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

Title:	Policy 9. Evaluation
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 strives to protect the *confidentiality*, *integrity*, and *availability* of *EPHI* by taking reasonable and appropriate steps to conduct, both centrally and at each *covered component*, periodic technical and non-technical evaluations of its security safeguards, including policies, controls, and processes, in response to environmental or operational changes affecting the security of *EPHI*, in order to demonstrate and document the extent of its compliance with its security policies and the *HIPAA Security Regulations*. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

Purpose of this Policy

Periodic evaluations of security safeguards, especially in response to environmental or operational changes, are necessary to re-affirm that *EPHI* continues to be protected in accordance with the *HIPAA Security Regulations.* 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 will undertake periodic technical and nontechnical evaluations of its security safeguards. To determine the extent of compliance with the standards implemented under the *HIPAA Security Regulations*, subsequent periodic reevaluations shall be conducted in response to environmental or operational changes occurring since the last evaluation that might impact the *confidentiality*, *integrity*, or *availability* of *EPHI*. Changes that may trigger a reevaluation of New York University's security safeguards include:

   1. Known *security incident*s
   2. Significant new threats or risks to security of *EPHI*

3. Changes to New York University's organizational or technical infrastructure

4. Changes to information security requirements or responsibilities

5. New security technologies that are available and new security recommendations

B. The evaluations shall be completed by a team designated by New York University's *EPHI* Security Officer. The evaluation may be conducted or certified by a third party if the University's *EPHI* Security Officer deems it necessary and appropriate, in which case such third party will be treated as a *business associate* of New York University in accordance with New York University's ***Business Associate Contracts and Other Arrangements policy*** (HIPAA Policy 10).

C. Each evaluation shall include reasonable and appropriate activities, such as:

1. A review of New York University's and/or the *covered component*'s security polices and procedures to evaluate their appropriateness and effectiveness at protecting against any reasonably anticipated threats or hazards to the *confidentiality*, *integrity*, and *availability* of *EPHI*.

2. A gap analysis to compare New York University's and/or the *covered component*'s security policies and procedures against actual practices.

3. An identification of threats and risks to *EPHI* and *EPHI Systems*, as set forth in New York University's ***Risk Analysis operational specification*** (see 2.A).

4. An assessment of New York University's and/or the *covered component*'s security controls and processes as reasonable and appropriate protections against the risks identified for *EPHI Systems*.

5. Testing and evaluation of New York University's and/or the *covered component*'s security controls and processes to determine whether they have been implemented properly and whether those controls and processes appropriately protect *EPHI*. An authorized *workforce member* shall be designated to conduct the testing.

D. The evaluation process and results shall be documented by the responsible *workforce member*(s) in a report that is provided to the *covered component*'s *EPHI* security officer and privacy officer and, as requested, to New York University's *EPHI* Security Officer and Privacy Officer.

E. Following each evaluation, New York University and/or the *covered component* shall update its security policies, procedures, controls, and processes if the results of the evaluation show that such updates are needed.

F. **HIPAA REGULATORY INFORMATION**

CATEGORY: Administrative Safeguards
TYPE: Standard
HIPAA HEADING: Evaluation
REFERENCE: 45 CFR 164.308(a)(8)(i)
SECURITY REGULATION STANDARDS LANGUAGE:
"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart."

Policy Definitions

Availability
Business associate
Confidentiality
Covered component
Data user
*Electronic Protected Health Information (*or *EPHI)*
EPHI systems
HIPAA Security Regulations
Information system
Integrity
Security incident
Workforce member

Related HIPAA Documents

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation
HIPAA Policy 2 – Security Management Process
HIPAA Operational Specification 2.A - Risk Analysis
HIPAA Policy 10 - Business Associate Contracts and Other Arrangements
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