

**THE TEXAS A&M UNIVERSITY SYSTEM  
HEALTH SCIENCE CENTER INTERNAL POLICIES**

---

**16.99.99.Z0.25                      Security of Electronic Medical Records Internal Policy**

*Approved January 26, 2011*

---

**1. GENERAL/OVERVIEW**

This policy applies to TAMHSC health care providers, its participating physicians and clinicians, employees and business units who provide management, administrative, financial, legal, and operational support to or on behalf of the health care provider and has been designated as a member of the TAMHSC Health Care Component. This policy pertains to protected health information covered by the TAMHSC Health Care Component's Notice of Privacy Practices.

**2. INTERNAL POLICY/RESPONSIBILITIES**

It is the policy of the TAMHSC to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Only designated units, departments or Entities that have been designated as part of the TAMHSC Health Care Component that manage electronic protected health information (EPHI) are subject to the HIPAA Security Rule<sup>1</sup> Regulations. This policy addresses the final HIPAA Security Rule which is effective April 21, 2005. Each covered component within the TAMHSC Health Care Component is responsible for adopting site-specific procedures and controls to address this policy.

The HIPAA Security Rule requires the TAMHSC Health Care Component to put into place appropriate administrative, technical and physical safeguards to protect the integrity, confidentiality and availability of electronic protected health information (EPHI) that is created, received or managed by the TAMHSC Health Care Component. Therefore, the TAMHSC Office of Information Technology (Information Security Officer) and each TAMHSC Health Care Component shall develop and implement the necessary requirements to ensure compliance.

**3. PROCESS**

**3.1 Electronic Protected Health Information (EPHI).**

- 3.1.1 EPHI includes any computer data relating to the past, present or future physical or mental health, health care treatment, or payment for health care.
- 3.1.2 EPHI includes information that can identify an individual and includes such information transmitted or maintained in electronic format.

3.1.2.1 Name

3.1.2.2 Social security number

3.2.2.3 Address

3.2.2.4 Date of birth

3.2.2.5 Medical history or medical record number

### 3.1 Exclusions.

3.1.1 Certain education and student treatment records are not considered Electronic Protected Health Information.

3.1.2 Student education records, including medical records (which are protected under the Buckley Amendment).

3.1.3 Medical records of employees received by the TAMHSC in its capacity as an employer.

3.1.4 Workers' compensation records. Although these records are not covered under the HIPAA Privacy or Security Rules, other A&M System Policies cover the confidentiality and security of these materials.

3.1.5 There are special provisions in the law governing the release of psychotherapy records.

### 3.2 Security Measures.

3.2.1 The following security measures address the 20 required standards of the HIPAA Security Rule that the TAMHSC Health Care Component must comply with respect to EPHI. Each covered component must review and modify their security measures as needed to sustain the reasonable and appropriate protection of EPHI's confidentiality, integrity and availability. Implementation of control solutions to address the 20 standards should be reasonable and appropriate, taking into account the following.

3.1.1.1 The size, complexity and capabilities of the covered component.

3.1.1.2 The covered component's technical infrastructure, hardware, and software security capabilities.

3.1.1.3 The costs of security measures.

3.1.1.4 The probability and criticality of potential risk to EPHI.

### 3.3 Administrative Safeguards.

#### 3.3.1 Annual Risk Analysis.

3.3.1.1 Pursuant to HIPAA Section 164.308(a)(1), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component shall conduct an annual Risk Analysis, which will provide an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI managed by the covered component.

3.3.1.2 This risk analysis is to be presented to the covered component's management, which will provide a documented response, including remediation steps, for any identified risks.

### 3.4 Risk Management.

3.4.1 Pursuant to HIPAA Section 164.308(a)(1), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will implement measures to reduce computer risks and vulnerabilities including the following.

3.4.1.1 Identifying and documenting potential risks and vulnerabilities that could impact systems managing EPHI.

3.4.1.2 Performing annual technical security assessments of systems managing EPHI in order to identify and remedy detected security vulnerabilities.

3.4.1.3 The documented results of these security assessments will be presented to the covered component's management, which will provide a documented response, including remediation steps, for any identified vulnerabilities.

### 3.5 Sanctions Policy.

3.5.1 Pursuant to HIPAA Section 164.308(a)(1), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will adhere to the sanctions statement found in this policy.

