

# NEW YORK UNIVERSITY

## HIPAA Information Security Policies, Specifications, and Definitions

### Policy 7. Security Incident Procedures

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

New York University strives to protect the *confidentiality, integrity, and availability* of *EPHI* by instituting and documenting reasonable and appropriate safeguards to identify, report, track, and respond to *security incidents* promptly. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

#### REASON FOR POLICY

Awareness of, response to, and creation of reports about *security incidents* in the context of its operations are integral parts of New York University's efforts to comply with the *HIPAA Security Regulations*.

#### OPERATIONAL REQUIREMENTS

A. New York University and each *covered component* shall implement a documented process for promptly identifying, reporting, tracking, and responding to *security incidents*, and will conduct training awareness on those *security incident* procedures.

#### B. HIPAA REGULATORY INFORMATION

**CATEGORY:** Administrative Safeguards

**TYPE:** Standard

**HIPAA HEADING:** Security Incident Procedures

**REFERENCE:** 45 CFR 164.308(a)(6)(i)

**SECURITY REGULATION STANDARDS LANGUAGE:** "Implement policies and procedures to address security incidents."

#### OPERATIONAL SPECIFICATIONS

##### 7.A Response and Reporting

1. New York University and each *covered component* shall include, as appropriate, in its documented process for promptly identifying *security incidents*, the following:
  - a. Risk analysis of *EPHI Systems*, as set forth in New York University's *Risk Analysis operational specification* (see 2.A).
  - b. On the basis of the risk analysis, identify what events constitute a *security incident* in the context of New York University's and the *covered component's* operations.
  - c. Process for identifying a *security incident*.

2. New York University and each *covered component* shall organize a *Security Incident Response Team (SIRT)* that is primarily responsible for *security incident* reporting and response will perform an investigation when evidence shows that a *security incident* has occurred and will respond promptly to the *security incident*. New York University and each *covered component* shall document its process for promptly responding to *security incidents*.
3. New York University and each *covered component* shall include, as appropriate, in its documented process for promptly reporting *security incidents*, a procedure for New York University *workforce members* to report a *security incident* to the appropriate identified management personnel. A New York University *workforce member* will not prohibit or otherwise attempt to hinder or prevent another New York University *workforce member* from reporting a *security incident* to the SIRT and shall cooperate fully with *security incident* investigations.
4. New York University and each *covered component* shall include training and awareness for *workforce members*, as appropriate, in its documented process for promptly identifying, reporting, tracking, and responding to *security incidents* in accordance with New York University's and the *covered component's* security policies and procedures.

## 5. HIPAA REGULATORY INFORMATION

**CATEGORY:** Administrative Safeguards

**TYPE:** REQUIRED Implementation Specification for *Security Incident Procedures Standard*

**HIPAA HEADING:** Response and Reporting

**REFERENCE:** 45 CFR 164.308(a)(6)(ii)

**SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:**

*"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."*

## DEFINITIONS

*Availability*

*Confidentiality*

*Covered component*

*Data user*

*Electronic Protected Health Information (or EPHI)*

*EPHI systems*

*HIPAA Security Regulations*

*Information system*

*Integrity*

*Security incident*

*Workforce member*

## RELATED HIPAA DOCUMENTS

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

HIPAA Operational Specification 2.A – Risk Analysis

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>>.