UNIVERSITY of MARYLAND
SCHOOL OF DENTISTRY

University of Maryland, School of Dentistry

Clinical information Management System

User Security Access Policy

I. POLICY STATEMENT

It shall be the policy of the University of Maryland, School of Dentistry that all users of the axiUm application, which houses all of our Patient's and Faculty's sensitive information, is regarded as confidential, is secure. Patient care information is the property of the patient with the University of Maryland, School of Dentistry being the gatekeeper of that information and the owner of the medium of storage, our axiUm application. University of Maryland, School of Dentistry shall maintain management processes to ensure that access to axiUm is restricted to authorized users with minimal access rights necessary to perform their role and responsibilities. Account provisioning and monitoring shall be reviewed annually.

II. POLICY PURPOSE

The purpose of this policy is to protect patients from inappropriate dissemination of identifiable information. This policy applies to all clinical staff, employees, vendors, volunteers, students and others who are members of the University of Maryland, School of Dentistry sites and Health Centers, and refers to all information resources, whether verbal, printed, or electronic, and whether individually controlled, shared, stand alone or networked. This policy also provides guidelines on employee access to patient data to ensure confidentiality and integrity of patient information.

III. DEFINITIONS

Access: The ability of a data user or application process to read, write, modify, or communicate information or otherwise make use of an information asset.

Access Profile: A list of the applications and/or databases a user (or application process) is permitted to access and the access levels granted in each of those applications and/or databases.

Audit: A formal review and identification of access to an information asset by an individual, organization, or application process.

Authorization: Documented approval to access University of Maryland, School of Dentistry health information assets based on the user's need to know.

Authorization and Access Control (AAC) Process: The process in which Departmental Directors request access for members of their department based on those members' roles and their role-based need to know, and Data Managers ensure that the needed access to applications is made available.

Need to Know: The principle that states that a user should access only the specific information necessary to complete his or her assigned job functions. This principle is applied in two main contexts:

1. Departmental Directors (or their Delegated Access Coordinators) apply this principle in determining the appropriate level of access to databases and/or applications needed by people in different roles in their department (see University of Maryland, School of Dentistry Policy, "Information Access: Responsibilities of Department Directors or Delegated Access Coordinators").
2. Authorized Data Users apply the principle every time they decide whether to access a specific individual's record or not, even if they have been granted full access to the application in which the record resides.

Once access to a database and/or application has been authorized, the authorized data user is still obligated to assess the appropriateness of each specific access on a need to know basis.

IV. POLICY STANDARDS

A. In order to ensure confidentiality, patient information collected and/or generated within the University of Maryland, School of Dentistry shall be maintained in such a manner that access to it is restricted to those with a need to know, and release of it is restricted to those with a legal right to know, as mandated by State and Federal laws. All patient information must be stored in the electronic patient record maintained by the University Of Maryland School Of Dentistry. E.g. axiUm clinical management, MiPACS and Dolphin Imaging.

B. It shall be the responsibility of the department management to determine its' members user access profile in order to complete their job functions. Viewing or obtaining information not needed for job completion constitutes unauthorized use of that information. It shall be the responsibility of the department management in conjunction with the HIPAA Officer and/or Security Officer to monitor and discipline members in all matters of information security. Authorization and Access Control Process includes:

- Creating identifier profile accounts for each student, staff, faculty and Dean's faculty, at the earliest possible point of contact between individual and SOD and upon completion of account application;
- Defining security access rights to commensurate with user job responsibilities;
- Onboarding and Off boarding forms to be completed by department management, to keep strict access to Patient Information and to assure that our Patients' Information is in proper hands during treatment and to inhibit access after dismissal
- Student user access profiles have an expiry date of June 30th of graduation year;
- Users must have limited access to axiUm records containing sensitive data based on scope of responsibility, a student or employee may not access private information if it is not relevant to individual's function;
- Student status updates and changes to be updated with the Registrar, to revoke any access due to any withdrawal, leave of absence, or grade retention;
- User access to accounts in axiUm shall be set to automatically disable November 30th each year for non-compliant users;

- User shall be granted access after required compliance training and assessments completed and confidentiality pledge signed;
- User access list shall be reviewed with department management at least annually to reflect current user access of user role or any change in employment status. This review shall be documented and retained by IT Administrators for audit verification purposes.

C. In order to safeguard patient confidentiality and integrity, annual reviews of user access to information resources is restricted to only authorized users. Validations shall be done annually that any User of axiUm is indeed updated in their Annual Compliance training, pass assessments and sign our Confidentiality Pledge. Validation safeguards include:

- Annual audits shall be reported to ascertain incomplete required yearly compliance training;
- Annual Compliance assessments are completed by November 30th of each year;
- Reminder email notifications to all axiUm users to advise of ANNUAL Compliance training and assessment completion by Nov. 30 of each year;
- Enforcing compliance, notices shall be sent prior to November 1st to departmental management to encourage their axiUm user compliancy timing;
- User access revoked to non-compliant individuals December 1st of each year;
- HIPAA Officer and/or Compliance Manager shall monitor access to confidential data and logged into user identifier accounts upon completion of annual compliance training and granted access of axiUm until the following November 30th date;
- Revoking user access to account, lock-outs, shall be implemented to non-compliant users;

D. It shall be the responsibility of management staff in each department in conjunction with the HIPAA Officer and/or Security Officer to inform their employees of this policy, and to develop and maintain, if appropriate, data confidentiality policies specific to their department, which are consistent with this policy. To assure knowledge of these policies, it shall be the responsibility of the department supervisors to assure that current policies be addressed at departmental staff meetings periodically. In addition, these policies shall be referred to and addressed in each orientation program and shall be included in any orientation “information packet" provided for new employees, trainees, volunteers, vendors, and clinical staff.

E. To maintain access for clinical users, the following entries must be entered for each patient appointment prior to 11p.m that day:

- Progress note
- In process or completed treatment
- Medical history update

F. Every clinical staff member, employee, trainee, student, vendor, and volunteer at the University of Maryland, School of Dentistry shall be responsible for maintaining confidentiality of all information entrusted to them. All personnel of the School of Dentistry is expected to exercise due care in any discussion or use of patient information. Limiting access to ONLY persons providing patient services in axiUm protects and guards against impermissible access and dissemination of confidential information.