### 3.6 Information System Activity Review.

3.6.1 Pursuant to HIPAA Section 164.308(a)(1), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will periodically review information system activity records, including, audit logs, access reports, and security incident tracking reports to ensure that implemented security controls are effective and that EPHI has not been potentially compromised. Measures should include the following.

- 3.6.1.1 Enabling logging on computer systems managing EPHI.
- 3.6.1.2 Developing a process for the review of exception reports and/or logs.
- 3.6.1.3 Developing and documenting procedures for the retention of monitoring data.
- 3.6.1.4 Log information should be maintained for up to six years, either locally on the server or through the use of backup tapes.
- 3.6.1.5 Periodically reviewing compliance to security policies and procedures. The documented results of these compliance reviews should be presented to the covered component's management, which will provide a documented response, including remediation steps, for any identified lapses in compliance.

### 3.7 Assigned Security Responsibility.

- 3.7.1 Pursuant to HIPAA Section 164.208(a)(2), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will identify a security official responsible for the adherence to this policy and to the implementation of procedures required to protect the confidentiality, integrity and availability of EPHI.

### 3.8 Workforce Security.

- 3.8.1 Pursuant to HIPAA Section 164.308(a)(3), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will establish procedures that ensure only authorized personnel have access to systems that manage EPHI. Measures that each covered component should address include the following.
  - 3.8.1.1 Establishing a procedure that requires managerial approval before any person is granted access to systems managing EPHI.
  - 3.8.1.2 Performing appropriate background checks, where appropriate, before any person is granted access to systems managing EPHI.
  - 3.8.1.3 Limiting authorized persons' access to EPHI to the extent that access to this information achieves the requirements of the person's job responsibilities.
  - 3.8.1.4 Implementing procedures for terminating access to EPHI when the employment of a person ends or the job responsibilities of the person no longer warrants access to EPHI. These procedures should include

changing of locks/combinations if necessary, removal from logical and physical access lists, account disablement, deletion of personal files, and the return of security items (such as keys, access cards, and laptops).

3.8.1.5 Periodically reviewing the accounts on systems managing EPHI to ensure that only currently authorized persons have access to these systems.

### 3.9 Information Access Management.

3.9.1 Pursuant to HIPAA Section 164.308(a)(4), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will establish procedures that ensure systems that manage EPHI have authorization controls that allow only authorized personnel access. Measures that each covered component should address include the following.

3.9.1.1 Workstations interfaces, applications, processes or other computer-based mechanisms for accessing EPHI that provide authorization controls which can ensure appropriate access based on authorized personnel's job role.

3.9.2 Ensuring that these systems require a unique identification/authentication mechanism with appropriate formats. Social security numbers should not be used as an identification/authentication mechanism.

3.9.3 Ensuring that these systems have password management features that enforce the use of passwords as part of the identification/authentication mechanism.

3.9.4 Ensuring that controlled privileged user accounts can be established (e.g. system administrators who typically require higher levels of access to EPHI).

### 3.10 Security Awareness and Training.

3.10.1 Pursuant to HIPAA Section 164.308(a)(5), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will undertake the following.

3.10.1.1 Having the covered component's security official receive periodic security updates.

3.10.1.2 Having all members of the Health Care Component take the TAMHSC Health Care Component HIPAA training course.

3.10.2 Ensuring procedures and logging mechanisms are in place for the security officer to receive alerts notifying of failed log-in attempts from unauthorized users. Users should be educated to note if unauthorized access has been

attempted (such as changed passwords and locked-out accounts, or noticing that a different username has been entered into a logon field).

### 3.11 Password Management.

3.11.1 Pursuant to HIPAA Section 164.308(a)(5), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will ensure the following controls are in place for creating, changing and safeguarding passwords on systems managing EPHI.

3.11.1.1 Passwords must be at least 8 characters long, include a varied set of characters (such as the use of numbers and symbols).

3.11.1.2 Passwords must not be shared.

3.11.1.3 Passwords must not be written down and stored in locations where they can be found.

3.11.1.4 Passwords must not use any word found in any dictionary or proper name.

3.11.1.5 Passwords must be forced to change periodically, and must be changed immediately if compromised.

### 3.12 Security Incident Procedures.

3.12.1 Pursuant to HIPAA Section 164.308(a)(6), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component must have procedures in place so that their security official is notified when a system managing EPHI is involved in a security incident (examples include virus or worm infection, accounts being compromised, and servers damaged from a denial of service attack).

