University of Maryland, School of Dentistry

Information Management Policy

Subject: III. Clinical – F. HIPAA

Department: HIPAA

Effective Date: March 2016

Reviewed and/or Revised: 09/01/2017

I. POLICY STATEMENT

It shall be the policy of the University of Maryland, School of Dentistry to capture, share, secure, maintain, and enhance the value of University of Maryland, School of Dentistry health information assets in all mediums through appropriate information management policies and actions that meet applicable Federal, State, regulatory, or contractual requirements and support the University of Maryland, School of Dentistry mission, vision, and values. Furthermore, it shall be the policy of University of Maryland, School of Dentistry to support and adhere to the rights and responsibilities of patients as specified in the State of Maryland Public Health and Mental Health Codes.

II. POLICY PURPOSE

The purpose of this policy is to identify and disseminate the University of Maryland, School of Dentistry's framework and principles for information management that guide our institutional actions and operations in protecting, generating, and sharing individually identifiable health information in support of the University of Maryland, School of Dentistry's mission, vision, and values.

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.

Account Administration**:** The process by which authorized data users are assigned accounts (sign-ons) to University of Maryland, School of Dentistry health information assets using the access controls (profiles) prepared by Data Managers.

Account Administrator**:** The individual acting at the direction of the Data Manager who implements controls on access to information assets by applying formal guidelines and practices to functions such as assigning user access codes, revoking user access

privileges, and setting file protection parameters. (The roles of account and system administrator may be combined for smaller databases.)

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

***Authentication*:** The process by which a user (or application process) identifies her or himself to an information system or resource. The user is required to provide at least one (often a combination) of the following unique elements:

1. Something that the user knows (such as a password or a personal identification number);
2. Something that the user has in her possession (such as a token or access card);
3. Something that is a characteristic or an expression of the user's physical being (such as finger or voice prints).

***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.

***Authorized Access Database (AAD)*:** The centralized repository of information about all University of Maryland, School of Dentistry Authorized Data Users, under the responsibility of one administrator. The Authorized Access Database must include at a minimum:

1. User name and a unique identifier
2. User login ID
3. Date access last changed, and start and stop date for authorized use of an account and/or application
4. User's Departmental Director or Delegated Access Coordinator
5. Application ID for each application
6. User's authorized access profile for each application

Authorized Data User (ADU): Individuals who have been granted authorization through the Authorization and Access Process to access specific University of Maryland, School of Dentistry health information assets in the performance of their assigned duties or in fulfillment of their role in the University of Maryland, School of Dentistry community. Authorized Data Users include, but are not limited to, faculty and staff members, employees, trainees, students, vendors, volunteers, contractors, and other affiliates of the University of Maryland, School of Dentistry as well as external users who have been granted accounts on University of Maryland, School of Dentistry health information assets under the terms of an information sharing agreement.

***Business Owner*:** The senior University of Maryland, School of Dentistry official (and his/her staff) having policy-level responsibility for managing a segment of the University of Maryland, School of Dentistry information assets by the Data Steward, e.g. Departmental Chairs, Directors of Units.

***Certification*:** Evaluation of the computer system(s), storage media, network(s), information transmissions, operating systems, and applications design supporting the University of Maryland, School of Dentistry health information assets which confirms that the appropriate security measures have been implemented in accordance with University of Maryland, School of Dentistry policies.

***Consent*:** The voluntary agreement of an informed and competent individual or their legal guardian for a given action relative to the individual (including the release of information). See individual entity policies.

***Contingency Plan*:** A routinely updated plan for responding to an emergency. At a minimum, it must include a data backup and disaster recovery plan.

Data Manager: University of Maryland Dental School Official and their staff who have been given operational level responsibility for the capture, maintenance, and dissemination of specific data by the appropriate Data Steward or Business Owner (Delegated Data Steward).

***Data Steward*:** The University of Maryland, School of Dentistry Executive Officer having policy-level responsibility for managing a segment of the University of Maryland, School of Dentistry's information resource as designated by the Regental by-laws. For the University of Maryland, School of Dentistry Health System, the official data steward is the Assistant Dean for Clinical Affairs.

