Carnegie Mellon

Health Insurance Portability and Accountability Act Information Security Policy

Document Information	
Identifier	
Status	Published
Approved	02/15/2008
Last Reviewed	02/15/2008
Last Updated	02/15/2008
Version	1.0

Carnegie Mellon

Revision History

Version	Published	Author	Description
1.0	02/15/2008	Doug Markiewicz	Initial publication. Policy adopted by Student Health Services and the University Group Health Plan. Reviewed by the Office of General Counsel and approved by the President's Council.

Carnegie Mellon

Purpose

In compliance with the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d), Carnegie Mellon University ("University") has adopted the following Information Security Policy ("Policy") to ensure reasonable protection of Protected Health Information ("PHI") and Electronic Protected Health Information ("EPHI"). It is the intent of this Policy to act as a supplement to, not a replacement for, the University's Data and Computer Security Policy.

Scope

This Policy is limited to University Covered Entities and applies to the security of PHI and EPHI (as defined by the Code of Federal Regulations 45 C.F.R. 160.103) as well as the security of any Information Systems that store or process EPHI. Covered Entities include Student Health Services and the University Group Health Plan. This Policy also applies to technology service providers, either internal or external to the University, as defined by each Covered Entity.

Maintenance

These Policies will be reviewed by the University Information Security Office and Covered Entities on an annual basis or as deemed necessary based on changes in technology that effect the protection of PHI and EPHI. In accordance with the Code of Federal Regulations, 45 C.F.R. 164.306(b)(2)(i), all iterations of this Policy will be retained for a minimum of 6 years.

Enforcement

Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to University Information Systems, and/or discipline up to and including termination of employment or contractor status with the University. Additional civil, criminal and equitable remedies may apply.

Exceptions

Exceptions to this Policy must be approved by the Information Security Office and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

Carnegie Mellon

Roles and Responsibilities

01 The **HIPAA Security Officer** is a University employee who is responsible for coordinating compliance with the HIPAA Security Rule as defined by the Code of Federal Regulations, 45 C.F.R. 160, 162 and 164. Each Covered Entity must designate a HIPAA Security Officer. The HIPAA Security Officer may delegate his or her responsibilities to other University employees.

02 The HIPAA Security Officer is responsible for:

a. Understanding how PHI and EPHI are used within the Covered Entity and by any Business Associate of the Covered Entity.

b. Understanding relevant security and privacy requirements dictated by HIPAA.

c. Implementing appropriate procedures to support this Policy.

d. Implementing a recurring awareness program to ensure Covered Entity personnel understand their obligations under this Policy.

e. Ensuring the Covered Entity adheres to this Policy and its supporting procedures.

f. Ensuring that any exceptions to this Policy or its supporting procedures are approved by the Information Security Office and formally documented.

g. Coordinating with the Information Security Office to identity and evaluate threats to the confidentiality and integrity of EPHI.

h. Coordinating with the Information Security Office to respond to actual or suspected breaches in the confidentiality or integrity of EPHI.

03 For the purpose of this Policy, a **User** is any employee or contractor of the Covered Entity who is authorized to access University Information Systems provided by or for the Covered Entity.

04 A User is responsible for:

a. Abiding by this Policy and its supporting procedures.

b. Reporting actual or suspected vulnerabilities in the confidentiality or integrity of EPHI to the HIPAA Security Officer.

c. Reporting actual or suspected breaches in the confidentiality or integrity of EPHI to the HIPAA Security Officer.

d. Reporting suspicious requests for PHI or EPHI to the HIPAA Security Officer

Carnegie Mellon

Principle Information Security Policies

05 Each Covered Entity must:

a. Have a designated HIPAA Security Officer.

b. Conduct a security risk assessment annually, at a minimum, to measure the potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI.

c. Implement reasonable and appropriate administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of EPHI.

06 Prior to conducting business with a third party that involves the storage or processing of EPHI, a Covered Entity must coordinate with the third-party to sign a Business Associate Contract that includes provisions for the third-party to reasonably safeguard EPHI.

