

NEW YORK UNIVERSITY

HIPAA Information Security Policies, Specifications, and Definitions

Policy 12. Workstation Use

Responsible Officer: Associate Provost and Chief Information Technology Officer
Effective Date: January 1, 2005
Compliance Deadline: April 21, 2005
Date of Latest Revision: December 23, 2004

POLICY STATEMENT

New York University and its *covered components* 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.

REASON FOR 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.

OPERATIONAL REQUIREMENTS

- A. Each *covered component* will define the authorized purposes of each *workstation* or class of *workstations* that can *access EPHI*.
- B. New York University and its *covered components* shall take reasonable and appropriate steps to ensure that *workforce members* understand which purposes and functions are authorized on their *workstations* and do not use *workstations* for unauthorized purposes or to perform unauthorized functions. *Workforce members* will be encouraged to report any unauthorized activity at a *workstation*.
- C. New York University *workforce members* will be instructed not to share *passwords* with others, except to assure business continuity, as set forth in New York University's ***Password Management operational specification*** (see 6.D). If *workforce members* suspect misuse of user IDs or *passwords*, 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 *workstations accessing 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 members* to activate their *workstation locking software* when they leave their *workstations* unattended for a period of time to be determined by the *covered component*.
 2. instruct New York University *workforce members* to log off from their *workstations* when their shift is complete.

3. take reasonable and appropriate steps to ensure that *workstations* removed from New York University facilities are protected with security controls equivalent to on-site *workstations*.
4. implement additional reasonable and appropriate precautions for portable *workstations* (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.”*

DEFINITIONS

Access

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://aspe.os.dhhs.gov/admsimp/pl104191.htm>>.

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/admsimp/FINAL/FR03-8334.pdf>>.