UNIVERSITY OF CALIFORNIA, SAN FRANCISCO
AUDIT AND ADVISORY SERVICES

School of Dentistry
Orthodontic Clinic - axiUm Access Controls
Project #15-043

December 2014

Orthodontic Clinic - axiUm Access Controls
Project #15-043

MANAGEMENT SUMMARY

As a supplemental audit for Fiscal Year 2014-15, Audit and Advisory Services (AAS) completed an access controls review of the axiUm system (axiUm) within the School of Dentistry (SOD) Orthodontic Clinic. AxiUm is a software package from the Exan Group designed for Dental Universities.

The purpose of the review was to assess user access controls within axiUm to assure that adequate segregation of access roles has been established, appropriate controls over editing and deleting of records are implemented, and user access is assigned based on job duties and operational needs.

To conduct the review, AAS interviewed Orthodontic Clinic personnel and Network and Information Services (NIS) personnel and reviewed the axiUm access controls, including user list, security configurations, and functionalities to validate access granted to Orthodontic Clinic personnel.

Based on the work performed, axiUm provides reasonable user access controls based on segregated access roles; and user access is generally assigned based on job duties. However, opportunities for improvement exist for managing access controls in a more consistent and efficient manner; and implementing controls over the delete function which allows for the removal of patient information from the official medical records.[1] Lastly, due to the current axiUm system design, manual processes and procedures are needed to monitor for the appropriate approval of procedures performed and documented by residents.

Additional information regarding the observations and associated management corrective action plans is detailed in the body of the report.

[1] The axiUm 'delete' function removes the deleted information from official medical records. Deleted information can be displayed as "strikethrough" if users choose an option to show deleted records.

I. BACKGROUND

As a supplemental audit for Fiscal Year 2014- 15, Audit and Advisory Services (AAS) completed an access controls review of the axiUm system (axiUm) within the School of Dentistry (SOD) Orthodontic Clinic. AxiUm is a software package from the Exan Group designed for Dental Universities, which was installed at SOD in December 2001. AxiUm allows clinic personnel to schedule appointments, document clinical and treatment information, and bill patients. Additionally, faculty/student/patient relationships are built-in, which allow faculty members to approve, monitor, and manage treatments performed by residents.

II. AUDIT PURPOSE AND SCOPE

The purpose of the review was to assess axiUm's access controls for Orthodontic personnel to validate that:

- Adequate segregation of access roles has been established;
- Appropriate controls over editing and deleting functions are implemented; and
- User access is assigned based on job duties and operational needs.

The procedures performed included the following:

- Interviewed SOD Network and Information Services (NIS) personnel to gain an understanding of the access controls in axiUm for Orthodontic personnel and the processes to create, change, and disable user accounts;
- Reviewed user accounts in axiUm for the Orthodontic Clinic to validate that access was granted based on job duties and operational needs;
- Reviewed axiUm security configurations for Security (Group) Levels created for Orthodontic Clinic personnel to assess patient restrictions for each group;
- Reviewed axiUm security configurations for individual user levels to assess appropriateness of assigned functionality to edit and delete patient records;
- Reviewed the functionality and use of bulk approvals for treatments performed by residents; and
- Reviewed assigned faculty for residents' patients to verify appropriateness of faculty assignment.

Since work performed was limited to the specific procedures stated above, this report is not intended to, nor can it be relied upon to provide an assessment of the effectiveness of controls beyond those areas and systems specifically reviewed. Fieldwork was completed in September 2014.

III. CONCLUSION

Based on the work performed, axiUm provides reasonable user access controls based on segregated access roles; and user access is generally assigned based on job duties. However, opportunities for improvement exist for managing access controls in a more consistent and efficient manner; and implementing controls over the delete function which allows for the removal of patient information from the official medical records.[2]

[2] The axiUm 'delete' function removes the deleted information from official medical records. Deleted information can be displayed as "strikethrough" if users choose an option to show deleted records.

Lastly, due to the current axiUm system design, manual processes and procedures are needed to monitor for the appropriate approval of procedures performed and documented by residents. Specifically, enhanced controls should be implemented in the following areas:

- System controls and user account management in axiUm
  - Develop Security (Group) Levels templates to manage user security in a consistent and efficient manner;
  - Develop and implement change management procedures to ensure all changes to user security configurations are documented, supported, and authorized; and
  - Perform periodic reviews to ensure appropriateness of user accounts and access levels.

- School of Dentistry clinical operations
  - Define and document roles and access levels for axiUm users to ensure the delete function (strikethrough) for medical records is only assigned as appropriate;
  - Monitor deleted medical records for completed treatments and approved procedures to ensure appropriateness;
  - Define and document approval requirements for treatments performed by residents to ensure residents' work is appropriately supervised and approved;
  - Assess the proper use of bulk approval for treatments performed by residents to ensure adequate review is performed; and
  - Develop and implement procedures to ensure current faculty members are reassigned to residents.

Detailed information on these observations and associated management corrective action plans are outlined in the tables in Attachment A.

