HIPAA Security Rule

Information Security Strategy

Department: Technology Services	**Policy Description:** Information Security Strategy
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-A1

PURPOSE

The purpose of this policy is to establish reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability of Tulane University's e-PHI by protecting e-PHI from unauthorized access, modification, destruction, or disclosure.

The purpose of the Tulane University Information Security Program is to:

- Establish policies, procedures, plans, and standard tools to secure information in compliance with state and federal security requirements, using minimum levels of industry standards.
- Support Tulane University's mission to provide continuity of service to patients.
- Maintain unbroken trust with patients and stakeholders through practice of good stewardship of information assets.

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 maintains an Information Security Program that complies with core business objectives as well as applicable state and federal regulations. The Information Security Program is a reflection of Tulane University's commitment to ensuring the confidentiality, integrity, and availability of e-PHI. Towards this end, Tulane University implements administrative, physical and technical safeguards as is reasonable and appropriate to protect its e-PHI. Tulane University ensures compliance with the Information Security Program by its workforce members.

Tulane University's Information Security Program addresses the standards described in the Security Rule by establishing policies and procedures to meet each one of the implementation specifications as reasonable and appropriate. Policies and procedures are reviewed and evaluated (based on any environmental and operational changes) on an annual basis by the Security Officer and his team. Policies and procedures are updated or added as necessary. Tulane University also repeats all required analyses of its information systems (e.g. risk analysis) periodically and in response to environmental and operational changes, as described in the ***Evaluation Policy***.

Tulane University is committed to complying with each one of the standards set out in the Security Rule, as described below. To meet these standards, Tulane University follows separately documented plans, policies and procedures and regularly analyzes its informational systems as described in the documents referenced below. These policies apply to all e-PHI maintained by Tulane University, as defined in the ***Glossary of Terms***. Because of the importance of the IDX system to the Tulane University Medical Group and its patients, and because of the amount and nature of the e-PHI maintained on the IDX system, Tulane University follows additional security procedures with respect to the IDX system, as more fully set forth in the ***FPP Information System Policies***.

Administrative Safeguards

Standard: Security Management Process

Tulane University takes reasonable steps to ensure the confidentiality, integrity and availability of e-PHI by implementing appropriate and reasonable policies, procedures and controls to prevent, detect and correct security violations. These steps include:

- As part of its ***Risk Analysis***, Tulane University identified and prioritized risks to the confidentiality, integrity and availability of e-PHI.
- Tulane University implemented measures to reduce the risks to e-PHI to appropriate and reasonable levels, as described in the ***Risk Management*** document.
- Under its ***Sanction*** policy, Tulane University applies appropriate sanctions against workforce members who fail to comply with its security policies and procedures.
- In its ***Information System Activity Review*** policy, Tulane University implements procedures to review records of activity on e-PHI Systems.

Standard: Assigned Security Responsibility

Tulane University takes reasonable steps to assign responsibility for its Information Security Program by identifying a Security Officer who is responsible for development and implementation of the policies and procedures. The responsibilities of the Security Officer are described in the ***Assigned Security Responsibility*** document.

Standard: Workforce Security

Tulane University ensures the confidentiality, integrity and availability of e-PHI by implementing reasonable safeguards to ensure that all members of its workforce have appropriate access to e-PHI, while preventing those workforce members who do not have access from obtaining access to e-PHI. Tulane University has established the following policies and procedures as part of its commitment to complying with this standard:

- In accordance with its ***Authorization and/or Supervision*** policy, Tulane University ensures that workforce members who work with or have the ability to access e-PHI are properly authorized and/or supervised.
- In accordance with its ***Workforce Clearance*** procedure, Tulane University's workforce members are screened during the hiring process.
- In accordance with its ***Termination*** procedures, Tulane University implements a documented process for terminating access to e-PHI when employment of workforce members ends or when access is no longer appropriate under Tulane University's ***Information Access Management*** and ***Access Establishment and Modification*** policies.

Standard: Information Access Management

Tulane University maintains and reviews documented policies and procedures for authorizing access to e-PHI in a manner consistent with the Security Rule. Access to e-PHI is determined and authorized by Tulane University's information systems owners, managers and/or supervisors of data users or their delegates. Access to e-PHI is only granted to workforce members who require access to specific information to accomplish their work responsibilities, and is granted on a need-to-know basis. Tulane University has established the following policies and procedures as part of its commitment to complying with this standard:

- Tulane University maintains that it has no clearinghouse functions, as described in its

Isolating Healthcare Clearinghouse Functions document.

- As described in its ***Access Authorization*** policy, Tulane University has a documented process for authorizing the appropriate access to e-PHI.
- Tulane University's process for establishing, documenting, reviewing and modifying access to e-PHI is set out in its ***Access Establishment and Modification*** policy.

