

# NEW YORK UNIVERSITY

## HIPAA Information Security Policies, Specifications, and Definitions

### Policy 15. Access Control

Responsible Officer: Associate Provost and Chief Information Technology Officer  
Effective Date: January 1, 2005  
Compliance Deadline: April 21, 2005  
Date of Latest Revision: May 11, 2005

### POLICY STATEMENT

New York University and each *covered component* strives to protect the *confidentiality, integrity, and availability* of *EPHI* by taking reasonable and appropriate steps to ensure that *EPHI Systems* support and are installed with technical safeguards to control and restrict *access* to such *EPHI Systems* to persons and software programs that are *authorized* to have such *access* in accordance with New York University's *Information Access Management policy* (HIPAA Policy 5). Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

### REASON FOR POLICY

Although *access* controls, as required by the *HIPAA Security Regulations*, may differ under normal and *emergency* conditions, they are integral to the safeguarding of *electronic protected health information*. This policy reflects New York University's commitment to comply with such Regulations.

### OPERATIONAL REQUIREMENTS

- A. Each *covered component* shall take reasonable and appropriate steps to support appropriate types of *access* control technology for *EPHI Systems*.
- B. New York University will implement appropriate technical security controls and methods that permit *access* to *EPHI Systems* only to *authorized* persons as set forth in the operational specifications below in this policy, including:
  - 1. Unique user identifiers (user IDs) that enable *workforce members* to be individually identified and tracked (no redundant user IDs) as set forth in the *Unique User Identification operational specification* (see 15.A).
  - 2. *Emergency access* procedures that enable *authorized workforce members* to obtain *access* to necessary *EPHI* during a *disaster* or other *emergency* as set forth in the *Emergency Access Procedure operational specification* (see 15.B).
  - 3. Automatic log-off from *EPHI Systems* of *workforce members* from their *workstations* as set forth in the *Automatic Logoff operational specification* (see 15.C).
  - 4. *Encryption* of *EPHI* on *EPHI Systems* as reasonable and appropriate as set forth in the *Encryption and Decryption operational specification* (see 15.D)

### C. HIPAA REGULATORY INFORMATION

**CATEGORY:** Technical Safeguards  
**TYPE:** Standard  
**HIPAA HEADING:** Access Control  
**REFERENCE:** 45 CFR 164.312(a)(1)

**SECURITY REGULATION STANDARDS LANGUAGE:** “Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) [Information Access Management].”

## OPERATIONAL SPECIFICATIONS

### 15.A Unique User Identification

1. Each *covered component* of New York University will take reasonable and appropriate steps to ensure that *access* to *EPHI Systems* is granted to *workforce members* using unique user identifiers (i.e., user IDs) that:
  - a. Identify individual *workforce members* (i.e., no redundant user IDs)
  - b. Permit activities performed on *EPHI Systems* to be traced to the individual *workforce member* through the unique identifier
2. Unique user identifiers (i.e., user IDs) shall not give any indication of *workforce members’* privilege levels.
3. New York University and each *covered component* will have a procedure for assigning unique user identifiers (user IDs), which can include any or all of the following, or another appropriate method:
  - a. *Workforce members’* names
  - b. Exclusive numbers (e.g., PIN, password)
  - c. Biometric identification
4. The *EPHI* security officer of each *covered component* shall review and approve the use of any group user identifiers to gain *access* to *EPHI Systems*.

### 5. HIPAA REGULATORY INFORMATION

**CATEGORY:** Technical Safeguards

**TYPE:** REQUIRED Implementation Specification for Access Control Standard

**HIPAA HEADING:** Unique User Identification

**REFERENCE:** 45 CFR 164.312(a)(2)(i)

**SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:**  
“Assign a unique name and/or number for identifying and tracking user identity.”

### 15.B Emergency Access Procedure

1. New York University and each *covered component* of New York University will take reasonable and appropriate steps to establish, implement, and document an *emergency access* procedure delineating the necessary steps to enable *authorized workforce members* to obtain *access* to necessary *EPHI* during a *disaster* or other *emergency*.
2. New York University and each *covered component* will provide all appropriate *workforce members* with periodic training and awareness on the *emergency access* procedure.
3. New York University and each *covered component* will provide appropriate *workforce members* with a current copy of the *emergency access* procedure and keep an appropriate number of copies at a secure off-site location in conjunction with the Disaster Recovery Plan, as set forth in the *Disaster Recovery Plan operational specification* (see 8.B), and the Emergency Mode Operation Plan, as set forth in the *Emergency Mode Operation Plan operational specification* (see 8.C).