Delegated Access Coordinator: An individual within a department or external entity designated by the Department Director (or Information Sharing Agreement, in the case of external entities) to:

1. Define, in consultation with the appropriate Data Managers, departmental access profiles for members of their department/unit by listing roles within the department and the appropriate level of access for individuals in those roles based on their need to know.
2. Notify the AAD Administrator when personnel status changes require access changes (e.g. hiring, termination, suspension, transfer). For detailed information, see University of Maryland, School of Dentistry Policy, "Information Access: Responsibilities of Department Directors or Delegated Access Coordinators".

***Directed Communication/Solicitations*:** The use of individually identifiable health information to promote fund raising, educational opportunities, special research or clinical activities, new forms of treatment, or notification of University of Maryland, School of Dentistry events. Contact with a patient to discuss or provide information

related to the above activities is not considered directed communication/solicitations if the inquiry is initiated by the patient. See University of Maryland, School of Dentistry Policy “Directed Communication/Solicitations”.

***Disclosure*:** The release of information to third parties about an individual which requires the individual's consent or release due to a legal or regulatory requirement.

Encryption: The reversible conversion of readable information into an unreadable protected form so that only a recipient who has the appropriate "key" can convert the information back into its original readable form.

***Health Information Asset*:** Any individually identifiable health information, in any form, on any medium.

Health Insurance Portability and Accountability Act (HIPAA): Federal statute requiring, among other things, the adoption of standards for the security and privacy of individually identifiable health information. Individually Identifiable Health Information - any information, including demographic and/or scheduling information collected about an individual, that:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse or any employee of the above; and
2. Relates to the past, present or future physical and/or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) Identifies the individual, or (ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

All of the following are considered by University of Maryland, School of Dentistry to fall into this category:

- Patient information collected by the University of Maryland, School of Dentistry or member information collected (e.g. transferred medical records, correspondence, telephone calls, e-mail, etc.); or
- Patient information generated by the University of Maryland, School of Dentistry or member information generated; or
- Information entrusted by the individual to a clinical staff member, employee, vendor, volunteer, student or other affiliate of University of Maryland Dental School; or
- Any knowledge a clinical staff member, employee, vendor, volunteer, student or other affiliate of University of Maryland, School of Dentistry gains in the course of fulfillment of his or her appointed role in the University of Maryland, School of Dentistry regarding the individual; or
- Research information collected, generated, maintained or disseminated by the University of Maryland, School of Dentistry that identifies individuals, or when combined with other data can reasonably lead to the identification of individuals.

***Information Asset*:** Any data in any form on any media.

Information Security Officer (ISO): That University of Maryland, School of Dentistry entity documented as formally assigned the responsibility for defining procedures to assure the security, integrity, and confidentiality of University of Maryland, School of Dentistry health information assets. This responsibility includes but is not limited to the oversight of:

- The use of security measures to protect data.
- The conduct of personnel in relation to the protection of data.
- The coordination of the AAC process and procedures with other operational entities necessary to provide for the security, integrity, and confidentiality of University of Maryland, School of Dentistry health information assets.

***Information Sharing Agreement* (Also known as, "Chain of Trust Agreement."):** A contract entered into by two parties in which they agree to exchange data while maintaining its security and confidentiality. (Part of administrative procedures to guard data integrity, confidentiality and availability.) For a description of the factors that must be present in an information sharing agreement between University of Maryland, School of Dentistry and any external entity seeking access to University of Maryland, School of Dentistry health information assets, see University of Maryland, School of Dentistry Policy, "Sharing University of Maryland, School of Dentistry Data with External Entities".

***Legally Restricted Information*:** Individually identifiable health information for which disclosure is specifically subject to additional legal requirements imposed by statute or administrative rule.

***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. "Need to Know" for further discussion and examples of this definition.

System Administrator: The individual responsible for the functions of installing, maintaining, and operating hardware and software platforms (system environments).

(The roles of system and account administrator may be combined for smaller databases.)

IV. POLICY STANDARDS

General Standards:

1. All persons with access to University of Maryland, School of Dentistry health information assets may only have such access on a need to know basis and must be approved and verified as Authorized Data Users at regular intervals (but no less than annually) by the appropriate Departmental Director (or Delegated Access Coordinator).

2. It is the responsibility of every Authorized Data User to maintain confidentiality of University of Maryland, School of Dentistry health information assets even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is public.

