UTHealth™
The University of Texas
Health Science Center at Houston

Office of Auditing & Advisory Services

17-111 Dental Service Research and Development Plan (DSRDP)
axiUm Dental Software System

We have completed our audit of the axiUm Dental Software System (axiUm). 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

The School of Dentistry (SoD) utilizes axiUm, an Electronic Health Record, provided by Exan. The dental clinic management system contains demographics, billing, medical history data, and the complete treatment record on dental patients.

The SoD Technology Services and Informatics (Clinical IT) division is responsible for granting users access to axiUm in accordance with the specifications on the Electronic Health Record User Authorization Form. Individual departments, Student Affairs, and Continuing Dental Education are responsible for determining the need for access and selecting the most appropriate function for the faculty/employee/student/preceptor/resident. The minimum necessary access is granted to each user. The Associate Dean for Patient Care (system owner) has final oversight.

OBJECTIVES

The objective of this audit was to determine whether access and application controls for axiUm are adequate and functioning as intended.

SCOPE PERIOD

The scope period was axiUm active users of October 31, 2017.

METHODOLOGY

The following procedures were performed:

- Selected a sample of users (10) and verified the Electronic Health Record User Authorization Form (for employees) or the Electronic Health Record New User Information Security Contract (for students, preceptors, residents) was completed.
- Selected a sample of change requests (10) and verified the Electronic Health Record Change Request Form was completed and that the change request was approved by the EHR Change Committee.
- Selected a sample of security level roles (5) and reviewed for certain application controls.
- Reviewed all active users in axiUm as of October 31, 2017 for appropriateness of access rights granted. We obtained information from axiUm in December 2017 and January 2018 to verify whether subsequent changes were made.
- Reviewed all active users in axiUm as of October 31, 2017 to determine whether user accounts are linked to UTHealth's Windows authentication.

- Reviewed screenprints of criteria in axiUm showing inactivity time limits for reasonableness.
- Reviewed screenprints of criteria in Fair Warning showing active reports implemented for axiUm for reasonableness. A suggestion was made for Patient Services Management to continue the institution-wide initiative for Fair Warning and implement additional scripts, as needed, upon completion of the assessment.
- Reviewed the "Log On As User" function in axiUm available to administrator users for reasonableness.
- Reviewed documentation of the last periodic user review performed to ensure proper separation of duties for selective users with heightened security roles.
- Reviewed the fiscal year 2017 disaster recovery report for axiUm to determine whether it was successful or resulted in any exceptions.
- Obtained confirmation there have not been any unexpected and/or unscheduled outages for axiUm during the last fiscal year as of October 31, 2017.

AUDIT RESULTS

A&AS identified areas of improvement related to axiUm:

- A periodic review of all users with access to axiUm has not been developed and implemented to ensure user privileges are appropriate. In addition, policies and procedures related to access controls were not consistently followed.
- A documented roles and functionalities of each user security level in axiUm has not been formalized at the time of audit. Prior to the end of fieldwork, a finalized version was provided to A&AS.

NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM

None

We would like to thank the staff and management within the SoD Clinical IT, SoD Patient Services, and UTHealth Information Technology who assisted us during our review.

Nathaniel Gruesen

Nathaniel Gruesen, MBA, CIA, CISA, CFE
Senior Audit Manager - General

MAPPING TO FY 2017 RISK ASSESSMENT

Risk (Rating)	R.94 Change protocols for axiUm are too cumbersome (High).

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Audit Manager	Nathaniel Gruesen, MBA, CIA, CISA, CFE
Auditor Assigned	Kathy Tran, CIA, CFE

End of Fieldwork Date	February 6, 2018
Issue Date	February 14, 2018

Copies to:
Audit Committee
Dr. John Valenza
Dr. Muhammad Walji
Dr. Kimberly Ruona
Joe Morrow
Kristine Estes
Anna Trieu
Diana Morcho

Issue #1	The following policies and procedures for access controls were noted: • Control AC-6 of the Security Control Standards Catalog (a supplement to the Texas Administrative Code 202) requires an organization to employ the principle of least privilege, allowing only authorized accesses for users which are necessary to accomplish assigned tasks in accordance with the organizational missions and business functions • Control AC–21 of the Security Control Standards Catalog (a supplement to the Texas Administrative Code 202) requires user login credentials to be provided based on job responsibilities and periodically reviewed for appropriateness. • UTHealth's ITPOL-004 Access Control Policy, Section 6.2.6 states, "Owners or their designees must review access lists regularly to ensure access privileges are appropriate. Timeframe for access list review should be established based on documented risk management decisions." • SoD EHR Access Management Policy states the Clinical IT department is responsible for granting access to axiUm in accordance with the specifications on the Electronic Health Record User Authorization Form. Students, residents, and preceptors are assigned to their corresponding security level in axiUm. The minimum necessary access is provided for each user. To satisfy this, the Clinical IT department requires documentation of training and management oversight if a user requested to have more access rights in axiUm in comparison to their job title. In addition, the following informal departmental procedures were noted: • All user accounts, with some exceptions, in axiUm should be linked to their corresponding UTHealth's active directory (AD) authentication. • Residents who also act as "Attending" for students will have their second axiUm account notated with an asterisk (*) in front of the username. These user accounts are not tied to the AD. The users can only access axiUm to approve record entries and charges by swiping their badges. The expiration date noted for these accounts assists in expiring these accounts when the accounts are no longer needed. A&AS reviewed all axiUm active users as of October 31, 2017 to determine whether the user accounts in axiUm are linked to AD as well as whether access rights granted to the users are appropriate. The following was noted: • User accounts are not always tied to AD and do not have expiration dates notated or have incorrect/invalid AD information. • User accounts no longer requiring access were not deactivated. Some of the reasons included the Clinical IT team was not made aware the student had graduated or left the institution, or was not informed the employees no longer needed access based on their