Issue Specific Information Security Policies

Access Control

07 Access to EPHI must be:

a. Authenticated in such a manner as to positively and uniquely identify the user.

b. Authorized by a designated Data Owner.

c. Consistent with the rule of least privilege, meaning a user is granted the minimum level of access necessary to perform authorized job responsibilities.

d. Logged.

e. Reviewed annually, at a minimum, to ensure such access is still appropriate.

f. Revoked when such access is no longer necessary to perform authorized job responsibilities.

08 All accounts that can be used to access EPHI must be protected with a strong password as defined by the Information Security Office.

09 All Information Systems that store, process or otherwise access EPHI, including User workstations, must be configured such that:

a. A screen saver is activated after a period of inactivity.

b. The Information System locks, requiring re-authentication, after a period of inactivity.

c. Open sessions are automatically disconnected after a period of inactivity.

Business Continuity Management

10 All Covered Entities must:

a. Maintain retrievable backup copies of all EPHI that must also meet the requirements of this Policy.

b. Periodically test the effectiveness of backup copies of EPHI.

c. Develop, implement and maintain a Business Continuity and Disaster Recovery Plan that includes provisions for the continuity of Information Systems that store or process EPHI.

d. Coordinate and execute periodic testing of Business Continuity and Disaster Recovery Plans.

Employee Owned Assets

11 Employee owned Information Systems must not be used to store or process EPHI.

Encryption

12 All EPHI must be encrypted during transmission over public networks such as the Internet.

13 All Covered Entities must take reasonable measures to encrypt stored EPHI.

Information Security Awareness

14 All employees and contractors of a Covered Entity must undergo periodic security awareness training specific to the requirements of HIPAA.

Information Security Breaches

15 All Covered Entities must regularly monitor Information Systems, that store or process EPHI, for security events.

16 All security incidents must be addressed in a manner that is consistent with guidance and procedures published by the Information Security Office.

Physical Security

17 All Carnegie Mellon University personnel must be positively and uniquely identified prior to gaining physical access to Information Systems that store or process EPHI.

18 Physical access to Information Systems that store or process EPHI must be controlled in a manner that prevents unauthorized physical access.

19 All repairs and alterations to physical security controls that aid in the protection of PHI and/or EPHI must be documented and available for review by the HIPAA Security Officer.

20 All recycling and disposal of electronic storage media that is used to store EPHI or that was previously used to store EPHI must be consistent with guidance and procedures published by the Information Security Office.

21 All physical relocation of Information Systems that store or process EPHI must be documented and available for review by the HIPAA Security Officer.

22 All Covered Entity personnel must maintain a workspace that is clear of PHI or EPHI whenever that workspace is unattended.

Carnegie Mellon

Glossary

Term	Definition
Covered Entity / Entities	For the purpose of this Policy, Covered Entities include the Carnegie Mellon University Group Health Plan, Student Health Services and any third-party who stores or processes PHI and/or EPHI on behalf of these entities.
Electronic Protected Health Information ("EPHI")	Individually identifiable health information transmitted by electronic media or maintained in electronic media.[1]
Health Information	Any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and that is related to the past, present or future physical or mental health condition of an individual, the provision of health care of an individual, or the past, present or future payment for the provision of healthcare to an individual.[1]
Individually Identifiable Health Information	Any heath information, as defined above, that identifies an individual or where there is reasonable basis to believe that the information can be used to identify an individual.[1]
Information System	Any electronic system that stores or processes information. An electronic system includes but is not limited to hardware components, software components and raw network data. Examples include: • Personal computers whether standalone or connected to a network • Servers whether standalone or connected to a network • Network devices such as routers and switches • Handheld computing devices such as PDAs and smart phones • Telephony equipment such as a VoIP system or facsimile machine • Operating systems such as Microsoft Windows, UNIX and/or Mac OSX • Commercial, open-source or in-house developed applications • Commercial, open-source or in-house developed databases • Storage devices such as CD, DVD, USB drive or magnetic tape • Internet facing and private websites
Protected Health Information	Individually identifiable health information transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium.[1]

[1] As defined by the Code of Federal Regulations, 45 C.F.R. 106.103. Definitions may be modified from their original form for the sake of clarity.