Standard: Security Awareness And Training

Tulane University is committed to providing security awareness and training to its workforce members who have access to e-PHI, including management, on an on-going basis. Workforce members are provided with training and supporting reference material to enable them to appropriately protect e-PHI. Tulane University's security awareness and training includes:

- In accordance with its ***Security Reminders*** policy, Tulane University provides security information and awareness to its workforce members.
- Tulane University trains and reminds its workforce members about the processes for guarding against, detecting and reporting malicious software that poses risks to e-PHI in accordance with its ***Protection from Malicious Software*** policy.
- In accordance with its ***Log-In Monitoring*** policy, Tulane University trains and reminds its workforce members about the processes for monitoring log-in attempts and reporting discrepancies.
- In accordance with its ***Password Management*** policy, Tulane University trains and reminds its workforce members about the processes for creating, changing and protecting passwords.

Standard: Security Incident Procedures

Tulane University is committed to promptly identifying, reporting and responding to security incidents.

- In accordance with its ***Response and Reporting*** policy, Tulane University identifies and responds to suspected or known security incidents and mitigates, to the extent practicable, harmful effects of known security incidents. Security incidents and their outcomes are documented pursuant to the procedures described in this policy.

Standard: Contingency Plan

Tulane University ensures the confidentiality, integrity and availability of e-PHI by preparing for and responding to emergencies or disasters that damage systems containing e-PHI. Tulane University takes reasonable steps to ensure that critical data will survive a disaster or other emergency and provides training to workforce members about Tulane University's disaster and emergency response procedures. Tulane University has established the following policies, procedures and plans as part of its commitment to complying with this standard:

- In accordance with its ***Data Backup*** plan, Tulane University backs up and stores copies of e-PHI.
- Through its ***Disaster Recovery*** plan, Tulane University implements procedures to recover e-PHI if impacted by a disaster or other emergency.
- In accordance with its ***Emergency Mode Operation*** plan, Tulane University takes reasonable steps to ensure the continuance of critical business processes that protect the security of e-PHI during and immediately following a disaster or other emergency.
- In accordance with its ***Testing And Revision*** procedures, Tulane University completes testing of its disaster recovery procedures and, if necessary, takes reasonable steps to ensure that such procedures are up to date and effective.
- In accordance with its ***Applications and Data Criticality Analysis*** policy, Tulane University has a process to identify and define the criticality of applications and data on e-PHI Systems.

Standard: Evaluation

Tulane University conducts periodic technical and non-technical evaluations of its security safeguards, including policies, controls and processes in order to demonstrate and document the extent of its compliance with its security policies and the Security Rule. Reevaluations are conducted in response to environmental or operational changes that might impact the confidentiality,

integrity or availability of e-PHI. Tulane University's evaluation procedures are documented in the ***Evaluation*** policy.

Physical Safeguards

Standard: Facility Access Controls

Tulane University limits physical access to e-PHI Systems and the facilities in which they are located while taking reasonable steps to ensure that properly authorized workforce members have access to such e-PHI Systems and facilities. Tulane University ensures, where possible, that e-PHI Systems are located in areas where physical access can be controlled in order to minimize the risk of unauthorized access. Tulane University takes reasonable steps to ensure that the level of protection provided for the e-PHI Systems, as well as the facilities in which they are housed, is commensurate with that of the identified threats and risks. Tulane University has established the following policies and procedures as part of its commitment to complying with this standard:

- As documented in its ***Contingency Operations*** policy**,** Tulane University has a procedure for allowing authorized workforce members to enter its facilities to take the necessary actions documented in its ***Disaster Recovery*** plan and ***Emergency Mode Operations*** plan.
- Tulane University's ***Facility Security*** plan details how it will protect its equipment and facilities in which e-PHI Systems are located from unauthorized physical access, tampering and theft.
- Through its ***Access Control and Validation*** procedures, Tulane University controls and validates workforce members' access to Tulane University's facilities based on their roles or functions.
- In accordance with its ***Maintenance Records*** policy, Tulane University documents repairs and modifications to the physical components of its facilities that are related to security.

Standard: Workstation Use

Tulane University maximizes the security of e-PHI by delineating the proper usages for each workstation, specifying which workstations are authorized to access e-PHI, and restricting all other workstations from gaining access to e-PHI. In accordance with its ***Workstation Use*** policy, Tulane University implements safeguards to confirm that workstations are used only for authorized purposes and prevents unauthorized access to e-PHI.

Standard: Workstation Security

Tulane University has implemented safeguards to prevent physical access by unauthorized users to workstations that can access e-PHI while ensuring that authorized workforce members have the appropriate access. These safeguards are described in Tulane University's ***Workstation Security*** document.

