in place to protect Axium backups, we examined UT Health San Antonio datacenter facility access reviews facilitated by Office of Information Security staff.

We conducted this audit in accordance with the standards set forth by the Institute of Internal Auditors' International Professional Practices Framework. 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 based on our audit objectives.

This audit was conducted by Robert Morgan, IT Audit Director, CISA, CISSP, GSNA, OCP of the UT Health San Antonio Internal Audit Department.

SUMMARY RESULTS

Axium is a critical component of academic and clinical operations at both the School and Dentistry and UT Health San Antonio. The loss or unavailability of the Axium EHR would represent both a significant potential patient safety hazard and a major disruption to School of Dentistry and its clinical operations. School of Dentistry leadership and institutional business continuity planning (BCP) managers have used the levels of these potential impacts as a determining factor in establishing very small tolerances for both Axium unavailability and data loss. Axium operational backup processes and procedures, should directly align with, and support, the requirements established within the School of Dentistry's BCP, and they should support timely notification of backup statuses with sufficient detail to aid in quickly identifying and resolving any failures.

Overall, the adequacy and operational effectiveness of the processes and controls associated with Axium information systems backup and recovery within the School of Dentistry could be improved, particularly in the area of contingency planning.

Tests of Data Backups and System Contingency Plans

Risk Rating[1]: High

Contingency plans are critical to protecting the availability and integrity of electronic protected health information (ePHI) data during unexpected adverse events, such as hardware and software failures, or cyber attacks. As a formal recognition of this criticality, CCFR Part 160 and Part 164, Subparts A and C, "Security Standards for the Protection of Electronic Protected Health Information" (commonly known as the HIPAA Security Rule) focus on ensuring the confidentiality, integrity, and availability of ePHI. The safeguards defined within the Security Rule include a Contingency Plan standard that includes five implementation specifications. Relevant to this review are two required specifications, 'Data Backup Plan' and 'Disaster Recovery Plan', and one addressable specification, 'Testing and Revision Procedures'. UT Health San Antonio, as a covered entity, is subject to the standards established within the Security Rule.

While a significant portion of contingency planning involves the development and testing of system contingency and data recovery plans, a smaller but no less critical practice involves the routine, operational testing of data backups. The routine testing of data backups ensures that, should primary sources of ePHI be lost or destroyed, exact copies of the data can be restored. The loss of critical data and often irrecoverable damage to organizations from recent threats such as ransomware have emphasized that the viability of these backups is often the most significant factor in reducing the damage to both the organization and the owners' of the protected data entrusted to the organization.

The School of Dentistry identified gaps in its contingency planning during 2018 IT risk assessment activities, and it is currently revising both its Axium data recovery and

[1] Refer to Appendix A – Audit Issue Ranking Definitions

systems contingency plans as well as, the larger School of Dentistry Business Continuity plans.

Developing contingency plans is a critical foundational step in protecting ePHI. However, the contingency plans should be regularly tested and revised as necessary. Operational schedules and resourcing levels are significant factors in determining the appropriate level of testing, be it scenario-based walkthroughs or live tests.

UT Health San Antonio regularly performs exercises designed to test various levels and aspects of the institution's business continuity plans (BCP). The School of Dentistry makes annual revisions to its portion of the BCP, and it participates in annual institutional BCP exercises. These exercises focus, however, on larger institutional BCP processes and do not provide the level of operational execution and validation that a School of Dentistry-scoped IT contingency plan exercise would provide. Given the criticality of the Axium EHR to the School of Dentistry and the institution as a whole, it is vital that the plans designed to protect it, be validated annually.

Recommendation

1. The School of Dentistry should continue efforts to improve and document the processes and procedures associated with Axium data backup and system contingency plans in order to reduce the risk to critical electronic protected health information.

2. The School of Dentistry should document and implement improved operational processes and procedures designed to routinely test the viability of Axium data backups.

3. The School of Dentistry should execute an annual functional test of the Axium system contingency plan and incorporate identified changes into revised contingency plans.

Management Response

1. An independent party (within UTHSCSA Dentistry, but not the document creator(s)) will execute our System Recovery Plan until the last step. The intent is to verify that instructions are easily read and understood by the Clinic IT team. Based on this execution, the document will be edited to make any necessary clarifications or updates for predictable execution. This process will be conducted in 2 phases. The first phase will be an execution of all steps of the protocol up to the step of mounting the actual backup file. This phase will be used to make any modifications to the backup document for assurance in execution. The second phase is complete execution, mounting the backup snapshot and evaluating application functionality and integrity. The second phase will require system shutdown and will be conducted annually.

Proposed Completion date: Phase 1 - May 30, 2019; Phase 2 – July 1, 2019

2. Schedule practice runs of our System Recovery Plan up until the point of actually bringing the backup machines live. The full process should not be done regularly because it will disrupt operations. On a monthly basis, a snapshot of a logical drive will be evaluated for data integrity.

   Proposed Completion date: May 15, 2019

3. Schedule an annual full run of our System Recovery Plan. Since this will disrupt operations, this should be done when regular clinics are not working. See #1 for full system recovery description.

   Proposed Completion date: July 1, 2019

Monitoring of Data Backup Processes

Risk Rating: Medium

The School of Dentistry has effective backup process and procedures in place to continually backup Axium in support of the BCP's requirements. In addition, the School of Dentistry IT staff currently receive automated backup process notifications. However, while automated Axium backup process notifications were operational, the current configuration for the notification has resulted in a high volume of daily emails associated with both the backup jobs and the backup infrastructure making it very difficult for IT staff within the School of Dentistry to identify areas of concern and action.

Recommendation

1. The School of Dentistry should continue efforts to refine the processes and procedures associated with Axium data backup job monitoring in order to ensure that backup failures are quickly identified and resolved.

Management Response

1. UT Dentistry Clinical Information Technology is currently in transition to move location and responsibility of backend infrastructure from UT Dentistry to UT Health IMS. Physical servers will be moved as part of the new Data Center on the North Campus.

   Email alerts we receive from the servers will be adjusted. This includes removing ones that no longer apply to our department (to be rerouted to IMS Network and Systems Operations). Warnings (what might become an issue) should be rerouted solely to IMS Operations, while errors and critical events (what is currently causing a problem) will be sent to both our department and IMS Operations.

   Proposed Completion date: June 15, 2019

Appendix A – Audit Issue Ranking Definitions

The audit issue was ranked according to the following University of Texas System Administration issue ranking guidelines:

- ***Priority*** – A Priority Finding is defined as an issue identified by internal audit that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Health San Antonio or the UT System as a whole.

- ***High*** – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to UT Health San Antonio either as a whole or to a significant college/school/unit level.

- ***Medium*** – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to UT Health San Antonio either as a whole or to a college/ school/unit level.

- ***Low*** – A finding identified by internal audit that is considered to have minimal probability of adverse effects to UT Health San Antonio either as a whole or to a college/ school/unit level.