

# NEW YORK UNIVERSITY

## HIPAA Information Security Policies, Specifications, and Definitions

### Policy 3. Assigned Security Responsibility

Responsible Officer: Associate Provost and Chief Information Technology Officer

Effective Date: January 1, 2005

Compliance Deadline: April 21, 2005

Date of Latest Revision: December 23, 2004

### POLICY STATEMENT

The Assigned Security Responsibility policy is a reflection of New York University's commitment to institute reasonable and appropriate safeguards to ensure the *confidentiality, integrity, and availability* of *EPHI* by assigning a single employee, New York University's *EPHI* Security Officer, the responsibility for overseeing the development and implementation of the policies and procedures required by *HIPAA Security Regulations*. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

### REASON FOR POLICY

Under the *HIPAA Security Regulations*, New York University is required to designate a security official who is responsible for the development and implementation of its security policies and procedures. This policy reflects the University's commitment to comply with such regulations. In addition, the appointment of a University *EPHI* Security Officer will provide organizational focus to, and highlight the importance of, the University's efforts to safeguard *EPHI*.

### OPERATIONAL REQUIREMENTS

- A. The University's *EPHI* Security Officer shall take reasonable and appropriate measures to:
1. Confirm that *EPHI Systems* are reasonably and appropriately protected and have reasonable and appropriate safeguards in order to safeguard the *confidentiality, integrity, or availability* of any of *EPHI*.
  2. Confirm that New York University is compliant with applicable federal, state, and local laws pertaining to security of *EPHI*.
  3. Confirm that recently acquired *EPHI Systems* have options that support required and/or addressable implementation specifications of the *HIPAA Security Regulations* and New York University's internal security requirements.
  4. Guide the development, documentation, and dissemination of appropriate security policies and procedures for the users and administrators of *EPHI Systems*.
  5. Approve and oversee the administration, implementation, and selection of New York University security controls for *EPHI Systems*.
  6. Review periodic reports from the *EPHI* security officers of the *covered components* that confirm that New York University *workforce members* receive security training on a periodic basis.
  7. Consult New York University's Privacy Officer to confirm that security policies, procedures, and controls support compliance with the HIPAA Privacy Regulations.
  8. Confirm that an inventory of *EPHI Systems* is maintained and updated on a periodic basis.

9. Review periodic reports from the *EPHI* security officers of the *covered components* that confirm that a risk analysis of *EPHI Systems* is completed on a periodic basis as set forth in New York University's ***Risk Analysis operational specification*** (see 2.A)
10. Oversee the implementation of an effective risk management program as set forth in New York University's ***Risk Management operational specification*** (see 2.B).
11. Confirm that the threats and risks to the *confidentiality, integrity, and availability* of *EPHI* are monitored and evaluated.
12. Confirm that records of *EPHI Systems* are developed, monitored, and audited to identify security incidents and malicious activity as set forth in New York University's ***Information System Activity Review operational specification*** (see 2.D).
13. Oversee the development and implementation of an effective security incident response policy and related procedures as set forth in New York University's ***Response and Reporting operational specification*** (see 7.A).
14. Confirm that adequate physical security controls exist to protect *EPHI*.
15. Create reports, as necessary, to inform the University administration of continuing compliance.

B. In addition to the University's *EPHI* Security Officer, each *covered component* will designate an *EPHI* security officer for the *covered component* with responsibility for ensuring the *confidentiality, integrity, and availability* of *EPHI* within the *covered component* in accordance with New York University's HIPAA Information Security Policies. The *EPHI* security officers of the *covered components* shall provide reports to the University's *EPHI* Security Officer in such a manner and at such times as the University's *EPHI* Security Officer may direct from time to time. Such reports may include incident reports, quarterly reports, and others.

## C. HIPAA REGULATORY INFORMATION

**CATEGORY:** Administrative Safeguards

**TYPE:** Standard

**HIPAA HEADING:** Assigned Security Responsibility

**REFERENCE:** 45 CFR 164.308(a)(2)

**SECURITY REGULATION STANDARDS LANGUAGE:** *"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."*

## DEFINITIONS

*Availability*

*Confidentiality*

*Covered component*

*Electronic Protected Health Information (or EPHI)*

*EPHI systems*

*HIPAA Security Regulations*

*Integrity*

*Workforce member*

## RELATED HIPAA DOCUMENTS

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation

HIPAA Policy 2 – Security Management Process

HIPAA Privacy Regulations covered component's Minimum Necessary Policy

Public Law 104-191, August 21, 1996, Health Insurance Portability and Accountability Act of 1996,

<<http://aspe.os.dhhs.gov/admsimp/pl104191.htm>>.

Part II, Department of Health and Human Services, 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule, February 20, 2003, <<http://aspe.hhs.gov/admsimp/FINAL/FR03-8334.pdf>>.