HIPAA Security Rule

Tulane University Encryption Policy

Department: Technology Services	**Policy Description:** Encryption (A)
Standard: Transmission Security	**Section:** 164.312(e)(1)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-42

PURPOSE

The purpose of this policy is to implement a mechanism to encrypt e-PHI during transmission over electronic communications networks whenever deemed appropriate.

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 uses encryption to protect the confidentiality, integrity and availability of e-PHI during transmission over electronic communications networks. Tulane University protects “data in motion” by implementing a combination of solutions that includes Virtual Private Networks (VPNs), Secure Sockets Layer (SSL) and other encryption technologies where appropriate.

Based on its risk analysis, Tulane University has determined that it would be reasonable and appropriate to encrypt e-PHI transmissions with respect to the IDX billing system.

Tulane University utilizes the following technologies to encrypt e-PHI

- Triple DES (3DES) via VPN tunnel

All encryption and decryption capabilities of products and systems have been tested to ensure proper functionality.

Based on its risk analysis, Tulane University has determined that it would not be reasonable and appropriate to require encryption of all e-PHI transmissions not relating to the IDX billing system, such as all emails. If a workforce member sends e-PHI that they believe requires additional protections based on amount, sensitivity, or other considerations, he or she should contact the Security Officer for guidance on encryption options.

RESPONSIBILITIES:

The Security Officer is responsible for implementing this policy and for overseeing the technologies used to encrypt e-PHI that is being transmitted over an electronic communications network.

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:
(e)(1) Standard: **Transmission security**. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
(2) Implementation specifications:
(ii) **Encryption** (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.