HIPAA Security Rule

Tulane University Password Management Policy

Department: Technology Services	**Policy Description:** Password Management (A)
Standard: Security Awareness and Training	**Section:** 164.308(a)(5)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-15

PURPOSE

The purpose of this policy is to implement procedures for creating, changing and safeguarding passwords.

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 requires that:

- All passwords be changed at least once every 6 months, or immediately if a breach of a password is suspected;
- User accounts that have system-level privileges granted through group memberships or programs have a unique password from all other accounts held by that user;
- Passwords not be inserted into email messages or other forms of electronic communication;
- Personal Computers and other portable devices such as Laptops and PDAs which may contain e-PHI must be password protected, and when possible, encrypt the e-PHI;
- Default vendor passwords be changed immediately upon installation of hardware or software; and,
- Where the Simple Network Management Protocol (SNMP) is used, the community strings be defined as something other than the standard defaults of “public,” “private,” and “system,” and be different from the passwords used to log in interactively. A keyed hash must be used where available (for example, SNMPv2).

Users must select strong passwords which must be at least 8 characters long and contain at least three of the following four character groups:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numerals (0 through 9)
- Non-alphabetic characters (!, $, #, %, etc.)

Training is provided to all workforce members regarding password management, including the following

topics:

- The process for creating and changing passwords, consistent with the above guidelines
- The importance of not maintaining a paper record of passwords
- The significance of keeping passwords confidential, using different passwords for different accounts and not including passwords in any automated log-in process
- The importance of logging off before leaving a workstation

If someone demands a password, workforce members must refer them to this document or have them call someone in the Information Security Department or contact the Security Officer.

Members of the workforce must not store passwords in an unsecured area. Passwords must not be stored on ANY computer system (including Palm Pilots or similar devices) without encryption.

RESPONSIBILITIES:

The Security Officer is responsible for ensuring the implementation of the ***Password Management*** policy.

Password cracking or guessing may be authorized to be performed on a periodic or random basis by the Security Officer. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Members of the workforce must not share their passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

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:
(5)(i) Standard: **Security awareness and training**. Implement a security awareness and training program for all members of its workforce (including management).
(ii) Implementation specifications. Implement:
(D) **Password management** (Addressable). Procedures for creating, changing, and safeguarding passwords.