HIPAA Security Rule

Tulane University Unique User Identification Policy

Department: Technology Services	**Policy Description:** Unique User Identification (R)
Standard: Access Control	**Section:** 164.312(a)(1)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-34

PURPOSE

The purpose of this policy is to assign a unique name and/or number for identifying and tracking user identity.

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 assigns each individual who accesses e-PHI to a unique user identification or login ID.

Tulane University records each unique user identifier that is issued and updates the list as new users are added. In an effort to discourage sharing of user IDs on certain commonly used applications, Tulane University makes a concerted effort to add new identifiers for new users quickly. Requests for group user IDs are denied unless it can be shown that the information system at issue does not contain any e-PHI.

Workforce members are instructed on the importance of confidentiality of user IDs and not allowing anyone else to use their unique ID.

All user IDs for temporary employees are disabled as of the date of termination. To ensure that malicious users have no access to “open” user IDs, those user IDs that are not currently being used, accounts are disabled after 91 days of inactivity.

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the ***Data Backup and Storage*** policy. All workforce members are responsible for maintaining the confidentiality of their user IDs.

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:

§ 164.312 Technical safeguards.

(a) A covered entity must, in accordance with § 164.306:
(a)(1) Standard: **Access control**. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
(2) Implementation specifications:
(i) **Unique user identification** (Required). Assign a unique name and/or number for identifying and tracking user identity.