

NEW YORK UNIVERSITY

HIPAA Information Security Policies, Specifications, and Definitions

Policy 16. Audit Controls

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 taking reasonable and appropriate steps to implement appropriate hardware, software, or procedural mechanisms on its or its *covered components'* information systems that contain or use *EPHI* to enable review of information system activity on an ongoing basis. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

REASON FOR POLICY

The implementation of audit control mechanisms to record and examine system activity in accordance with the *HIPAA Security Regulations* establishes a minimum level of security in order to safeguard *electronic protected health information*.

OPERATIONAL REQUIREMENTS

- A. Where feasible, New York University's and each *covered component's* information systems shall have the appropriate hardware, software, or procedural auditing mechanisms to generate reports of *auditable events*. New York University and each *covered component* shall review the audit mechanism on at least a periodic basis.
- B. New York University and each *covered component* shall maintain and implement a process for audit log maintenance, including:
 - 1. Identification of *workforce members* who review logs (e.g., network logs and application-level logs)
 - 2. Frequency of log review
 - 3. Procedure for determining how *auditable events* are identified during audit log review and reported to the appropriate New York University manager or executive
 - 4. Retention period of logs

C. HIPAA REGULATORY INFORMATION

CATEGORY: Technical Safeguards

TYPE: Standard

HIPAA HEADING: Audit Controls

REFERENCE: 45 CFR 164.312(b)

SECURITY REGULATION STANDARDS LANGUAGE: "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

DEFINITIONS

Auditable event

Availability

Confidentiality

Covered component

Electronic Protected Health Information (or EPHI)

HIPAA Security Regulations

Integrity

Workforce member

RELATED HIPAA DOCUMENTS

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

HIPAA Operational Specification 2.A – Risk Analysis

HIPAA Operational Specification 2.D – Information System Activity Review

HIPAA Policy 7 - Security Incident Procedures

HIPAA Operational Specification 7.A - Response and Reporting

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>>.