

UNIVERSITY OF PITTSBURGH

POLICY

**SUBJECT: SECURITY OF ELECTRONIC MEDICAL RECORDS—
COMPLIANCE WITH THE HEALTH INSURANCE PORTABILITY AND
ACCOUNTABILITY ACT OF 1996 (HIPAA)**

DATE: March 18, 2005

I. SCOPE

This policy sets forth the framework for the University's compliance with the Security Rule of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). It is applicable only to those units of the University that have been designated as "covered components" under HIPAA. This policy is limited to the final HIPAA Security Rule. Other aspects of law, including rules governing privacy and human subject research, are addressed in other University policies. See the University's IRB website for policies governing human subject research, and the University's Policies, Procedures and Handbooks web site for policies concerning privacy and computer security.

The University recognizes that adequate and appropriate security is necessary for HIPAA's privacy rules to work as intended.

II. POLICY

It is the policy of the University of Pittsburgh to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Only designated units, departments or Schools of the University that manage electronic protected health information (EPHI) are subject to the HIPAA Security Rule Regulations. This policy addresses the final HIPAA Security Rule which is effective April 21, 2005. Each covered component within the University is responsible for adopting site-specific procedures and controls to address this policy.

III. REQUIREMENTS

The HIPAA Security Rule requires the University 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 University's covered components.

EPHI includes any computer data relating to the past, present or future physical or mental health, health care treatment, or payment for health care. EPHI includes information that can identify an individual, such as name, social security number, address, date of birth, medical history or medical record number, and includes such information transmitted or maintained in electronic format, but excluding certain education and student treatment records. Not included within EPHI are student education records, including medical records (which are protected under the Buckley Amendment), medical records of employees received by the University in its capacity as an employer, and workers' compensation records. Although these records are not covered under the HIPAA Privacy or Security Rules, other University Policies cover the confidentiality and security of these materials. There are special provisions in the law governing the release of psychotherapy records.

IV. SECURITY MEASURES

The following security measures address the 18 standards of the HIPAA Security Rule that covered components need to 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 18 standards should be reasonable and appropriate, taking into account:

- The size, complexity and capabilities of the covered component;
- The covered component's technical infrastructure, hardware, and software security capabilities;
- The costs of security measures; and
- The probability and criticality of potential risk to EPHI.

1. **Administrative Safeguards**

- 1.1 To address HIPAA Section 164.308(a)(1) involving **Risk Analysis**, all covered components will perform a yearly 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. 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. Covered components can request CSSD to perform the risk analysis.

- 1.2 To address HIPAA Section 164.308(a)(1) involving **Risk Management**, all covered components will implement measures to reduce computer risks and vulnerabilities, including:
 - 1.2.1 Identifying and documenting potential risks and vulnerabilities that could impact systems managing EPHI.
 - 1.2.2 Performing annual technical security assessments of systems managing EPHI in order to identify and remedy detected security vulnerabilities. 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. Covered components can request CSSD to perform technical security assessments.

- 1.3 To address HIPAA Section 164.308(a)(1) involving **Sanction Policy**, covered entities will adhere to the sanctions statement found in this policy, found under V. SANCTIONS.

- 1.4 To address HIPAA Section 164.308(a)(1) involving **Information System Activity Review**, all covered components 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:
 - 1.4.1 Enabling logging on computer systems managing EPHI.
 - 1.4.2 Developing a process for the review of exception reports and/or logs.

- 1.4.3 Developing and documenting procedures for the retention of monitoring data. Log information should be maintained for up to six years, either locally on the server or through the use of backup tapes.
- 1.4.4 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. Covered components can request CSSD to perform compliance reviews.

- 1.5 To address HIPAA Section 164.208(a)(2) involving **Assigned Security Responsibility**, each covered 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.

- 1.6 To address HIPAA Section 164.308(a)(3) involving **Workforce Security**, all covered components will establish procedures that ensure only authorized personnel have access to systems that manage EPHI. Measures that each covered component should address include:
 - 1.6.1 Establishing a procedure that requires managerial approval before any person is granted access to systems managing EPHI.
 - 1.6.2 Performing appropriate background checks, where appropriate, before any person is granted access to systems managing EPHI.
 - 1.6.3 Limiting authorized persons' access to EPHI to the extent that access to this information achieves the requirements of the person's job responsibilities.
 - 1.6.4 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).
 - 1.6.5 Periodically reviewing the accounts on systems managing EPHI to ensure that only currently authorized persons have access to these systems.

- 1.7 To address HIPAA Section 164.308(a)(4) involving Information Access Management, all covered components will establish procedures that ensure that systems that manage EPHI have authorization controls that allow only authorized personnel access. Measures that each covered component should address include:
- 1.7.1 Using systems—such as 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.
 - 1.7.2 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.
 - 1.7.3 Ensuring that these systems have password management features that enforce the use of passwords as part of the identification/authentication mechanism.
 - 1.7.4 Ensuring that controlled privileged user accounts can be established (e.g. system administrators who typically require higher levels of access to EPHI).
- 1.8 To address HIPAA Section 164.308(a)(5) involving **Security Awareness and Training**, all covered components will undertake the following
- 1.8.1 Having the covered component’s security officer receive periodic security updates. Covered components can request these periodic security updates from CSSD.
 - 1.8.2 Having all members of a covered component take the University’s HIPAA security rule training course.
 - 1.8.3 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).
- 1.9 To address HIPAA Section 164.308(a)(5) involving **Password Management**, all covered components will ensure the following controls are in place for creating, changing and safeguarding passwords on systems managing EPHI:
- 1.9.1 Passwords must be at least 8 characters long, include a varied set of characters (such as the use of numbers and symbols).