4. New York University's *EPHI* Security Officer and the *EPHI* security officer of each *covered component* will be responsible for approving the *emergency access* procedure as appropriate, updating it from time to time as necessary, and confirming that the procedure appropriately balances the need for *emergency access* to *EPHI* during a *disaster* or other *emergency* with the need to protect the *confidentiality, integrity, and availability* of *EPHI*.

#### 5. HIPAA REGULATORY INFORMATION

**CATEGORY:** Technical Safeguards

**TYPE:** REQUIRED Implementation Specification for Access Control Standard

**HIPAA HEADING:** Emergency Access Procedure

**REFERENCE:** 45 CFR 164.312(a)(2)(ii)

**SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:**

*"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency."*

### 15.C Automatic Logoff

1. When feasible, electronic sessions will be terminated and *workforce members* will be logged out of *EPHI Systems* after a number of minutes to be determined by the *covered component* (e.g., 3/5/10 minutes), requiring the user to be identified and authenticated again in order to regain *access* and continue the session.
2. New York University's *EPHI* Security Officer or the *covered component's EPHI* security officer will determine when it is not reasonable or appropriate to implement electronic automatic logoff mechanisms on certain *EPHI Systems* and will approve equivalent alternative mechanisms (e.g., screen/session locking, screensaver implemented after period of time).
3. New York University *workforce members* will be instructed to terminate electronic sessions on *EPHI Systems* when such sessions are completed and to log off from or lock their *workstations* or other *EPHI Systems* when their shifts are completed or when they expect to be away from their *workstation* or other *EPHI System* for an extended period of time (e.g., for lunch, meetings, breaks).

#### 4. HIPAA REGULATORY INFORMATION

**CATEGORY:** Technical Safeguards

**TYPE:** ADDRESSABLE Implementation Specification for Access Control Standard

**HIPAA HEADING:** Automatic Logoff

**REFERENCE:** 45 CFR 164.312(a)(2)(iii)

**SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:**

*"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."*

### 15.D Encryption and Decryption

1. Based on its *risk analysis*, New York University shall determine when to implement *encryption* for *EPHI* and *EPHI Systems* and the type and quality of the *encryption* algorithm and *cryptographic key* length.
2. New York University's *EPHI* Security Officer and the *EPHI* security officer of the *covered component*, based on the results of the *risk analysis*, shall approve the *encryption* mechanism used.
3. When *encryption* is used, New York University and each *covered component* shall:

- a. protect its *cryptographic keys* against modification and destruction, and protect its private keys against *unauthorized* disclosure.
  - b. implement a documented process for managing the *cryptographic keys* used to encrypt *EPHI* stored or maintained on *EPHI Systems*.
  - c. periodically determine activation and deactivation dates for its *cryptographic keys*.
4. New York University's *EPHI* Security Officer and each *covered component's* *EPHI* security officer shall maintain documentation defining when *encryption* is utilized to protect *EPHI* stored or maintained on *EPHI Systems*, and how such *encryption* is implemented.

## 5. HIPAA REGULATORY INFORMATION

**CATEGORY:** Technical Safeguards

**TYPE:** ADDRESSABLE Implementation Specification for Access Control Standard

**HIPAA HEADING:** Encryption and Decryption

**REFERENCE:** 45 CFR 164.312(a)(2)(iv)

**SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:**

*"Implement a mechanism to encrypt and decrypt electronic protected health information."*

## DEFINITIONS

*Access*

*Availability*

*Confidentiality*

*Covered component*

*Cryptographic key*

*Disaster*

*Electronic Protected Health Information (or EPHI)*

*Emergency*

*Encryption*

*EPHI systems*

*HIPAA Security Regulations*

*Integrity*

*Workforce member*

*Workstation*

## RELATED HIPAA DOCUMENTS

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

HIPAA Operational Specification 2.A – Risk Analysis

HIPAA Operational Specification 2.B – Risk Management

HIPAA Policy 5 - Information Access Management

HIPAA Operational Specification 5.A - Access Authorization

HIPAA Operational Specification 5.B - Access Establishment and Modification

HIPAA Operational Specification 6.D – Password Management

HIPAA Operational Specification 8.B - Disaster Recovery Plan

HIPAA Operational Specification 8.C - Emergency Mode Operation Plan

HIPAA Policy 11 - Facility Access Controls

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

HIPAA Policy 12 – Workstation Use

HIPAA Policy 19 - Transmission Security

HIPAA Operational Specification 19.A - Integrity Controls

HIPAA Operational Specification 19.B – Encryption

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>>.