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

Title:	Policy 17. Integrity Controls
Effective Date:	January 1, 2005
Reviewed:	August 13, 2021
Revised:	April 10, 2020
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 protect the *integrity* of *EPHI* that New York University creates, receives, maintains, or transmits from un*authorize*d modification or destruction. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

Purpose of this Policy

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

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. 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 un*authorize*d 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 un*authorized* 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 un*authorize*d 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 member*s 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."*

Policy Definitions

Authorize
Availability
Business associate
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://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