- 1.9.2 Passwords must not be shared.
 - 1.9.3 Passwords must not be written down and stored in locations where they can be found.
 - 1.9.4 Passwords must not use any word found in any dictionary or proper name.
 - 1.9.5 Passwords must be forced to change periodically, and must be changed immediately if compromised.
- 1.10 To address HIPAA Section 164.308(a)(6) involving **Security Incident Procedures**, all covered components 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). The security official is to notify the University's Technology Help Desk, which will log the incident.
- 1.11 To address HIPAA Section 164.308(a)(7) involving **Contingency Plan**, all covered components 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:
- 1.11.1 Having procedures for creating and maintaining backups of EPHI adequate to both restore EPHI and the systems maintaining this data.
 - 1.11.2 Establishing procedures to restore any loss of data due to a disaster. At a minimum, each University covered component should maintain backup tapes at an off-site location that can be used to restore EPHI and the systems maintaining this data. 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.
 - 1.11.3 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 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.

1.11.4 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, 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. 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.

1.12 To address HIPAA Section 164.308(a)(8) involving **Evaluation**, each covered component should perform an annual review to demonstrate its compliance with the University's HIPAA Security Rule Policy. 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. Covered components can request this evaluation to be performed by CSSD.

2. **Physical Safeguards**

- 2.1 To address HIPAA Section 164.310(a)(1) involving **Facility Access Controls**, each covered 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 covered component should address include:
- 2.1.1 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. 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).
 - 2.1.2 Documenting those persons who are permitted authorized access to the isolated room.
 - 2.1.3 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.
 - 2.1.4 Providing a log of access to the isolated room, which can be either a written log or an electronic record from an ID card reader).
 - 2.1.5 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.
- 2.2 To address HIPAA Section 164.310(b) involving **Workstation Use**, each covered 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. This security measure extends to the use of laptops and home machines. These workstations should have the following security tools installed: anti-virus software with updated virus definitions, spyware detection software with updated spyware definitions, and an automated patch management system for operating system updates. Covered components can request these security tools from CSSD.

- 2.3 To address HIPAA Section 164.310(c) involving **Workstation Security**, each covered component will ensure that physical safeguards are in place to protect workstations that access and manage EPHI, including: cable locks (for desktops and for laptops), screens that are turned away from unauthorized users, and access authorization mechanisms that require a user ID and password to access the workstation. The workstation should also be configured with a password-protected screensaver that is evoked after five minutes of inactivity.
- 2.4 To address HIPAA Section 164.310(d)(1) involving **Device and Media Controls**, each covered 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. 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:
- 2.4.1 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.
- 2.4.2 Ensuring that backups of EPHI are created before systems managing EPHI are moved.

3. Technical Safeguards

- 3.1 To address HIPAA Section 164.312(a)(1) involving **Access Control**, each covered 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:
- 3.1.1 Assigning a unique name and or number of identifying and tracking user identity on systems managing EPHI.
 - 3.1.2 Establishing procedures for obtaining necessary EPHI during an emergency, in which normally unauthorized personnel require access to EPHI or the systems that manage EPHI.
 - 3.1.3 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.
 - 3.1.4 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. EPHI is not to be transferred using ftp (file transfer protocol), which is a cleartext protocol that can allow the confidentiality and integrity of data to be compromised.
- 3.2 To address HIPAA Section 164.312(b) involving **Audit Controls**, each covered 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:
- User access and account activity
 - Exception reports
 - Dormant account reports
 - System resource monitoring
 - Data integrity controls
 - Failed log-in reports

- Users switching user IDs during an on-line session
- Attempts to guess passwords
- Attempts to use privileges that have not been authorized
- Modifications to production application software
- Modifications to system software
- Changes to user privileges
- Changes to logging subsystems

Logs should be securely retained for a minimum of one year using an archiving solution that allows for recovery within 24 hours upon request.

- 3.3 To address HIPAA Section 164.312(c)(1) involving **Integrity**, each covered component should ensure that systems and applications managing EPHI have the capability to maintain data integrity at all times. Examples of integrity capabilities include error-correcting memory, disk storage with build-in error detection and correction, checksums, and encryption.
- 3.4 To address HIPAA Section 164.312(d) involving **Person or Entity Authentication**, each covered component should have controls in place that verify that a person seeking access to EPHI is the one claimed. Access to data should be controlled using the following acceptable authentication measures: username and password, token-base authentication, biometrics, and challenge and response mechanisms.
- 3.5 To address HIPAA Section 164.312(e)(1) involving **Transmission Security**, each covered component should have controls in place that ensures that the integrity of EPHI is maintained when in transit. 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). The use of e-mail for transmitting EPHI should be avoided; if required, e-mails with EHPI should be encrypted.

V. SANCTIONS

It shall be the responsibility of each covered component to implement procedures to meet the requirements of HIPAA set forth in this policy. Every employee in a covered component with access to EPHI is required to adhere to all HIPAA mandates. Violation of this policy may result in disciplinary action up to and including termination of employment. Under federal law, violation of the HIPAA privacy rule may result in civil monetary penalties of up to \$250,000 per year and criminal sanctions including fines and imprisonment.

VI. ADDITIONAL INFORMATION

For additional information about this Policy, contact the University's HIPAA Security Officer.