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

Title:	Policy 19. Transmission Security
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* while it is transmitted over *electronic communications network*s. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

Purpose of this Policy

In order to ensure the *confidentiality*, *integrity*, and *availability* of *electronic protected health care information* (*EPHI*), New York University will implement technical security measures to guard against un*authorize*d *access* as required by 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 its *covered components* will take reasonable and appropriate steps to implement security measures to protect the *integrity* of *EPHI* while it is being transmitted over *electronic communications network*s, as set forth in its ***Integrity Controls operational specification*** (see 19.A) and its ***Encryption operational specification*** (see 19.B).

B. **HIPAA REGULATORY INFORMATION**

CATEGORY: Technical Safeguards
TYPE: Standard
HIPAA HEADING: Transmission Security
REFERENCE: 45 CFR 164.312(e)(1)

SECURITY REGULATION STANDARDS LANGUAGE: "*Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network*."

Operational Specifications

19.A Integrity Controls

1. When the *covered component*'s risk analysis determines it to be necessary, the *covered component* will use *integrity* controls to ensure that the value and state of its *EPHI* is maintained during transmission and that *EPHI* is protected against un*authorize*d alteration or destruction during transmission over *electronic communications network*s.

2. The *EPHI* security officer of each *covered component* will approve the implemented *integrity* controls for the respective *covered component* and will take reasonable and appropriate steps to confirm effective implementation of the *integrity* controls, to review and update them as necessary, and to report as necessary to the New York University's *EPHI* Security Officer.

3. *Protected health information* stored, whether intentionally or not, in a photocopier, facsimile, and other devices is subject to the HIPAA Privacy and Security Rules.

4. The *EPHI* security officer of each *covered component* will determine whether it is appropriate for that *covered component* to accept the use of the external portable medium on their systems when an individual requests to receive *PHI* in a particular electronic form and format. If the *EPHI* security officer of the *covered component* determines there is an unacceptable level of risk, the individual may opt to receive an alternative form of the *EPHI.*

5. Each *covered component* will provide affected New York University *workforce member*s with training and awareness regarding *integrity* controls implemented to protect *EPHI* from un*authorize*d alteration or destruction during transmission over *electronic communications network*s.

6. **HIPAA REGULATORY INFORMATION**

   CATEGORY: Technical Safeguards
   TYPE: ADDRESSABLE Implementation Specification for Transmission Security Standard
   HIPAA HEADING: Integrity Controls
   REFERENCE: 45 CFR 164.312(e)(2)(i)
   SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: "*Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."*

19.B Encryption

1. When a *covered component* of New York University deems it necessary, the *covered component* will use *encryption* to protect the *confidentiality*, *integrity*, and *availability* of *EPHI* during transmission over *electronic communications network*s.

2. New York University's *EPHI* Security Officer and/or the *covered component*'s *EPHI* security officer will approve the *encryption* methods used to protect the *confidentiality*, *integrity*, and *availability* of *EPHI* during transmission over an *electronic communications network*.

3. The *covered component*'s *EPHI* security officer will implement a process for managing and protecting the *cryptographic key*s used to encrypt its *EPHI* against modification or destruction, will protect its private keys against un*authorize*d disclosure, and will implement a process for managing the *cryptographic key*s used to encrypt *EPHI* transmitted over *electronic communications network*s.

4. Each *covered component* will provide appropriate New York University *workforce member*s with training and awareness regarding *encryption* methods implemented to protect *EPHI* from un*authorize*d alteration or destruction during transmission over *electronic communications network*s.

5. **HIPAA REGULATORY INFORMATION**

CATEGORY: Technical Safeguards
TYPE: ADDRESSABLE Implementation Specification for Transmission Security Standard
HIPAA HEADING: Encryption
REFERENCE: 45 CFR 164.312(e)(2)(ii)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: "*Implement a mechanism to encrypt protected health information whenever deemed appropriate.*"

Policy Definitions

Access
Authorize
Availability
Business associate
Checksum
Confidentiality
Covered component
Cryptographic key
Electronic communications network
Electronic Protected Health Information (or *EPHI*)
Encryption
Hash (or *hash value*)
Integrity
Message authentication code
Protected Health Information (PHI)
Workforce member

Related HIPAA Documents

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation
HIPAA Operational Specification 2.A – Risk Analysis
HIPAA Policy 17 – Integrity
HIPAA Operational Specification 17.A – Mechanism to Authenticate Electronic Protected Health Information
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