HIPAA Security Rule

Tulane University Access Authorization Policy

Department: Technology Services	**Policy Description:** Access Authorization Policy (A)
Standard: Information Access Management	**Section:** 164.308(a)(4)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-10

PURPOSE

The purpose of this policy is to establish procedures for granting access to e-PHI. This includes, for example, authorization required to access a workstation, transaction, program, process or other mechanism.

SCOPE

This policy applies to Tulane University Medical Group, its participating physicians and clinicians, and all University employees and business units who provide management, administrative, financial, legal, and operational support to or on behalf of Tulane University Medical Group and have been designated as part of the Tulane University HIPAA Health Care Component.

POLICIES AND PROCEDURES

Tulane University ensures that access to e-PHI is granted and authorized appropriately. The Information Technology (IT) Department grants access to the network and e-PHI only with specific authorization from a responsible party, such as a department head or owner of e-PHI.

Tulane University maintains two levels of access to the IDX system. The View Only Mode is the default mode assigned to each authorized user and allows individuals to view, but not to add or modify, entries in the IDX system. The Full Access Mode allows users to add, delete and modify entries within the IDX system. Only those workforce members who require full access to the IDX system in order to carry out their job responsibilities are afforded this level of access, including workforce members in the following job descriptions:

- TUHC Patient Service Coordinator
- TUHC Cancer Service Coordinator
- Central Business Office Payment Poster
- Central Business Office Refund Clerk
- IDX Master Scheduler

The Security Officer, or his designee, is responsible for determining which job functions require access to the IDX system and which workforce members within these job functions require access to the Full Access Mode. This determination is based on the IDX Security Analysis, as well as each workforce member's need to know. The principles of least privilege, the ***Minimum Necessary*** standard from the HIPAA Privacy Rule, and separation of duties, are factors that influence the access rights granted to an individual or an entity.

Access must be granted only on the basis of a valid business need and is documented. Any change in status as indicated by a Payroll Action Form process will trigger a review of access privileges.

Tulane University has determined that it would not be reasonable or appropriate to define different levels of access for e-PHI stored in locations other than the IDX system, such as personal computers or other portable devices (e.g., laptops and PDAs). Given that ownership and control of this e-PHI is dispersed among many individuals, departments, and divisions of Tulane University, it would not be practicable to establish and enforce uniform levels of access and access procedures throughout Tulane University. In addition, as described in the ***Information Security Strategy*** policy, Tulane University has determined that the e-PHI maintained on these systems generally is not as critical to the day-to-day operation of Tulane University as the e-PHI on the IDX system, and, thus, the consequences of unauthorized alteration or deletion are generally not as great. Devices containing e-PHI are password-protected as set out in the ***Password Management*** policy to ensure that only authorized workforce members have access.

RESPONSIBILITIES:

The Security Officer is responsible for ensuring the implementation of the ***Access Authorization*** policy. The Security Officer must review the access rights of individuals to ascertain that they are aligned with the individual’s job’s role or function.

Employees who violate this policy will be subject to disciplinary action up to and including termination of employment. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or the Security Officer. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, every effort will be made to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment.

IMPLEMENTATION SPECIFICATION:

§ 164.308 Administrative safeguards.

(a) A covered entity must, in accordance with § 164.306:
(4)(i) Standard: **Information access management**. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
(ii) Implementation specifications:
(B) **Access authorization** (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.