	new role. These user accounts have been deactivated as a result of the review. • User accounts were not assigned to the most appropriate security levels available in axiUm at the time of the review. This was due to changes made to the security levels; however, the users were not moved accordingly. The user accounts have been moved to the most appropriate security level as a result of the review. • User accounts appears to have more access rights than required; however, documentation of training and/or management oversight to support the current security level the users reside had not been provided to the Clinical IT department. Additionally, A&AS noted the Director – UT Dentists and Patient Care is responsible for monitoring users with potential segregation of duties (dual roles that allow the user to enter and delete charges in axiUm) twice a year. Evidence of the semi-annual review is retained electronically with the completed date notated on the spreadsheet. This periodic review, however, does not ensure all users with access to axiUm is appropriate at any specific point in time.
Recommendation #1	We recommend the system owner (or designee) perform a review, and where necessary, develop and implement procedures to ensure user accounts in axiUm are: • Linked to the AD or mitigating controls are in place if it is not applicable; • Deactivated in a timely manner for users no longer requiring access; and • Granted only authorized accesses for users which are necessary to accomplish assigned tasks in accordance with the organizational missions and business functions (principle of least privilege). In addition, a process to perform a periodic review of all users with access to axiUm should be developed and implemented. Evidence documenting the review should be retained.
Rating	Medium
Management Response	System owner (or designee) will implement a process for an annual review of all users to ensure privileges are consistent with each user's current job role/title. The process will include documented evidence of the review and will be retained in the Office of Patient Care. • Clinical IT team will continue the current process of ensuring all user accounts in axiUm have an expiration date, as applicable (primarily students, preceptors, and residents). Accounts without expiration dates will be linked to the most recent available AD information. • The Clinical IT team has now updated their process to request a specific expiration date for residents per program instead of using the default one. In addition, they will reach out to ensure they are receiving the transfer/termination report for the entire university, not just the School of Dentistry. In addition, Clinical IT began

	setting a two week expiration date upon users appearing on the transfer report. The user is then notified of the expiration date and that they are required to submit a new EHR User Authorization Form in order to retain access to axiUm in their new role, if indicated. This process was implemented last year to help ensure users are in the appropriate security level and only retain access when needed. Finally, the Clinical IT team will work with Patient Services to ensure all accounts are updated based on the annual review of accounts for appropriate access. The Office of Patient Care will modify the student/resident Clinical Check-out Form to include Clinical IT notification of mid-year student withdrawals (DS4/DS3/DH/Res) and work with new staff in the Office of Student & Academic Affairs to ensure that mid-year withdrawals or dismissals are formally communicated to Clinical IT (DS2/DS1). • Clinical IT team will revise the EHR User Authorization Form instructions to include the requirements of documented training and management oversight for any security level requests not aligned to their job title within HCM system. Current users without documentation will be moved to the appropriate security level. Security level revisions will be considered once the necessary documentation is provided.
Responsible Party	Kimberly Ruona, DDS, Associate Dean for Patient Care
Implementation Date	July 1, 2018

Issue #2	Control AC–2 of the Security Control Standards Catalog (a supplement to the Texas Administrative Code 202) requires management to establish group and role membership as well as specify access privileges for each user account. While the Clinical IT department has proactively worked to tighten the access controls to ensure the minimum necessary access is provided to each user, a documented roles and functionalities of each user security level has not been formalized at the time of audit. Prior to the end of fieldwork, A&AS was provided with a finalized version of the roles and functionalities spreadsheet documenting what each of the 33 active security levels in axiUm can and cannot do in axiUm.
Recommendation #2	We recommend Clinical IT Management work with Patient Services Management to compile and formalize the roles and functionalities of each security level in axiUm. This will assist to provide an overview of what each security level can and cannot do in axiUm.
Rating	Medium
Management Response	The current security levels and functionalities have been documented and approved by the System Owner and Patient Services Management. The finalized documentation was provided to A&AS.
Responsible Party	Kimberly Ruona, DDS, Associate Dean for Patient Care
Implementation Date	April 1, 2018 (if any additional changes are identified)