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

| | |
|---|---|
| **Title:** | Policy 12. Workstation Use |
| **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 its *covered component*s will specify and maintain reasonable and appropriate safeguards to maximize the security of *EPHI* by delineating proper *workstation* use. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

## Purpose of this Policy

New York University provides policies and specifications on *workstation* use that include documented instructions/procedures delineating the proper functions to be performed and the manner in which those functions are to be performed in order to maximize the security of *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 define the authorized purposes of each *workstation* or class of *workstation*s that can *access EPHI*.

B. New York University and its *covered component*s shall take reasonable and appropriate steps to ensure that *workforce member*s understand which purposes and functions are authorized on their *workstation*s and do not use *workstation*s for unauthorized purposes or to perform unauthorized functions. *Workforce member*s will be encouraged to report any unauthorized activity at a *workstation*.

C. New York University *workforce member*s will be instructed not to share *password*s with others, except to assure business continuity, as set forth in New York University's ***Password Management operational specification*** (see 6.D). If *workforce member*s suspect misuse of user IDs or *password*s, they are required to

promptly report that misuse to New York University's *EPHI* Security Officer and/or the *covered component*'s *EPHI* security officer.

D. Each covered component shall document and implement reasonable and appropriate procedures that indicate the manner in which *workstation*s *access*ing *EPHI* are located in physically secure areas and display screens are positioned or protected, in order to minimize the risk of *access* by unauthorized individuals and prevent unauthorized viewing of *EPHI*. This is more specifically addressed in New York University's ***Workstation Security policy*** (HIPAA Policy 13). Documentation and procedures should include such topics as:
    1. instruct New York University *workforce member*s to activate their *workstation* locking software when they leave their *workstation*s unattended for a period of time to be determined by the *covered component*.
    2. instruct New York University *workforce member*s to log off from their *workstation*s when their shift is complete.
    3. take reasonable and appropriate steps to ensure that *workstation*s removed from New York University facilities are protected with security controls equivalent to on-site *workstation*s.
    4. implement additional reasonable and appropriate precautions for portable *workstation*s (e.g., laptops, PDAs, portable medical equipment) that store *EPHI*.

**E. HIPAA REGULATORY INFORMATION**

**CATEGORY:** Physical Safeguards
**TYPE:** Standard
**HIPAA HEADING:** Workstation Use
**REFERENCE:** 45 CFR 164.310(b)
**SECURITY REGULATION STANDARDS LANGUAGE:** *"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic protected health information."*

## Policy Definitions

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

## Related HIPAA Documents

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation
HIPAA Policy 4 – Workforce Security
HIPAA Operational Specification 4.C – Termination Procedures
HIPAA Operational Specification 6.D – Password Management
HIPAA Policy 13 - Workstation Security
HIPAA Operational Specification 15.C – Automatic Logoff
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