3. Each clinical staff member, employee, trainee, student, vendor, volunteer, or contractor, or other affiliate of the University of Maryland, School of Dentistry with access to University of Maryland, School of Dentistry health information is subject to and has the responsibilities outlined in this policy as well as those outlined in their organization's policy on confidentiality of information. For external entities, this is covered by a Business Associate Agreement, see University of Maryland, School of Dentistry Policy "Sharing University of Maryland, School of Dentistry Data with External Entities".

4. Individually identifiable health information is the property of the individual to whom the information pertains and the University of Maryland, School of Dentistry is the steward of that information and the owner of the storage medium.

5. If an Authorized Data User elects to place individually identifiable health information onto a mobile device, then the device must be registered with the Office of Information Technology. The device must be encrypted and he or she is responsible for ensuring that the device is password protected.

6. A person must be identified by the Data Steward (or Business Owner) as the Data Manager for each University of Maryland, School of Dentistry health information asset.

7. The University of Maryland, School of Dentistry Information Security Officer shall provide assistance to the University of Maryland, School of Dentistry community on interpretation of existing policy, cataloging of University of Maryland, School of Dentistry health information assets and individually identifiable health information, monitoring and tracking violations and appeals, identifying areas of

risk, defining security controls, and maintaining the AAD in collaboration with other departments that hold information about individuals' job status and access privileges.

8. All University of Maryland, School of Dentistry health information assets containing individually identifiable health information in any medium must be registered by the appropriate Data Manager in the Authorized Access Database.

9. If any University of Maryland, School of Dentistry staff member chooses to maintain a database containing individually identifiable health information generated in the course of performing professional responsibilities, he/she will be responsible as Data Manager for that database and must follow all applicable rules.

10. Individuals have the right to correct inaccurate individually identifiable health information. The appropriate process for validating and processing such corrections is determined individually by each organization, and specified in that organization's policies (see, University of Maryland, School of Dentistry Privacy Policy “Amendment of Incomplete or Incorrect Protected Health Information”). Each Data Manager is responsible for ensuring that validated correction requests relevant to University of Maryland, School of Dentistry data assets under his/her control are implemented.

11. In order to protect the individually identifiable health information entrusted to University of Maryland, School of Dentistry, all directed communication/solicitations shall adhere to University of Maryland, School of Dentistry Policy “Directed Communication/Solicitations”.

12. University of Maryland, School of Dentistry (through the ISO) shall create, administer and oversee policies to ensure the prevention, detection, containment and correction of breaches of security, integrity, and confidentiality.

13. University of Maryland, School of Dentistry,(through the ISO) shall evaluate and certify that appropriate security systems and measures are implemented. For external entities, this is part of the Information Sharing Agreement.

14. The security management process shall be the responsibility of the Business Owner, according to the guidelines set by the ISO, and must include, at a minimum, the implementation of:
(i) Risk analysis, based on information asset contents and user population, to determine the likely occurrence and severity of loss of potential incidents.
(ii) Risk management including formal, documented procedures for monitoring, detection, auditing, reporting, and responding to breaches of security, integrity, and confidentiality.

(iii) A disciplinary process including procedures for the potential discipline, up to and including dismissal, for misuse, misappropriation of data, or acts of omission or commission which result in breaches of security, integrity, or confidentiality.

15. The prevention of access to University of Maryland, School of Dentistry health information assets by unauthorized or untrained personnel shall be addressed by personnel security policies, including provisions that:
    - (i) Ensure that all personnel with access or potential access to University of
    - (ii) Maryland, School of Dentistry health information assets have gone through personnel clearance procedures — they have been screened, are specifically authorized for that access, are trained in relevant University of Maryland, School of Dentistry confidentiality policies, and have attested knowledge of and compliance with those policies.
    - (iii) (ii) Ensure that operating and maintenance personnel are given the access necessary for them to perform their system maintenance responsibilities without compromising individually identifiable health information.
    - (iv) (iii) Ensure that personnel performing maintenance activities related to University of Maryland, School of Dentistry health information assets are supervised by authorized, knowledgeable persons.
    - (v) (iv) Require maintenance of records of those granted physical access to University of Maryland, School of Dentistry health information assets.
    - (vi) (v) Employ personnel security policy and procedures.
    - (vii) (vi) Ensure that system users, including technical maintenance personnel, are trained in system security.

