

University of Maryland, School of
Dentistry

Confidentiality of Patient Information Policy

I. POLICY STATEMENT

It shall be the policy of the University of Maryland, School of Dentistry that all information regarding care of the individual patient be maintained as confidential information. Patient care information is the property of the patient; University of Maryland, School of Dentistry is the steward or caretaker of that information and the owner of the medium of storage.

II. POLICY PURPOSE

The purpose of this policy is to protect the patient, the clinical team, and the University of Maryland, School of Dentistry from inappropriate dissemination of information regarding care of individual and collective patients. 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. Proper handling of external requests for patient information is addressed in the Privacy Policy. This policy also provides guidelines and examples on employee access to patient identifiable information to ensure confidentiality and integrity of patient information.

III. DEFINITIONS

Aggregate Data: A collection of patient care or clinical information which does not reveal the identity of individual patients.

Central Repository of Patient Information: A physical archive or storage area where one or more of the several components of patient information are permanently maintained. E.g. Axium, Dolphin Imaging and Romexis.

Clinical Staff: Attending, courtesy, honorary, and visiting physicians, house officers and fellows, special purpose trainee staff members and nurses having practice privileges for the diagnosis and treatment of patients at the University of Maryland, School of Dentistry clinics.

Confidential Information: Any individually identifiable health information received, used or accessed by personnel of the School of Dentistry or its affiliated entities must be treated as protected and confidential.

Data Steward: Individual or department having access to patient information and having capability of providing for storage or transfer of patient information subject to this policy.

Due Care: That degree of care which other prudent, competent, persons providing patient services would exercise in similar circumstances.

University of Maryland, School of

Dentistry

Inappropriate Dissemination: Seeking access to and/or disclosing confidential information, regardless of intent, in verbal, written or electronic form:

- To individuals not involved in the care, treatment or clinical operations of that the University of Maryland Dental School patient; or
- To individuals who are involved with or know the patient but have no need to know the information; or
- In a setting where that information could be overheard by individuals who have no need to know (e.g., in elevators, lobbies, waiting rooms, hallways, dining rooms, etc.); or
- In a setting where information can be read or transferred from an unattended computer monitor; or
- Through sharing another person's electronic password.

Need to Know: Necessary to fulfill the mission or charge of the University of Maryland, School of Dentistry and its clinical staff, employees, trainees, students, volunteers, or vendors to provide quality patient care, education and research.

Patient Information: All information, data and/or knowledge relating to the care of a the University of Maryland, School of Dentistry sites and Health Centers patients, including but not limited to:

- The medical record, including data recorded on paper, on microfilm, or in a computer data base; or
- Pictorial, graphic, or multimedia representations (e.g. photographs, x-ray films ECG tracings, videotape); or
- Tissue specimens obtained for histological examination; or
- Administrative data, such as the data included in the University of Maryland School of Dentistry clinic management system; or
- Business or Financial Records.

Personnel: Any faculty, staff, students, and visitors of the School of Dentistry.

Trainee: Any individual involved, directly or indirectly, in the provision of patient care, one aspect of which is to further that individual's knowledge; includes house officers, dentistry students, nursing students, and other health care professions students. A trainee may or may not receive financial compensation from the University of Maryland, School of Dentistry.

Vendor: Any individual or organization that sells or otherwise provides a good or service to the University of Maryland, School of Dentistry.

Volunteer: Any individual providing a service to the University of Maryland, School of Dentistry, coordinated through the Director of Volunteers in each corporate area, who receives no financial compensation from the University of Maryland, School of Dentistry for that service.

University of Maryland, School of

Dentistry

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. Axiom, Dolphin Imaging and MiPACS.

B. It shall be the responsibility of management in each department to determine what information its members need access to in order to complete their job functions. Viewing or obtaining information not needed for job completion, regardless of the medium of storage, constitutes unauthorized use of that information. It shall be the responsibility of department management in conjunction with the HIPAA Officer and/or Security Officer to monitor and discipline members in all matters of information security.

C. 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 are 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.

D. It shall be the responsibility of respective data stewards in conjunction with the HIPAA Officer and/or Security Officer to maintain secure access to their electronic data and to provide such information in response to questions regarding potential breach of confidentiality. When feasible, audit trails shall be maintained of access to both aggregate and patient-identifiable electronic data.

E. In order to help ensure that only those employees with a need to know patient identifiable information are granted access to such information, data stewards will, on an annual basis, review who has access to patient identifiable information in central repositories of patient information under their purview.

F. Hard copy printouts and patient-identifiable electronic data will be stored in a secure area and maintained in a confidential manner as is currently required of paper medical records.

G. 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.

**University of Maryland, School of
Dentistry**

H. Every clinical staff member, faculty, trainee, student, vendor, and volunteer at the University of Maryland, School of Dentistry shall be responsible for taking annual HIPAA training and passing the HIPAA quiz in order to have access to clinical systems.

I. The University of Maryland, School of Dentistry characterizes as unethical and unacceptable any activity through which an individual:

1. Voluntarily allows or participates in inappropriate dissemination of confidential patient information; or
2. Interferes with the intended use of the information resources; or
3. Without authorization, destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of patient information and/or information resources; or
4. Without authorization invades the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources.

J. Infractions of this confidentiality policy shall be subject to the disciplinary action of the University of Maryland, School of Dentistry, up to and including dismissal and/or loss of privileges. Invasion of another person's right to privacy can have legal consequences in addition to disciplinary action from the University of Maryland, School of Dentistry.

K. Requests for access to patient identifiable data needed for research purposes must be accompanied by IRB approval.

L. Communication regarding confidentiality policies and monitoring of these policies for clinical staff shall be channeled through the Clinical Affairs Office or the Office of Information Technology.