EHR Access Management Policy

1. RESPONSIBILITY

School of Dentistry Departments and Administrative Unit Responsibilities

1. Determining the need for EHR access for employees (faculty, staff, volunteers), students, residents, externs, and contractors
2. Selecting the most appropriate role or function of the axiUm account for the person.
3. Obtaining required authorization by the person's supervisor, department administrator, or department chair.
4. Submit the completed access request form to IT (https://support.dental.uw.edu).
5. Check with Patient Revenue Cycle to see if provider requires insurance enrollment.
6. Inform IT when the person no longer needs access, goes on extended leave, or is no longer affiliated with the School of Dentistry by submitting an IT account termination request.
7. Ensuring appropriate credentialing is in place if required by the person's axiUm role.

School of Dentistry Compliance Office Responsibilities

1. Enforce compliance policies.

School of Dentistry Student Services Responsibilities

1. Providing IT a list of all incoming predoctoral students.
2. Notifying IT if a predoctoral student goes on leave or is no longer registered as a student.
3. Providing IT a list of all graduating predoc students and the account termination date.
4. Notify IT of any predoctoral students who require access beyond the account termination date.

School of Dentistry IT is responsibilities

1. Ensuring the Access Request Form is complete for all account requests before processing.
2. Access is granted according to the specifications on the Access Request Form.
3. Verify assigned HIPAA training and School of Dentistry agreements have been completed in the School of Dentistry's Learning Management System prior to account creation. OMS and AGD Residents are contractually allowed to complete HIPAA training up to 30 days after their start date and may complete HIPAA training after axiUm access has been provisioned.
4. All modification and termination requests and notifications are processed correctly. The IT team is the only group able to alter user profiles or security.

2. SCOPE

This policy applies to all users accessing the UW School of Dentistry's EHR system and related imaging systems.

3. DEFINITIONS

Term	Definition
EHR	Electronic Health Record (General term used for axiUm, MiPACS, and related imaging systems at the School of Dentistry)
HIPAA	Health Insurance Portability and Accountability Act
Protected Health Information (PHI)	Individually identifiable health information transmitted or maintained in any form or medium by a Covered Entity or its Business Associate.

4. STANDARDS

Access control procedures ensure that access to the EHR is appropriate, regardless of the method of access. These procedures ensure that access given to people has been granted by the owner through appropriate access rights. The EHR includes but is not limited to data containing protected health information (PHI) and other confidential information.

The following procedures apply to access control:

New Users

New users must follow one of two paths for access to the EHR: 1) New predoctoral students access via Student Services, 2) New faculty, staff, volunteer, graduate student, resident, extern, and contractor access is requested by their department or administrative office via submission of the Access Request Form to SOD IT.

In accordance with HIPAA regulations and UW policy, contractors and other people not affiliated with UW must have a signed Business Associates Agreement and Personal Data Processing Agreement on file prior to requesting access.

Modifying or Terminating Accounts

EHR account modification must be originated by the following methods: 1) A new Access Request Form specifying the security change 2) the transfer/termination report sent by UW SOD HR monthly to the IT team, or 3) a special request is sent by an authorized individual.

Modified Users via Access Request Form

A new Access Request Form must be submitted using the same process as a new user request.

Transfer Process via Transfer/Termination Report

If the transfer is to an entity outside of the School of Dentistry, the account is deactivated on their termination date or when the HR transfer/termination report is received by SOD IT (whichever is sooner). In the case of an internal transfer, the new department or administrative office is then required to follow the same procedures as a new employee to modify access.

Terminating Access

Access to the EHR must be terminated using the following methods: 1) Access Request Form submitted to SOD IT requesting account termination. 2) HR Termination/Transfer report sent to SOD IT. 3) Student Services notification to SOD IT notifying them of any student terminations or withdrawals. 4) Special Requests can be sent by Administrative Managers, Department Chairs or Deans to SOD IT requesting immediate deactivation of an account prior to the monthly termination report. In addition, those same groups must notify SOD IT of Leave of Absences. During a Leave of Absence the users account is deactivated until notification from the requestor to reactivate the account upon return.

Security Level Assignment

Security levels are assigned based on user role and job duties. Students, residents and preceptors are assigned to the corresponding security level. All other users are assigned the appropriate security level based on the role and job duties specified on the Access Request Form specified by the unit initiating the request. Appropriate access is provided for each user based on the specified role(s) on the Access Request Form.

New and Modified axiUm Security Level

When new or modified axiUm security level is defined in the axiUm system, management must approve the new or modified security level and its access rights prior to having them implemented in the axiUm system.

5. EXCEPTIONS

Requests for exceptions to this policy should be submitted to the Associate Dean of Clinics for review and consideration. If the job function selected does not match the user's job title and a higher level of security is requested, documentation outlining management oversight and proof of training must be provided.

6. CONTACTS

Contact	Role	Department/Office, Title	Phone	Email
Gary Farris	Policy Owner	SOD, Asst. Dean of Finance and Resources	206.616.9158	gfarris@uw.edu
Tom Ruddle	Policy Author	SOD IT, Director of IT	206.221.4007	truddle@uw.edu

7. REVISION HISTORY

Author	Version	Reason for Change	Effective Date
Gary Farris	1.01	Audit updates	6/22/2020
Tom Ruddle	1.0	Document Creation	3/31/2020