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

Title:	Policy 6. Security Awareness and Training
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 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 member*s 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.

Purpose of this Policy

NYU has the responsibility under the *HIPAA Security Regulations* for providing and documenting security awareness and training for University *workforce member*s 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.

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* 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. *Risk*s 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 member*s with access to *EPHI*.

D. Each *covered component* shall provide security information and awareness reminders and updates to its *workforce member*s, 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 member*s, including those who work remotely, receive security information and awareness reminders periodically and as needed, including:
    a. on information security *risk*s 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 *risk*s, and on selected security topics, including:
        i. New York University security policies and procedures
        ii. New York University security controls and processes
        iii. Significant *risk*s 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 *risk*s 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 *risk*s 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 member*s 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 member*s 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 member*s about guarding against, detecting, and reporting *malicious software*. Training and awareness for *workforce member*s 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 member*s 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 *password*s 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 *password*s to maintain accountability.
   c. Permit *workforce member*s to select and change their own *password*s.
   d. Require unique *password*s that meet the standards defined by New York University (e.g., no *password* re-uses for a minimum period of time).
   e. Require *password*s not to be displayed in clear text when inputting into *EPHI Systems*.
   f. Require *password*s to be given to New York University *workforce member*s in a secure manner, through a pre-defined process.
   g. Require changing of default vendor *password*s 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 member*s to use the following standards when possible to create strong, secure *password*s:
   a. A minimum length of *password*s is eight (8) characters
   b. A combination of numeric, non-alphanumeric, and alphabetical characters and of capital and lowercase letters.
   c. *Password*s 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 member*s with training and awareness on appropriately creating, changing, and safeguarding *password*s 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 *password*s when assigned for new log-in.
   c. The importance of avoiding maintaining *password*s in a paper record.
   d. The significance of changing *password*s and avoiding reusing *password*s.

e. The significance of keeping *password*s confidential.
f. The significance of using different *password*s for personal and business accounts.
g. The importance of not including *password*s in any automated log-in process.
h. The importance of changing *password*s 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."*

Policy Definitions

Anti-virus software
Availability
Business associate
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://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