Standard: Device and Media Controls

Tulane University takes reasonable steps to protect, account for, properly store, back up and dispose of its hardware and electronic media in accordance with specific procedures. Tulane University takes reasonable steps to track all incoming hardware and electronic media and transfers of hardware and electronic media as they are moved into, out of and within its facilities. Tulane University has established the following policies and procedures as part of its commitment to complying with this standard:

- In accordance with its ***Disposal*** policy, hardware and electronic media that contain e-PHI are disposed of properly when no longer required.
- In accordance with its ***Media Re-Use*** policy, Tulane University removes e-PHI before electronic media are made available for re-use.
- In accordance with its ***Accountability*** policy, Tulane University logs and tracks hardware and electronic media that are received, removed from or moved within its facilities
- In accordance with Tulane University's ***Data Backup and Storage*** policy, hardware and electronic media are backed up and stored in a secure manner.

Technical Safeguards

Standard: Access Control

Tulane University takes reasonable steps to ensure that e-PHI Systems support and are installed with technical safeguards to control access to such e-PHI Systems in order to comply with Tulane University's ***Access Authorization*** and ***Access Establishment and Modification*** policies. Tulane University has implemented the following technical policies and procedures to ensure that only those persons or software programs that are authorized have access to systems that maintain e-PHI:

- In accordance with its ***Unique User Identification*** policy, Tulane University grants access to e-PHI Systems via unique user identifiers (user IDs) that identify individual workforce members' identity and enable tracing of activities performed on e-PHI Systems to an individual workforce member.
- Tulane University's ***Emergency Access*** procedure delineates the necessary steps for authorized workforce members to obtain access to e-PHI during an emergency.
- In accordance with its ***Automatic Logoff*** policy, Tulane University's workforce members end electronic sessions on e-PHI Systems when such sessions are completed, unless they can be secured through locking mechanisms. In addition, Tulane University has implemented electronic procedures on e-PHI Systems to terminate sessions after a period of inactivity.
- As described in Tulane University's ***Encryption and Decryption*** documentation, encryption is used to protect the confidentiality, integrity and availability of e-PHI when determined to be necessary by the ***Risk Analysis*** and ***Risk Management*** results.

Standard: Audit Controls

Tulane University implements appropriate hardware, software or procedural mechanisms on its information systems to enable review of information system activity on an ongoing basis. These mechanisms are described in Tulane University's ***Audit Controls*** policy.

Standard: Integrity

Tulane University is committed to protecting e-PHI from unauthorized modification or destruction. In order to comply with this standard, Tulane University has implemented the following policy

- In accordance with its ***Mechanism to Authenticate Electronic Protected Health Information*** policy, Tulane University takes reasonable steps to ensure that e-PHI is protected from unauthorized modification or destruction.

Standard: Person Or Entity Authentication

Tulane University ensures the confidentiality, integrity and availability of e-PHI by taking reasonable steps to ensure that any person or entity requesting access to e-PHI is authenticated prior to obtaining access. Tulane University verifies the identity of any person or entity requesting access to e-PHI prior to granting access, as described in its ***Person or Entity Authentication*** policy.

Standard: Transmission Security

Tulane University implements technical security measures to guard against unauthorized access to e-PHI that is being transmitted over an electronic communications network. Tulane University has established the following policies and procedures as part of its commitment to complying with this standard:

- In accordance with its ***Integrity Controls***, Tulane University utilizes integrity controls to protect the integrity of e-PHI while it is being transmitted over electronic communications networks, as deemed necessary from the ***Risk Analysis***. Such integrity controls ensure that electronically protected e-PHI is not improperly modified without detection.
- As described in its ***Encryption*** policy, Tulane University encrypts e-PHI while it is being transmitted over electronic communications networks.

Organizational Framework

Standard: Policies and Procedures
As described in its ***Policies and Procedures*** document, Tulane University has established and implemented organizational policies and procedures to address the requirements of the Security Rule, as well as informed its workforce members about the policies and procedures that apply to them generally and their individual roles.

Standard: Documentation
Tulane University maintains written documentation of the policies and procedures that it implements to comply with the Security Rule. In accordance with its ***Documentation*** policy, Tulane University maintains such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later, makes documentation available to those workforce members responsible for implementation of required procedures and reviews and updates documentation periodically.

RESPONSIBILITIES:

All individuals, groups, and organizations identified in the scope of this policy are responsible for:

- Compliance with all security policies

The Security Officer is responsible for:

- The development, implementation, and maintenance of Tulane University security policies
- Working with employees to develop procedures and plans in support of security policies

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.