Carnegie Mellon

# HIPAA Frequently Asked Questions

| Document Information | |
|---|---|
| Identifier | |
| Status | Published |
| Published | 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 |

Carnegie Mellon

# HIPAA Frequently Asked Questions

**1. What is HIPAA?**

HIPAA, or the Health Insurance Portability and Accountability Act, was enacted by the federal government in 1996. The original intent of HIPAA was to help ensure the continuation of health insurance coverage when an individual left his or her job. HIPAA was then expanded to include a number of provisions to simplify and lower the costs of processing health information. A number of these provisions deal with the standardization of electronic transactions. Implementation of security standards is a subset of these provisions.

**2. What is the HIPAA Security Rule?**

HIPAA calls for the adoption of security standards to help protect health information; however, it does not define specific security requirements. HIPAA simply calls for administrative, technical and physical safeguards to ensure the confidentiality and integrity of health information. The Department of Health and Human Services published the HIPAA Security Rule to better define these requirements.

**3. Is there more to HIPAA than just security?**

Yes, security is just one piece of HIPAA. There are numerous other requirements related to privacy, health insurance portability and standardization of health information processing. Information on HIPAA requirements unrelated to security can be found on the Department of Health and Human Services website.

**4. What type of information is protected by HIPAA?**

HIPAA defines protected information in several forms. Health information is defined as 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. Individually Identifiable Health Information is defined as any Health Information that identifies an individual or where there is reasonable basis to believe that the information can be used to identify an individual. Protected Health Information (“PHI”) is defined as Individually Identifiable Health Information transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium. Electronic Protected Health Information (“EPHI”) is defined as Individually Identifiable Health Information transmitted by electronic media or maintained in electronic media. Individually Identifiable Health Information and Protected Health Information are essentially the same. They include information in written, verbal and electronic form. EPHI is a subset of PHI and PHI is a subset of Health information. The HIPAA Security Rule uses the terms PHI and EPHI when defining its requirement.

**5. Who must comply with the HIPAA Security Rule?**

Any Health Plan, Health Care Clearinghouse or a Health Care Provider who transmits health information in electronic form must comply with the HIPAA Security Rule. A Health Plan is defined as an individual or group plan that provides or pays the cost of medical care. A Health Care Clearinghouse is defined as a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and ``value-added'' networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving

entity. A Health Care Plan is defined as a provider of services, a provider of medical or health services and any other person or organization who furnishes, bills or is paid for health care in the normal course of business.

**6. What are the repercussions of non-compliance with HIPAA?**

Failure to comply with HIPAA requirements could result in significant financial loss through civil penalties and damage to brand and reputation. HIPAA states that civil penalties up to $100 per day per person can be issued for non-compliance. While this does not seem like a large sum, it can quickly add up. If student health information was exposed for 1000 students over the course of 30 days, the fines could reach $3,000,000.

**7. What is the University's HIPAA Information Security Policy?**

The HIPAA Security Rule requires implementation of various policies and procedures to help safeguard protected health information. The University's HIPAA Information Security Policy was developed by the Information Security Office to meet policy requirements. All Covered Entities must comply with this Policy.

**8. How do I know if the University's HIPAA Information Security Policy applies to me?**

The Office of General Counsel has determined that the University Group Health Plan and Student Health Services are both Covered Entities under the terms of the HIPAA Security Rule. The University's HIPAA Information Security Policy applies to Covered Entities. Certain aspects of the Policy may indirectly apply to other departments that provide services to a Covered Entity. Questions regarding such requirements should be directed at the Covered Entity's HIPAA Security Officer.

**9. What are the repercussions of non-compliance with the University's HIPAA Information Security Policy?**

Failure of an individual to act in accordance with the University's HIPAA Information Security Policy can result in a loss of use privileges as well as termination of employment.

**10. What steps can be taken to validate compliance with the University's HIPAA Information Security Policy?**

The Information Security Office can assist with conducting a security risk assessment to ensure proper controls are in place to comply with the HIPAA Security Rule and the University's HIPAA Information Security Policy. If you would like the Information Security Office to assist with performing a security risk assessment, please send an email to iso@andrew.cmu.edu.

**11. What steps can be taken if a requirement of the University's HIPAA Information Security Policy cannot be met?**

If you feel there is a HIPAA Security Rule requirement or a requirement within the University's HIPAA Information Security Policy that you cannot comply with, you should contact the Information Security Office via email at iso@andrew.cmu.edu to discuss the circumstances. Exceptions to HIPAA security requirements must be thoroughly documented and reasonable compensatory controls must be put in place to mitigate the risk associated with non-compliance.

**12. Can protected health information be transmitted through email?**

Protected health information should not be transmitted through email services. Email, in its native state, is an insecure form of communication and HIPAA specifically requires controls to ensure integrity and confidentiality of protected health information. However, there are ways to secure email communication. If there is a business need to send protected health information through email, the Information Security Office should be engaged to ensure proper controls are put in place prior to sending.

Carnegie Mellon

**13. Can protected health information be transmitted through fax services?**

Protected health information should not be transmitted using traditional fax services. HIPAA requires that access to protected health information be authenticated and there is no effective way to determine who has access to the receiving end of a fax transmission. Additionally, traditional fax services do not sufficiently protect the integrity and confidentiality of the data being sent over the phone line.

**14. Can protected health information be sent to a third-party service provider?**

Before protected health information can be provided to a third-party service provider, HIPAA requires that a Business Associate Contract be signed stating that the third-party will implement reasonable safeguards to protect the confidentiality and integrity of protected health information. The Office of General Counsel should be engaged to assist in the development of such a contract. The Information Security Office should also be engaged to ensure there are no additional security requirements beyond that of HIPAA. Send email to iso@andrew.cmu.edu if you would like someone within the Information Security Office to review a third-party service contract prior to signing.

**15. Does the HIPAA Security Rule apply to research involving health information?**

While research is largely protected from HIPAA security requirements, the University Institutional Review Board ("IRB") provides specific information related to research and HIPAA compliance. Additional information can be found on the IRB website by clicking here.

**16. Who is required to undergo HIPAA security awareness training?**

HIPAA requires that all Covered Entities undergo security awareness training. This includes employees responsible for day to day operation and handling of health information as well as their managers. This also includes researchers affiliated with a Covered Entity. Training should specifically address the security requirements of HIPAA.

**17. Who should be contacted in the event of a security breach or suspected security breach?**

The Information Security Office must be informed when there is a breach or suspected security breach of information security. This is particularly important when protected health information may be involved. Procedures for how to appropriately respond to a suspected computer compromise can be found at the following location:

Procedure for Responding to a Compromised Computer
http://www.cmu.edu/iso/governance/procedures/first-respond.html

**18. Who should be contacted with questions related to HIPAA security?**

If you have any questions or concerns related to HIPAA security, please send email to the Information Security Office at iso@andrew.cmu.edu.