### 3.13 Contingency Plan.

3.13.1 Pursuant to HIPAA Section 164.308(a)(7), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component must have procedures in place to respond to an emergency or other occurrence (such as fire, flood, vandalism, and unrecoverable hardware failures) that damages systems managing EPHI. Measures that each covered component should address include the following.

3.13.1.1 Having procedures for creating and maintaining backups of EPHI adequate to both restore EPHI and the systems maintaining this data.

- 3.13.1.2 Establishing procedures to restore any loss of data due to a disaster. At a minimum, each TAMHSC Health Care Component should maintain backup tapes at an off-site location that can be used to restore EPHI and the systems maintaining this data.
- 3.13.1.3 In the case of a system that maintains EPHI that has been identified by the annual HIPAA risk analysis as critical to business, medical or academic operations, the covered component should have a documented and tested disaster recovery plan for all critical server-based systems, communications, and infrastructure items (such as e-mail, voice-mail, fax server, etc.). This disaster recovery plan should be appropriate in scope, reflect recent system updates, include crisis management team changes, and include the latest results of the covered component's disaster recovery test.
- 3.13.1.4 In the case of a system that maintains EPHI that has been identified by the annual HIPAA risk analysis as critical to business, medical or academic operations, the Health Care Component should have an emergency mode operation plan that enables continuation of critical process to assure access to EPHI and provide for adequate protection of the security of EPHI while operating in emergency mode.
- 3.13.1.5 In the case of a system that maintains EPHI that has been identified by the annual HIPAA risk analysis as critical to business, medical or academic operations, and thereby requiring a disaster recovery plan, the covered component should perform yearly recovery tests to ensure the effectiveness of the plan as well as to provide training and experience to those persons responsible for implementing a disaster recovery plan.
- 3.13.1.6 A recovery test should also be performed following significant changes to systems maintaining EPHI. Results of the testing should be presented to the covered component's management, which will provide a documented response, including remediation steps, for any identified deficiencies with the disaster recovery plan. During testing, the covered component should ensure that appropriate security measures are in place to prevent unauthorized disclosure of EPHI.

#### 3.14 Evaluations.

- 3.14.1 Pursuant to HIPAA Section 164.308(a)(8), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component should perform an annual review to demonstrate its compliance with the HIPAA Security Rule Policy.

3.14.2 Results of the review are to be presented to the covered component's management, which will provide a documented response, including remediation steps, for any identified gaps in compliance with the policy.

### 3.15 Physical Safeguards.

3.15.1 Pursuant to HIPAA Section 164.310(a)(1), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will ensure that systems which manage EPHI are kept in areas with physical security controls that restrict access (an "isolated room"). Measures that each Health Care Component should address include the following.

3.15.1.1 Ensuring that, at a minimum, servers and network equipment which manage EPHI should be kept in an isolated room with controls that prevent unauthorized access to these systems.

3.15.1.2 These controls can include entry doors that require a key or combination locks, or that require a security token (such as magnetic strip ID card with identification information).

3.15.2 Documenting those persons who are permitted authorized access to the isolated room.

3.15.3 Requiring unauthorized persons (such as vendors, contractors, and visitors) to be escorted and monitored by an authorized person when entering and remaining in the isolated room.

3.15.4 Providing a log of access to the isolated room (which can be either a written log or an electronic record from of an ID card reader.)

3.15.5 Ensuring that records of facility maintenance or maintenance to systems managing EPHI are kept, documenting who performed the maintenance, who authorized the maintenance, and details of the maintenance activities, including dates and times.

### 3.16 Work station Use and Security.

3.16.1 Pursuant to HIPAA Section 164.310(b), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will ensure that only designated workstations possessing appropriate security controls will be used to access and manage EPHI, and that these workstations are not used in publicly-accessible areas nor used by multiple users not authorized to access EPHI.

3.16.2 This security measure extends to the use of laptops and home machines. These workstations should have the following security tools installed.

