NEW YORK UNIVERSITY
HIPAA Information Security Policies, Specifications, and Definitions

Title:	Policy 16. Audit Controls
Effective Date:	January 1, 2005
Reviewed:	August 13, 2021
Revised:	April 10, 2021
Issuing Authority:	Executive Vice President; Vice President for Information Technology and Global University Chief Information Officer
Responsible Officer:	Executive Vice President; Vice President for Information Technology and Global University Chief Information Officer

Policy

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 component*s' 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.

Purpose of this 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*.

Scope of this Policy

Affected by these policies are all *covered component*s that may be designated by the University from time to time, including the NYU School of Medicine, NYU College of Dentistry, and the Student Health Center, and areas designated part of the health care component of the University from time to time but only to the extent that each component performs activities that would make such component a *business associate* of a component of the University that performs covered functions if the two components were separate legal entities (i.e., *support components*), including the Office of the Bursar, Controller's Division, including Accounts Payable, NYU Information Technology (NYU IT), Office of Insurance and Risk Management, Internal Audit, Office of Compliance and Risk Management, Office of General Counsel, Office of Sponsored Programs, University Relations and Public Affairs, Public Safety, Treasury Applications, and University Development and Alumni Relations. The NYU School of Medicine follows HIPAA-related policies and procedures created specifically for its environment; School of Medicine compliance with HIPAA is coordinated through Langone Medical Center. These policies affect all NYU *workforce member*s in *covered component*s.

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 event*s. 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 member*s who review logs (e.g., network logs and application-level logs)
    2. Frequency of log review
    3. Procedure for determining how *auditable event*s 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."*

Policy Definitions

Auditable event
Availability
Business associate
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://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

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/admnsimp/FINAL/FR03-8334.pdf.

American Recovery and Reinvestment Act of 2009. Title XIII, Health Information Technology for Economic and Clinical Health (HITECH), Public Law 111–5—February 17, 2009, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

Department of Health and Human Services. Office of the Secretary. 45 CFR Parts 160 and 164. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, January 25, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf