

# NEW YORK UNIVERSITY

## HIPAA Information Security Policies, Specifications, and Definitions

### Policy 6. Security Awareness and Training

Responsible Officer: Associate Provost and Chief Information Technology Officer  
Effective Date: January 1, 2005  
Compliance Deadline: April 21, 2005  
Date of Latest Revision: April 15, 2005

#### POLICY STATEMENT

New York University and each *covered component* strives to protect the *confidentiality, integrity, and availability* of *EPHI* by developing, implementing, and reviewing periodically a documented program for providing security training and awareness to New York University *workforce members* who have access to *EPHI Systems*, including management, prior to being provided access to *EPHI* to enable them to appropriately protect *EPHI*. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

#### REASON FOR POLICY

NYU has the responsibility under the *HIPAA Security Regulations* for providing and documenting security awareness and training for University *workforce members* in order that those persons can properly carry out their functions while appropriately safeguarding *EPHI*. This policy reflects New York University's commitment to comply with such Regulations.

#### OPERATIONAL REQUIREMENTS

- A. Each *covered component* shall provide training and supporting reference materials to *workforce members*, as appropriate, to carry out their functions with respect to the security of *EPHI*. The method of delivery of such training shall be determined by the *covered component* and may include on-site or remote training. After the training has been conducted, New York University will maintain such records as it deems appropriate that confirm that a *workforce member* received training. Training should include:
  1. Awareness of and familiarity with New York University's and the *covered component's* security policies, specifications, and procedures, including:
  2. The secure usage of *EPHI*, as set forth in ***Protection from Malicious Software operational specification*** (see 6.B), ***Log-in Monitoring operational specification*** (see 6.C), and ***Password Management operational specification*** (see 6.D).
  3. *Risks* to the *confidentiality, integrity, and availability* of *EPHI*.
  4. Legal and business responsibilities of New York University and the *covered component* for protecting *EPHI*.
- B. New York University's *EPHI Security Officer* and each *covered component's EPHI security officer* will determine the frequency of the security training and awareness regarding log-in monitoring in accordance with New York University's ***Security Awareness and Training policy*** (HIPAA Policy 6).
- C. New York University and each *covered component* shall make its security policies and procedures available for reference and review by its *workforce members* with access to *EPHI*.

- D. Each *covered component* shall provide security information and awareness reminders and updates to its *workforce members*, as set forth in its ***Security Reminders operational specification*** (see 6.A).

## E. HIPAA REGULATORY INFORMATION

**CATEGORY:** Administrative Safeguards

**TYPE:** Standard

**HIPAA HEADING:** Security Awareness and Training

**REFERENCE:** 45 CFR 164.308(a)(5)(i)

**SECURITY REGULATION STANDARDS LANGUAGE:** “*Implement a security awareness and training program for all members of its [a covered entity’s] workforce (including management).*”

## OPERATIONAL SPECIFICATIONS

### 6.A Security Reminders

1. New York University’s *EPHI* Security Officer and each *covered component*’s *EPHI* security officer shall be responsible for taking reasonable steps to ensure that New York University *workforce members*, including those who work remotely, receive security information and awareness reminders periodically and as needed, including:
  - a. on information security *risks* and how to follow New York University’s security policies and procedures.
  - b. on how to use *EPHI Systems* in a manner that reduces security *risks*, and on selected security topics, including:
    - i. New York University security policies and procedures
    - ii. New York University security controls and processes
    - iii. Significant *risks* to *EPHI Systems*
    - iv. Legal and business responsibilities of New York University for protecting *EPHI Systems*
  - c. when any of the following events occur:
    - i. Substantial revisions are made to New York University’s security policies or procedures.
    - ii. Substantial new security controls are implemented at New York University.
    - iii. Significant changes are made to existing New York University security controls.
    - iv. Substantial changes are made to New York University legal or business responsibilities.
    - v. Substantial threats or *risks* arise against *EPHI Systems*.
2. Means of providing security information and awareness reminders and updates may include, but are not limited to, e-mail reminders, posters, letters, *workforce member* meetings, security days, screen savers, *information system* sign-on messages, newsletter articles, and information posted to a Web site.

### 3. HIPAA REGULATORY INFORMATION

**CATEGORY:** Administrative Safeguards

**TYPE:** ADDRESSABLE Implementation Specification for Security Awareness and Training Standard

**HIPAA HEADING:** Security Reminders

**REFERENCE:** 45 CFR 164.308(a)(5)(ii)(A)

**SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:** “*Implement: ...Periodic security updates.*”

### 6.B Protection From Malicious Software

1. New York University and each *covered component* of New York University will develop, implement, and periodically review a documented process for guarding against, detecting and reporting *malicious software* that pose *risks* to *EPHI*. New York University's and each *covered component's malicious software* prevention, detection, and reporting procedures shall include:
  - a. *Anti-virus software* installed and updated on *EPHI Systems*.
  - b. Procedures for New York University *workforce members* to report suspected or confirmed *malicious software*.
  - c. Plan for recovering from *malicious software* attacks.
  - d. Process to examine electronic mail attachments and downloads before they can be used on *EPHI Systems*.
2. New York University *workforce members* shall not bypass or disable *anti-virus software* installed on *EPHI Systems* unless properly authorized to do so.
3. New York University and each *covered component* will provide periodic training and awareness to its *workforce members* about guarding against, detecting, and reporting *malicious software*. Training and awareness for *workforce members* on protection from *malicious software* shall include, for example, the following topics:
  - a. How to discover *malicious software*
  - b. How to report *malicious software*
  - c. How to discover *malicious software* fraud
  - d. How to not download or receive *malicious software* including not opening or launching email attachments that may contain *malicious software*
  - e. How to use *anti-virus software* appropriately

#### 4. HIPAA REGULATORY INFORMATION

**CATEGORY:** Administrative Safeguards

**TYPE:** ADDRESSABLE Implementation Specification for Security Awareness and Training Standard

**HIPAA HEADING:** Protection from Malicious Software

**REFERENCE:** 45 CFR 164.308(a)(5)(ii)(B)

**SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:**

*"Implement: ...Procedures for guarding against, detecting, and reporting malicious software."*

### 6.C Log-In Monitoring

1. New York University and each *covered component* will develop, implement, and periodically review a documented process for monitoring log-in attempts to *EPHI Systems* and reporting log-in discrepancies. The log-in process may include, for example, the following attributes:
  - a. Notification displays upon log-in stating that the system must only be accessed by an authorized New York University *workforce member*.
  - b. Help messages that could assist an unauthorized user are not provided during the log-in process.
  - c. Limitations on the number of unsuccessful log-in attempts are implemented.
  - d. The system does not state which part of the log-in information is correct or incorrect if there is an error.
  - e. Prior to successfully completing the log-in process, *information system* or application identifying information is not provided.
  - f. Limit the time allowed for the log-in procedure.
  - g. Record failed log-in attempts.
  - h. After the specific pre-determined number of failed log-in attempts, a time period is documented before permitting further log-in attempts, or any further attempts are rejected until a designated New York University *workforce member* has given authorization.

- i. Upon completion of a successful log-in, the date and time of the previous successful log-in by the *workforce member* are displayed.
2. New York University will provide training and awareness periodically and as needed to New York University *workforce members* regarding the procedures for monitoring log-in attempts and reporting discrepancies regarding their access or log-in attempts. The log-in monitoring training and awareness shall include the following topics:
  - a. How to detect a log-in discrepancy
  - b. How to report a log-in discrepancy
  - c. How to successfully use New York University's secure log-in process

### 3. HIPAA REGULATORY INFORMATION

**CATEGORY:** Administrative Safeguards

**TYPE:** ADDRESSABLE Implementation Specification for Security Awareness and Training Standard

**HIPAA HEADING:** Log-in Monitoring

**REFERENCE:** 45 CFR 164.308(a)(5)(ii)(C)

**SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:**

*"Implement: ...Procedures for monitoring log-in attempts and reporting discrepancies."*

## 6.D Password Management

1. Each *covered component* of New York University shall develop, implement, and review a documented process for appropriately creating, changing, and safeguarding *passwords* used to verify users' identities and to obtain access to *EPHI*. New York University's *password* management procedure may include, for example:
  - a. Require and force regular *password* changes (e.g., every 30/60/90 days).
  - b. Require and force the use of individual *passwords* to maintain accountability.
  - c. Permit *workforce members* to select and change their own *passwords*.
  - d. Require unique *passwords* that meet the standards defined by New York University (e.g., no *password* re-uses for a minimum period of time).
  - e. Require *passwords* not to be displayed in clear text when inputting into *EPHI Systems*.
  - f. Require *passwords* to be given to New York University *workforce members* in a secure manner, through a pre-defined process.
  - g. Require changing of default vendor *passwords* immediately following installation of hardware or software.
  - h. Prohibit the use of "Admin" or "Administrator" as login for administrator accounts or of "Demo" for demonstration logins.
2. New York University shall require its *workforce members* to use the following standards when possible to create strong, secure *passwords*:
  - a. A minimum length of *passwords* is eight (8) characters
  - b. A combination of numeric, non-alphanumeric, and alphabetical characters and of capital and lowercase letters.
  - c. *Passwords* that are not easily guessable or obtained by using personal information such as names, pet's name, license plate, birthday
3. New York University and each *covered component* shall provide its *workforce members* with training and awareness on appropriately creating, changing, and safeguarding *passwords* used to verify users' identities and to obtain access to *EPHI*. *Password* management training and awareness shall include the following requirements for access to *EPHI Systems*:
  - a. New York University's *password* standards and guidelines.
  - b. The process for changing temporary *passwords* when assigned for new log-in.
  - c. The importance of avoiding maintaining *passwords* in a paper record.

- d. The significance of changing *passwords* and avoiding reusing *passwords*.
- e. The significance of keeping *passwords* confidential.
- f. The significance of using different *passwords* for personal and business accounts.
- g. The importance of not including *passwords* in any automated log-in process.
- h. The importance of changing *passwords* when there is an indication of *password* or *information system* compromise.
- i. The importance of logging off before leaving workstation.
- j. The importance of selecting a strong *password* (i.e., one that is of eight characters in length, is not easily guessable, and is a mixture of upper and lower case letters, numerals, and special characters.)

#### 4. HIPAA REGULATORY INFORMATION

**CATEGORY:** Administrative Safeguards

**TYPE:** ADDRESSABLE Implementation Specification for Security Awareness and Training Standard

**HIPAA HEADING:** Password Management

**REFERENCE:** 45 CFR 164.308(a)(5)(ii)(D)

**SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:**

*“Implement: ....Procedures for creating, changing, and safeguarding passwords.”*

## DEFINITIONS

*Anti-virus software*

*Availability*

*Confidentiality*

*Covered component*

*Electronic Protected Health Information (or EPHI)*

*EPHI systems*

*HIPAA Security Regulations*

*Information system*

*Integrity*

*Malicious code*

*Malicious software*

*Password*

*Risk*

*Virus*

*Workforce member*

*Worm*

## RELATED HIPAA DOCUMENTS

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

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