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

Title:	Policy 18. Person or Entity Authentication
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 maintaining a documented *authentication* process for verifying the identity of any person or entity prior to granting them access to *EPHI*. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

Purpose of this Policy

In order to corroborate the authenticity of a person or entity prior to granting access to *EPHI* as required by the *HIPAA Security Regulations*, an *authentication* mechanism should be in place. 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. New York University and each *covered component* shall use appropriate *authentication* methods to confirm that only properly authenticated and authorized persons or entities access *EPHI*. Appropriate access methods may include:
   1. Unique user identifiers (user IDs)
   2. Security identifier (password)
   3. Password systems
   4. Personal Identification Number (PIN) systems
   5. *Security token system*s
   6. *Biometric identification system*s
   7. Telephone callback systems
   8. Digital signatures

B. New York University's *authentication* processes may include:
    1. Documented procedures for granting persons and entities *authentication* credentials or for changing an existing *authentication* method.
    2. Uniquely identifiable *authentication* identifiers in order to track the identifier to a *workforce member*.
    3. Documented procedures for detecting and responding to any person or entity attempting to access *EPHI* without proper *authentication*.
    4. Removing or disabling *authentication* credentials in *EPHI Systems* for persons or entities that no longer require access to *EPHI*.
    5. Periodic validation that no redundant *authentication* credentials have been issued or are in use.
    6. Protection of *authentication* credentials (e.g., passwords, PINs) with appropriate controls to prevent unauthorized access.
    7. When feasible, masking, suppressing, or otherwise obscuring the passwords and PINs of persons and entities seeking to access *EPHI* so that unauthorized persons are not able to observe them.

C. Access methods for *authentication* to *EPHI Systems* shall not be built into logon scripts. Exceptions may be made only after review and approval by the *EPHI* security officer of the *covered component*.

D. New York University shall limit *authentication* attempts to its *EPHI* to no more than the number of attempts reasonably determined by the *covered component*'s *EPHI* security officer within a specified time. *Authentication* attempts that exceed the limit may result, as appropriate, in:
    1. Disabling relevant account for an appropriate period of time
    2. Logging of event
    3. Notifying appropriate New York University management

E. New York University's *EPHI* Security Officer shall take reasonable and appropriate steps to ensure that *workforce member*s are provided training and awareness about the *authentication* methods used by New York University or by the appropriate *covered component*.

F. **HIPAA REGULATORY INFORMATION**

CATEGORY: Technical Safeguards
TYPE: Standard
HIPAA HEADING: Person or Entity Authentication
REFERENCE: 45 CFR 164.312(d)
SECURITY REGULATION STANDARDS LANGUAGE: *"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."*

Policy Definitions

Authentication
Availability
Business associate
Biometric identification system
Confidentiality
Covered component
Electronic Protected Health Information (or *EPHI*)
EPHI Systems
HIPAA Security Regulations
Integrity
Security token system
Workforce member

Related HIPAA Documents

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation
HIPAA Policy 6 - Security Awareness and Training
HIPAA Operational Specification 6.C - Log-in Monitoring
HIPAA Operational Specification 6.D - Password Management
HIPAA Policy 15 - Access Control
HIPAA Operational Specification 15.A - Unique User Identification
HIPAA Operational Specification 15.C - Automatic Logoff
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