

NEW YORK UNIVERSITY

HIPAA Information Security Policies, Specifications, and Definitions

Policy 17. Integrity

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 protect the *integrity* of *EPHI* that New York University creates, receives, maintains, or transmits from *unauthorized* modification or destruction. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

REASON FOR POLICY

In order to safeguard *EPHI*, it is important to corroborate that *EPHI* has not been altered or destroyed in an *unauthorized* manner as required pursuant to the *HIPAA Security Regulations*. This policy reflects New York University's commitment to comply with such Regulations.

OPERATIONAL REQUIREMENTS

- A. New York University and each *covered component* shall implement a process for protecting the *integrity* of its *EPHI*, to include:
1. When feasible, procedure for implementing appropriate *integrity* controls on *EPHI*, as set forth in *Mechanism to Authenticate EPHI operational specification* (see 17.A).
 2. Procedure for verifying that controls used to protect the *integrity* of *EPHI* are functioning appropriately and not impacting New York University's functionality and workflow.
 3. Procedure outlining how New York University detects, reports, and responds to attempted or successful *unauthorized* modification or destruction of *EPHI*.
- B. New York University's methods used to protect the *integrity* of *EPHI* shall be approved by the University's *EPHI* Security Officer and each *covered component's* methods used to protect the *integrity* of *EPHI* shall be approved by the *covered component's* *EPHI* security officer.

C. HIPAA REGULATORY INFORMATION

CATEGORY: Technical Safeguards

TYPE: Standard

HIPAA HEADING: Integrity

REFERENCE: 45 CFR 164.312(c)(1)

SECURITY REGULATION STANDARDS LANGUAGE: "Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

OPERATIONAL SPECIFICATIONS

17.A Mechanism to Authenticate Electronic Protected Health Information

1. Each *covered component* of New York University will take reasonable and appropriate steps to implement electronic mechanisms to prove that *EPHI* has not been altered or destroyed in an *unauthorized* manner, including:
 - a. which *EPHI* will be authenticated
 - b. which electronic mechanisms would be reasonable and appropriate
2. New York University's *EPHI* Security Officer and/or each *covered component's* *EPHI* security officer, as appropriate, will approve the electronic mechanisms that have been implemented to protect *EPHI* from *unauthorized* alteration or destruction and to authenticate the *integrity* of *EPHI*, and will take reasonable and appropriate steps to ensure that the electronic mechanisms are reviewed and that *integrity* incident reports are generated from the electronic mechanisms.
3. New York University will take reasonable and appropriate steps to train *workforce members* regarding the electronic mechanism(s) the *covered component* has implemented to confirm the *integrity* of *EPHI*.

4. HIPAA REGULATORY INFORMATION

CATEGORY: Technical Safeguards

TYPE: ADDRESSABLE Implementation Specification for Integrity Standard

HIPAA HEADING: Mechanism to Authenticate Electronic Protected Health Information

REFERENCE: 45 CFR 164.312(c)(2)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

“Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.”

DEFINITIONS

Authorize

Availability

Checksum

Confidentiality

Covered component

Digital signature

Electronic Protected Health Information (or EPHI)

Encryption

Hash (or hash value)

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 Policy 4 - Workforce Security

HIPAA Policy 5 - Information Access Management

HIPAA Policy 6 - Security Awareness and Training

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>>.