

NEW YORK UNIVERSITY

HIPAA Information Security Policies, Specifications, and Definitions

Policy 5. Information Access Management

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 strives to protect the *confidentiality, integrity, and availability* of *EPHI* by taking reasonable steps to manage access to *EPHI* appropriately. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

REASON FOR POLICY

Safeguarding access to *EPHI* and *EPHI Systems* is integral to the University's compliance efforts under the *HIPAA Security Regulations*. This policy reflects New York University's commitment to comply with such regulations by taking reasonable and appropriate steps to manage access to *EPHI*.

OPERATIONAL REQUIREMENTS

- A. Each *covered component's Minimum Necessary Policy*, which is one of its HIPAA Privacy policies, and other policies as appropriate, shall be the basis for the type and extent of authorized access to *EPHI*. Access to *EPHI* will be granted only to *workforce members* who require specific information to accomplish the work responsibilities of their position, and will be granted on a need-to-know basis. Access shall be specified, documented, reviewed periodically, and revised as necessary.
- B. Access to *EPHI* shall not be granted until New York University *workforce members* have been properly cleared in accordance with New York University's *Workforce Security policy* (HIPAA Policy 4).
- C. Access to *EPHI* shall not be attempted by *workforce members* who are not properly cleared in accordance with New York University's *Workforce Security policy* (HIPAA Policy 4) and properly authorized to access such *EPHI* under this policy.
- D. New York University *workforce members* who manage systems containing or transporting *EPHI*, as well as managers and/or supervisors of *workforce members* who use data, shall determine and authorize appropriate access to *EPHI Systems* and document the process for authorizing such access, as set forth in its *Access Authorization operational specification* (see 5.A).
- E. New York University and each *covered component* shall document the process for establishing, documenting, reviewing, and modifying access to *EPHI*, as set forth in the University's *Access Establishment and Modification operational specification* (see 5.B).

F. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards
TYPE: Standard

HIPAA HEADING: Information Access Management

REFERENCE: 45 CFR 164.308(a)(4)(i)

SECURITY REGULATION STANDARDS LANGUAGE: “Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.”

OPERATIONAL SPECIFICATIONS

5.A Access Authorization

1. New York University is committed to take reasonable and appropriate steps to ensure that appropriate access to *EPHI* is granted.
2. Each *covered component* of New York University will implement a documented process for granting and authorizing appropriate access to *EPHI*, to include where feasible:
 - a. Procedure for permitting various levels of access to *EPHI*.
 - b. Procedure for logging and tracking authorization of such access to *EPHI*.
 - c. Procedure for reviewing and revising, on a periodic basis, authorization of access to *EPHI*.

3. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards

TYPE: ADDRESSABLE Implementation Specification for Information Access Management Standard

HIPAA HEADING: Access Authorization

REFERENCE: 45 CFR 164.308(a)(4)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
“Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.”

5.B Access Establishment and Modification

1. Each *covered component* of New York University will create a documented process for establishing, documenting, reviewing, and modifying access to *EPHI* in accordance with New York University’s *Information Access Management policy* (HIPAA Policy 5) and as set forth in the *Access Authorization operational specification* (see 5.A), to include:
 - a. Procedure for establishing and documenting different access levels to *EPHI*.
 - b. Procedure for documenting establishment of access to *EPHI*.
 - c. Procedure for reviewing on a regular basis *workforce members’* access privileges to *EPHI*.
 - d. Procedure for modifying the access privileges of *workforce members* to *EPHI*, as appropriate, based on the periodic reviews.
2. Each *covered component* shall properly authorize and train New York University *workforce members* to access *EPHI*, and shall document that process, to include:
 - a. Definition and classification of permitted access methods (e.g., user ID and password, two factor authentication, log-on procedure).
 - b. Definition and classification of length of time access will be permitted (e.g., indefinite; a fixed period for temporary employees; or a fixed limited period based on business need).
 - c. Procedure for granting and changing a *workforce member’s* access method.
 - d. Procedure for managing access rights in a networked and distributed environment.

- e. Procedure for appropriate logging and tracking of activities by an authorized *workforce member* on *EPHI*.
3. Security controls or methods that establish access to *EPHI* shall include:
 - a. The disabling or removing of access methods for *workforce members* who no longer require access to *EPHI*.
 - b. Confirmation that redundant user identifiers (i.e., user IDs) are not created.
 - c. User identifiers (i.e., user IDs) that enable *workforce members* to be uniquely identified. *Workforce members'* privilege levels will not be reflected in the structure of user IDs.
 - d. Each *covered component* will implement appropriate operational measures approved by the *covered component's EPHI* security officer when a legacy system is in place that permits only common or shared identifiers.
 4. Each *covered component* shall log and track modifications of New York University *workforce members'* access rights and securely maintain the tracking and logging information. Tracking and logging shall provide the following information:
 - a. Date and time of modification.
 - b. Identification of *workforce members* whose access is being modified.
 - c. Description of modified access rights.
 - d. Reason for modification of access rights.

5. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards

TYPE: ADDRESSABLE Implementation Specification for Information Access Management Standard

HIPAA HEADING: Access Establishment and Modification

REFERENCE: 45 CFR 164.308(a)(4)(ii)(C)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

“Implement policies and procedures that, based upon the covered entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.”

DEFINITIONS

Availability

Confidentiality

Covered component

Electronic Protected Health Information (or EPHI)

EPHI systems

HIPAA Security Regulations

Integrity

Workforce member

RELATED HIPAA DOCUMENTS

HIPAA Policy 1 - Overview: Policies, Procedures, and Documentation

HIPAA Policy 11 - Facility Access Controls

HIPAA Operational Specification 11.C - Access Control and Validation Procedures

HIPAA Policy 15 - Access Control

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://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>>.