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

Title:	Policy 14. Device and Media 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 and each *covered component* strives to protect the *confidentiality*, *integrity*, and *availability* of *EPHI* by taking reasonable and appropriate steps to control its hardware and *electronic media* through the entire lifecycle, from initial receipt to final removal. Such control includes reasonably and appropriately protecting, accounting for, properly storing, backing up, and disposing of its hardware and *electronic media* in accordance with specific control procedures and tracking all incoming hardware and *electronic media* and transfers of hardware and *electronic media* as they are moved into, out of, and within its facilities. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

Purpose of this Policy

It is important to have media control in the form of documented policies and procedures that govern the receipt and removal of hardware and/or software, 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. Each *covered component* shall take reasonable steps to identify periodically hardware and *electronic media* that contain or provide *access* to *EPHI* and to document and store the inventory appropriately in a secure manner. These steps include:
    1. disposal
    2. media re-use
    3. accountability
    4. data backup and storage

B. HIPAA REGULATORY INFORMATION

CATEGORY: Physical Safeguards

TYPE: Standard
HIPAA HEADING: Device and Media Controls
REFERENCE: 45 CFR 164.310(d)(1)
SECURITY REGULATION STANDARDS LANGUAGE:
"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility."

Operational Specifications

14.A Disposal

1. Each *covered component* of New York University will take reasonable and appropriate steps to dispose of *EPHI* when it is no longer needed, in a manner so as to permanently, completely, and irreversibly delete *EPHI* and to prevent future *access* by un*authorize*d individuals. Each *covered component* also shall follow the New York University Asset Management requirements regarding computer disposal/surplus.

2. Each *covered component* shall take reasonable and appropriate steps to remove *EPHI* from hardware and media, prior to final disposal or *re-use*. The *covered component*'s *EPHI* security officer shall be responsible for approval of the erasing tool to be used and shall take reasonable steps to ensure that it is used properly as set forth in New York University's ***Media Re-use operational specification*** (see 14.B).

3. HIPAA REGULATORY INFORMATION

CATEGORY: Physical Safeguards
TYPE: REQUIRED Implementation Specification for Device and Media Controls Standard
HIPAA HEADING: Disposal
REFERENCE: 45 CFR 64.310(d)(2)(i)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: *"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."*

14.B Media Re-use

1. Each *covered component* of New York University will take reasonable and appropriate steps to remove or overwrite *EPHI* on its *electronic media* before the media are *re-use*d for any purpose in order to prevent un*authorize*d *access* to the *EPHI.*

2. HIPAA REGULATORY INFORMATION

CATEGORY: Physical Safeguards
TYPE: REQUIRED Implementation Specification for Device and Media Controls Standard
HIPAA HEADING: Media Re-use
REFERENCE: 45 CFR 164.310(d)(2)(ii)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use."

14.C Accountability

1. Each *covered component* of New York University will take reasonable and appropriate steps to establish and maintain records of movements of hardware and *electronic media* on which *EPHI* is or was stored.

2. HIPAA REGULATORY INFORMATION

CATEGORY: Physical Safeguards
TYPE: ADDRESSABLE Implementation Specification for Device and Media Controls Standard

HIPAA HEADING: Accountability
REFERENCE: 45 CFR 164.310(d)(2)(iii)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Maintain a record of the movements of hardware and electronic media and any person responsible therefore."

14.D Data Backup and Storage

1. Each *covered component* of New York University will take reasonable and appropriate steps to ensure that exact, retrievable *backup* copies of *EPHI* are made before movement of equipment when needed. Each *covered component* will define and document an appropriate retention period for the *backup* copies of *EPHI*.

2. HIPAA REGULATORY INFORMATION

CATEGORY: Physical Safeguards
TYPE: ADDRESSABLE Implementation Specification for Device and Media Controls Standard
HIPAA HEADING: Data Backup and Storage
REFERENCE: 45 CFR 164.310(d)(2)(iv)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."

Policy Definitions

Access
Availability
Authorize
Backup
Business associate
Confidentiality
Covered component
Electronic media
*Electronic Protected Health Information (*or *EPHI)*
HIPAA Security Regulations
Integrity
Re-use
Workforce member

Related HIPAA Documents

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation
HIPAA Operational Specification 8.A - Data Backup Plan
HIPAA Privacy Regulations covered component's Minimum Necessary Policy

Asset Management Policy – Computer Disposal/Surplus, http://www.nyu.edu/asset/

Standard for Destruction and Disposal of Electronic Equipment and Data, http://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/standard-for-destruction-and-disposal-of-electronic-equipment-an.html

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