16. The security management process shall be the responsibility of the Business Owner, according to the guidelines set by the ISO, and must include, at a minimum, formal, documented policies and procedures to limit physical access while ensuring that properly authorized access is allowed, including contingency planning for how security is to be maintained in the event of an emergency. These controls shall include, but not be limited to:
    - (i) Applications and data criticality analysis.
    - (ii) A data backup plan.
    - (iii) Disaster recovery.
    - (iv) Emergency mode operation.
    - (v) Equipment control (into and out of site), including workstation and laptop computers.
    - (vi) A facility security plan coordinated with Campus Public Safety Office.
    - (vii) (vii) Procedures for verifying access authorizations prior to physical access.
    - (viii) Maintenance records.
    - (ix) Sign-in for visitors and escort, if appropriate.

17. To ensure that appropriate access control of University of Maryland, School of Dentistry health information assets are in place and to fulfill the obligation to keep information timely, accurate, complete, and confidential, all information systems and application programs must adhere to the following principles:
    (i) Data Stewards, Business Owners, Data Managers, Account and System
    (ii) Administrators are accountable for ensuring that the information security policies are fully executed.
    (iii) Information systems and application programs must provide a mechanism to control authentication, authorization, and audit.
    (iv) All members of the University of Maryland, School of Dentistry "community" shall be assigned a unique University of Maryland, School of Dentistry name identifier, users assigned a specified account shall be the sole user of that account and its associated identification methods; they shall not be shared. Identification methods include, but are not limited to, login names or IDs, password and pass phrases, digital certificates and signatures, PIN, tokens, smart card, biometrics (voice and finger printing), and other forms of personal identification.
    (v) Authentication shall include establishment of criteria for account eligibility, creation, maintenance, and expiration.
    (vi) When passwords are used as an authentication mechanism, a password shall be present, be of a minimal length, be changeable by the end user, be encrypted, be non-reusable (uniqueness) and have a timed forced renewal.
    (vii) Intruder detection and lockout (maximal limit of 3-5 attempts with a 15-30 minute timeout upon violation) shall be set on for the account.
    (viii) Electronic communication and exchange of health information that occurs over open networks such as the Internet must include strong authentication, adequate encryption, and effective administration of keys and passwords for encryption.
    (ix) Applications shall provide an automatic logoff/lockout after a specified period of inactivity of interaction with that application; a user shall re-authenticate to gain access to the application. The period of inactivity shall be long enough to provide for continuous user interaction with the application, yet short enough not to permit access to a possibly unattended session (no longer than 10 minutes).
    (x) One authoritative source shall hold the identifications for University of Maryland, School of Dentistry users, information systems, applications, and their processes. This authoritative source shall include the identification information of application processes which access University of Maryland, School of Dentistry health information assets for purposes of capturing, providing, and/or receiving information.

18. External data users shall have access to University of Maryland, School of Dentistry health information assets only upon the completion of an Business Associate Agreement with University of Maryland, School of Dentistry, as

described in University of Maryland, School of Dentistry Policy, "Sharing Information with External Entities".

19. There may be cases in which a state, federal, or regulatory agency requires that it be granted access to University of Maryland, School of Dentistry health information assets under law or regulation.

20. All data users shall receive education on the expectations, knowledge, and skills related to information security prior to being given access to University of Maryland, School of Dentistry health information assets. University of Maryland, School of Dentistry Information Technology Department shall verify that potential Authorized Data Users have received security education before access to University of Maryland, School of Dentistry information is granted.

21. To the extent technologically practical, system administrators shall maintain ongoing internal audit processes which record system activity such as log-ins, file accesses, and security incidents.

22. To the extent that an audit trail shows access to an individual's individually identifiable health information, it shall be made accessible to that individual at the individual's request in the event that questions arise about improper access to his or her records.

23. All Authorized Data Users, both internal and external, shall be made aware that from time to time or as indicated by events and circumstances, audits may be conducted.

24. Breaches of confidentiality under this policy are subject to appropriate disciplinary action up to and including discharge or termination of contract/relationship.

For additional information, please refer to the UMB IT Policy.