- 3.16.2.1 Anti-virus software with updated virus definitions.
  - 3.16.2.2 Spyware detection software with updated spyware definitions.
  - 3.16.2.3 An automated patch management system for operating system updates.
  - 3.16.2.4 Screens that are turned away from unauthorized users, and access authorization mechanisms that require a user ID and password to access the workstation.
- 3.16.3 The workstation should also be configured with a password-protected screensaver that is evoked after five minutes of inactivity.
- 3.17 Device and Media Controls.
- 3.17.1 Pursuant to HIPAA Section 164.310(d)(1), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will ensure that procedures are in place to govern the receipt and removal of hardware and electronic media that contains EPHI into and out of a facility, and the movement of these items within the facility.
  - 3.17.2 Media can include hard disks, tapes, floppy disks, CD ROMs, optical disks, and other means of storing computer data. Measures that each covered component should address include the following.
    - 3.17.2.1 Disposing of media with EPHI when it is discarded or reused using means that prevent its recovery, including erasing and overwriting media before disposal, physically destroying the media, and preventing systems that managed EPHI from being sold or donated before ensuring that EPHI has been fully removed.
    - 3.17.2.2 Ensuring that backups of EPHI are created before systems managing EPHI are moved.
- 3.18 Technical Safeguards.
- 3.18.1 Access Control. Pursuant to HIPAA Section 164.312(a)(1), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component will ensure that security controls are in place to protect the integrity and confidentiality of EPHI residing on computer systems, including applications, databases, workstations, servers, and network equipment. Measures that each covered component should address include the following.

- 3.18.1.1 Assigning a unique name and or number of identifying and tracking user identity on systems managing EPHI.
- 3.18.1.2 Establishing procedures for obtaining necessary EPHI during an emergency, in which normally unauthorized personnel require access to EPHI or the systems that manage EPHI.
- 3.18.1.3 Configuring systems to terminate a logon session after a predetermined time of inactivity. Mechanisms to accomplish logon session terminations include password-protected screen-savers, automatic logoff of the application or network session, and the ability to manually lock out access when leaving a workstation.
- 3.18.1.4 Encrypting EPHI that is transferred or stored on systems not controlled by the covered component. This can include e-mails, interfaces between applications, data stored on removable media (such as CD ROMs and floppy diskettes), and on files that are transferred over networks.
- 3.18.1.5 EPHI is not to be transferred using ftp (file transfer protocol), which is a clear-text protocol that can allow the confidentiality and integrity of data to be compromised.

### 3.19 Audit Controls.

- 3.19.1 Pursuant to HIPAA Section 164.312(b), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component should have audit controls implemented that allow an independent reviewer to review system activity. Audit logs that should be captured on systems managing EPHI include the following.
  - 3.19.1.1 User access and account activity.
  - 3.19.1.2 Exception reports.
  - 3.19.1.3 Dormant account reports.
  - 3.19.1.4 System resource monitoring.
  - 3.19.1.5 Data integrity controls.
  - 3.19.1.6 Failed log-in reports.
  - 3.19.1.7 Users switching user IDs during an on-line session.
  - 3.19.1.8 Attempts to guess passwords.

- 3.19.1.9 Attempts to use privileges that have not been authorized.
  - 3.19.1.10 Modifications to production application software.
  - 3.19.1.11 Modifications to system software.
  - 3.19.1.12 Changes to user privileges.
  - 3.19.1.13 Changes to logging subsystems.
  - 3.19.2 Logs should be securely retained for a minimum of one year using an archiving solution that allows for recovery within 24 hours upon request.
- 3.20 Integrity.
- 3.20.1 Pursuant to HIPAA Section 164.312(c)(1), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component should ensure that systems and applications managing EPHI have the capability to maintain data integrity at all times. Examples of integrity capabilities include the following.
    - 3.20.1.1 Error-correcting memory.
    - 3.20.1.2 Disk storage with build-in error detection and correction.
    - 3.20.1.3 Checksums.
    - 3.20.1.4 Encryption.
- 3.21 Transmission Security.
- 3.21.1 Pursuant to HIPAA Section 164.312(e)(1), the TAMHSC Privacy/Security Officer and the TAMHSC Health Care Component should have controls in place that ensures that the integrity of EPHI is maintained when in transit.
  - 3.21.2 Secure transmission mechanisms that encrypt EPHI as well as confirms that data integrity has been maintained should be used (such as cryptorouters, SSH, SSL, and the use of digital signatures).
  - 3.21.3 The use of e-mail for transmitting EPHI should be avoided; if required, e-mails with EHPI should be encrypted.

#### **4. VIOLATIONS**

The Privacy Officer has general responsibility for implementation of this policy. 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 Privacy 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.

## **OFFICE OF RESPONSIBILITY**

### **Vice President of Finance and Administration**

---

<sup>i</sup> HIPAA Code: §164.208, §164.308, § 164.309, §164.310