HIPAA Security Rule

Tulane University Response and Reporting Policy

Department: Technology Services	**Policy Description:** Response and Reporting (R)
Standard: Security Incident Procedures	**Section:** 164.308(a)(6)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-16

PURPOSE

The purpose of this policy is to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to Tulane University; and, document security incidents and their outcome.

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

This policy is an action plan for dealing with intrusions, cyber-theft, fires, floods, denial of service and other security related events and involves the following seven steps:

1. Preparing for a Security Incident
2. Detecting and Reporting Security Incidents
3. Assembling the Incident Response Team
4. Limiting Further Damage
5. Gathering Evidence
6. Fixing the Damage
7. Analyzing the Incident

Step 1: Preparing for a Security Incident

Every network will at some point be a victim of a computer security incident. System and network administrators must be prepared for security incidents and be able to respond quickly to minimize and repair the damage. Tulane University has taken the following steps in preparation for a security incident:

- *Identification of the Security Incident Response Team ("SIRT")* – the Security Officer, Privacy Official, Director of Network Services and others as appointed by the CIO.
- *Acquisition of specialized security training* – All members of the SIRT were trained on how to respond to a computer security incident, including the reporting process, disaster recovery plan and other protocol.

- *Verification of the deployment of Intrusion Detection Systems (IDS)* – The SIRT is responsible for periodically verifying that the IDS is enabled.
- *Verification of Data Backup Plan and its implementation* – The SIRT received training concerning the data backup plan and periodically tests it to ensure operation.
- *Identification of management contacts* – The SIRT has a list of senior management and legal department members to contact in case of a severe emergency.

Step 2: Detecting and Reporting Security Incidents

As soon as security incidents are detected they should be immediately reported to the SIRT or the Security Officer.

Tulane University has developed a formal reporting procedure to alert the SIRT of a security incident. All employees and contractors are made aware of the procedure for reporting security incidents, and are required to report such incidents as quickly as possible. When deemed appropriate by the Security Officer, those individuals who report incidents are notified of results after the incident has been dealt with and closed. Moreover, the IT Department may use these incidents in user awareness training as examples of what could happen, how to respond to such incidents, and how to avoid them in the future.

All users of information services are trained to note and report any observed or suspected security weaknesses in, or threats to, systems or services, as well as malfunctions in hardware, software, or other systems. Such matters are reported either to management or to the Security Officer as quickly as possible. Users are informed that they should not, in any circumstances, attempt to prove a suspected weakness. This is for their own protection, as testing weaknesses might be interpreted as a potential misuse of the system. Members of the IT Department are also instrumental in early identification of incidents by tracking help calls, unexplained entries into log files, system crashes, and poor network performance.

In addition, there is an incident response procedure, setting out the action to be taken on receipt of an incident report.

Step 3: Assembling the Security Response Team

Upon notification of an incident, the SIRT must meet to evaluate and determine the incident's potential cause. Once it is confirmed that a security incident has occurred, the SIRT will take appropriate steps, which may include one or more of the following:

- Noting the symptoms of the problem and any messages appearing on the screen
- Isolating the computer, if possible, and ensure that use of it is stopped immediately
- Immediately reporting the incident to the chief information officer.

Users must not attempt to remove any suspected software unless authorized to do so. Appropriately trained and experienced staff authorized by the SIRT is responsible for carrying out recovery activities.

Step 4: Limiting Further Damage

Once the initial data has been collected, immediate steps need to be taken to minimize the spread of the damage. These steps may include disabling Internet access as well as disabling file servers, email servers, communication devices and other systems. Any workstation(s) impacted should be isolated, if possible, and their use stopped. If equipment is to be examined, it should be disconnected from any organizational networks before being re-powered. Diskettes and other media should not be transferred to other workstations. If the incident involved unauthorized access, any potentially compromised password should be changed immediately.

Step 5: Gathering Evidence

The SIRT must gather all possible evidence to fully understand the type of attack and its scope. The team needs to address questions such as:

- How many systems are impacted?
- What levels of privileges were accessed?
- How widespread is the vulnerability?
- How far into the internal systems did the intruder get?
- Which systems have been compromised, including:
    - The hardware addresses of the compromised systems
    - The system names
    - The IP addresses of the compromised systems
    - Any e-PHI data processed by those systems
    - Any applications installed on the systems
    - The location of the systems
- Any risk to e-PHI stored by systems?
- Was the incident accidental or intentional?

All of the information collected must be thoroughly documented and reported. Dedicated systems must be used for incident analysis and forensics. The involved personnel will be appropriately trained before using such applications.

Finally, the SIRT must make a copy of all evidence.

Step 6: Fixing the Damage

Having gathered all the evidence, the SIRT must get involved in leading eradication efforts before putting the system back online, including:

- Deleting, removing or replacing malicious files
- Testing potentially compromised machines to determine that they are working properly
- Modifying or re-creating user accounts and associated passwords if there was any evidence of unauthorized access.
- Restoring data from trusted backups.

After the impacted systems are cleaned and protected, they may be brought back online. All such systems and infrastructure must be monitored for other similar, subsequent incidents.

Step 7: Analyzing the Incident

After the incident has been resolved; the SIRT re-groups to do a post-event de-briefing. The objective is to assess the incident and the response, and to identify any specific areas of concern. The team must have a full and complete understanding of the incident and how to prevent such incidents from occurring in the future.

The SIRT must attempt to quantify and monitor the types, volumes and costs of incidents and malfunctions. This information will be used to identify recurring or high impact incidents or malfunctions. This may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, and may be taken into account in the security policy review process.

The SIRT will use this analysis to make recommendations to management on how to prevent similar incidents. At management's request, this will be in the form of a written report and include a factual background and account of steps taken, as well as recommendations for any improvements to processes and procedures.

RESPONSIBILITIES:

The Security Officer has ultimate responsibility for determining the appropriate level of response to a security incident. All such response must be in accordance with established policies and procedures. At a minimum, the Security Officer and/or his/her team must immediately consider a response that includes the steps listed above.

Members of the workforce will immediately report any and all suspected violations of information security to the Security Officer.

All incident reporting and response activities must be conducted strictly on a need-to-know basis.

The Security Incident Report to be completed by the Security Officer or a member of his/her team will include as much information as possible about the following:

- Contact information of the person reporting the incident (name, phone, address, email)
- Date and time of the incident
- Detailed description of the incident
- Any further information, such as unusual activities or individuals associated with the incident

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:
(6)(i) Standard: **Security incident procedures**. Implement policies and procedures to address security incidents.
(ii) Implementation specifications:
Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.