Orthodontic Clinic - axiUm Access Controls
Project #15-043
Attachment A: Observations and Management Corrective Actions

A. System controls and user account management in axiUm

No.	Observations	Risks/Effect	Management Corrective Actions
A.1	**Security (Group) Level Templates** SOD NIS is unable to manage the current provisioning process for axiUm in a consistent and efficient manner. There are over 120 Security Level templates in addition to the individual user level security which is configured separately. UCOP Business and Finance Bulletin IS-3 Electronic Information Security (IS-3)[3] stipulates that authorization process should determine whether or not an identified individual or class has been granted access rights to an information resource and determining what type of access is allowed (IS-3§III.C.2.a).	Failure to control user security in a systematic and managed method increases the risk that users with unnecessary privileges may go unnoticed.	By July 31, 2015, SOD NIS should develop and reduce the number of templates for all Security (Group) Levels and manage user security in a consistent and efficient manner.
A.2	**Change Management** A change management process has not been implemented to properly track changes made to user accounts and privileges. As a result, operational needs and justifications for access privileges granted to users are unknown. IS-3 stipulates that all changes to a system be conducted in accordance with a planned change management process which includes monitoring and logging of all changes and documented authorization for changes (IS-3§III.C.2.e).	Failure to implement change management procedures increases the risk of unauthorized changes occurring without being detected.	By July 31, 2015, SOD NIS should establish and implement change management procedures. Any changes made to Security (Group) Levels and individual user level security configurations should be documented, supported, and authorized.

[3] IS-3 Electronic Information Security(http://policy.ucop.edu/doc/7000543/BFB-IS-3)

A.3	**Periodic Reviews of User Accounts** Periodic review of user access is not performed to validate that authorized users are granted appropriate level of access. Our review of Orthodontic Clinic user accounts identified that one user had duplicate accounts. Additionally, instructor privilege for approving procedures documented by residents was granted to dental assistants and an x-ray technician inappropriately. IS-3 stipulates that access must be revoked upon termination or when job duties no longer require a legitimate business reason for access (IS-3§III.C.1.a). IS-3 also stipulates that access authorization shall be limited, using technical or procedural controls, to the least permission necessary for the performance of duties (IS-3§III.C.1.a).	Failure to revoke accounts of users who no longer require access to the system increases the risks of unauthorized access to the system.	1. During the course of the review, SOD NIS corrected the duplicate accounts and removed the inappropriate instructor privileges. No further action required. 2. By September 30, 2015, upon completion of the new Security Level templates (in A.1), SOD NIS will establish procedures to review users and access levels for all axiUm accounts on an annual basis.

B. School of Dentistry Operations

No.	Observations	Risks/Effect	Management Corrective Actions
B.1	**Evaluation of User Roles and Access Levels** Some security settings in axiUm pair the delete and edit functions together as a single option; therefore, many users who need edit rights are also granted the delete function unnecessarily. Additionally, many users have privileges to use the delete function to remove patient information from the official medical records even after procedures were completed or approved. Deleted procedures are not a part of official medical records, but can be displayed as strikethrough if users choose the option.	Medical records can be maliciously or mistakenly deleted.	1. By June 30, 2015, SOD Dean's Office will work with SOD NIS to define and document roles and access levels that should have the delete function. 2. By September 30, 2015, SOD Dean's Office will evaluate and determine a practice for monitoring medical records deleted after treatments were completed or residents' procedures were approved. 3. By September 30, 2015, SOD

	Review of users in the Orthodontic Clinic identified the following:[4] • 16 users can edit and delete all accessible in-progress or completed treatments entered by anybody; • 24 users can delete all accessible treatments after approval; • 17 users can edit and delete all approved notes; and, • 39 users can edit and delete all approved labs.		Dean's Office, in conjunction with SOD NIS, will develop training materials and guidelines for the appropriate use of the delete function and provide training sessions to users.
B.2	**<u>Approvers for Procedures Documented by Residents</u>** There are no established requirements defining who is authorized to approve procedures documented by residents at the Orthodontic Clinic. Due to system design, axiUm allows instructors and faculty members to approve all 'accessible' procedures documented by residents, regardless of whether they are the attending instructor or faculty member. As a result, procedures documented by residents may be approved inappropriately.	The absence of clearly defined requirements for approving procedures performed by residents increases the risk that procedures are inappropriately approved.	SOD NIS has already submitted a request to the vendor for a future enhancement to restrict approvers. As an interim solution, SOD Orthodontic Clinic will determine and document approval requirements for residents and communicate the requirements to approvers by January 31, 2015.
B.3	**<u>Bulk Approval</u>** It is a common practice for Orthodontic Clinic instructors to perform bulk approvals; therefore, patient procedures may be approved without proper review. As a default setting within axiUm, all unapproved procedures documented by residents are automatically displayed when a patient is selected, and axiUm allows users with approval privileges to approve all procedures as a single transaction (Bulk).	The ability to approve procedures in bulk increases the risk that procedures performed by residents are not appropriately reviewed prior to approval.	SOD NIS has already submitted a request to the vendor for a future system enhancement to change the default setting to select procedures. As an interim solution, SOD Orthodontic Clinic, in conjunction with SOD NIS, will develop procedures and instructions for requiring proper reviews of procedures prior to approval and communicate these procedures to approvers by December 31, 2014.

[4] There are other areas where security settings can be configured in axiUm for determining accessibility based on assigned patients, screens/data fields, and clinics.

B.4	**<u>Assignment of Faculty</u>** Review of assigned faculty for Orthodontic Clinic patients identified that three faculty members who were separated from the Orthodontic Clinic or on leave were still assigned to residents' patients. Additionally, one resident is assigned as faculty for two patients. A faculty must also be assigned to patients if residents are assigned as providers; however, there is no process to reassign faculty members when they separate or on leave from the University.	The absence of a process to review and reassign current faculty members increases the risk of lack of accountability for overseeing residents' work.	By June 30, 2015, SOD Orthodontic Clinic will develop and implement procedures to reassign faculty.