HIPAA Security Rule

Tulane University Person or Entity Authentication Policy

Department: Technology Services	**Policy Description:** Person or Entity Authentication (R)
Standard: Person or Entity Authentication	**Section:** 164.312(b)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-40

PURPOSE

The purpose of this policy is to implement procedures to verify that the person or entity seeking access to e-PHI is the one claimed.

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

Authentication is the mechanism that verifies that an individual is who they claim to be. It is the first step in gaining access to any secured computing environment and is the basis for allowing or denying access to sensitive information. Authentication is based on one or more of the three following factors:

- Something that the person knows such as a password
- Something that the person has such as a smart card or token
- Something the person is such as a fingerprint.

This policy sets a minimum acceptable level of authentication for users or entities at Tulane University.

Tulane University limits authentication attempts to its e-PHI maintained in the IDX system to no more than three unsuccessful attempts in direct access mode. There is no limit of unsuccessful attempts in Web access mode; however, each unsuccessful attempt in Web mode is logged. Authentication attempts that exceed the limit result in:

- Disabling of relevant account for a period of time
- Logging of event
- Notification to the departmental security officer.

Tulane University immediately removes authentication credentials for persons or entities no longer requiring access to e-PHI and periodically validates that no redundant authentication credentials have been issued. Authentication credentials are protected by passwords**.** Workforce members are instructed to keep

authentication credentials confidential.

With respect to e-PHI maintained in locations other than the IDX system, Tulane University verifies that a person or entity seeking access to e-PHI is the one claimed by requiring strong password protection as indicated in the ***Password Management Policy***.

RESPONSIBILITIES:

All individuals identified in the scope of this policy are responsible for:

- Using, as instructed, any authentication method required by the Security Officer
- Abiding by all requirements set forth for the protection of passwords at Tulane University.

The Tulane University Security Officer is responsible for:

- Evaluating and implementing strong authentication solutions when appropriate.
- Ensuring the password administration options of all software packages are set to reflect the password requirements outlined above
- Monitoring compliance of the workforce to this policy and responding to any security incidents which may arise from it

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:
(d) Standard: **Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.