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

Title:	Policy 13. Workstation 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* by taking reasonable and appropriate steps to implement physical safeguards for all *workstation*s that can access *EPHI*, to restrict access to authorized *workforce member*s. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

Purpose of this Policy

Security of *workstation*s with *EPHI* is an essential ingredient of general security both internal and external to New York University, including the implementation of physical safeguards for *workstation*s that access *EPHI*, 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* will strive to place *workstation*s *access*ing *EPHI* in physically secure locations that minimize the *risk* of physical *access* by unauthorized persons.

B. Each *covered component* will take reasonable and appropriate steps to prevent unauthorized persons from viewing *EPHI* on *workstation*s.

C. Each *covered component* will take reasonable and appropriate steps to require *workforce members* to protect the physical security of portable *workstations* that store EPHI.

D. **HIPAA REGULATORY INFORMATION**

CATEGORY: Physical Safeguards
TYPE: Standard
HIPAA HEADING: Workstation Security
REFERENCE: 45 CFR 164.310(c)
SECURITY REGULATION STANDARDS LANGUAGE: *"Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."*

Policy Definitions

Access
Availability
Business associate
Confidentiality
Covered component
*Electronic Protected Health Information (*or *EPHI)*
HIPAA Security Regulations
Integrity
Risk
Workforce member
Workstation

Related HIPAA Documents

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation
HIPAA Operational Specification 2.A - Risk Analysis
HIPAA Policy 11 – Facility Access Controls
HIPAA Operational Specification 11.B - Facility Security Plan
HIPAA Policy 12 - Workstation Use
HIPAA Privacy Regulations covered component's Minimum Necessary Policy
Responsible Use of NYU Computers and Data 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