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

Title:	Policy 3. Assigned Security Responsibility
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

The Assigned Security Responsibility policy is a reflection of New York University's commitment to institute reasonable and appropriate safeguards to ensure the *confidentiality*, *integrity*, and *availability* of *EPHI* by assigning a single employee, New York University's *EPHI* Security Officer, the responsibility for overseeing the development and implementation of the policies and procedures required by *HIPAA Security Regulations*. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

Purpose of this Policy

Under the *HIPAA Security Regulations*, New York University is required to designate a security official who is responsible for the development and implementation of its security policies and procedures. This policy reflects the University's commitment to comply with such regulations. In addition, the appointment of a University *EPHI* Security Officer will provide organizational focus to, and highlight the importance of, the University's efforts to safeguard *EPHI*.

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. The University's *EPHI* Security Officer shall take reasonable and appropriate measures to:
    1. Confirm that *EPHI Systems* are reasonably and appropriately protected and have reasonable and appropriate safeguards in order to safeguard the *confidentiality*, *integrity*, or *availability* of any of *EPHI*.
    2. Confirm that New York University is compliant with applicable federal, state, and local laws pertaining to security of *EPHI*.

3. Confirm that recently acquired *EPHI Systems* have options that support required and/or addressable implementation specifications of the *HIPAA Security Regulations* and New York University's internal security requirements.
4. Guide the development, documentation, and dissemination of appropriate security policies and procedures for the users and administrators of *EPHI Systems*.
5. Approve and oversee the administration, implementation, and selection of New York University security controls for *EPHI Systems*.
6. Review periodic reports from the *EPHI* security officers of the *covered component*s that confirm that New York University *workforce member*s receive security training on a periodic basis.
7. Consult New York University's Privacy Officer to confirm that security policies, procedures, and controls support compliance with the HIPAA Privacy Regulations.
8. Confirm that an inventory of *EPHI Systems* is maintained and updated on a periodic basis.
9. Review periodic reports from the *EPHI* security officers of the *covered component*s that confirm that a risk analysis of *EPHI Systems* is completed on a periodic basis as set forth in New York University's ***Risk Analysis operational specification*** (see 2.A)
10. Oversee the implementation of an effective risk management program as set forth in New York University's ***Risk Management operational specification*** (see 2.B).
11. Confirm that the threats and risks to the *confidentiality*, *integrity*, and *availability* of *EPHI* are monitored and evaluated.
12. Confirm that records of *EPHI Systems* are developed, monitored, and audited to identify security incidents and malicious activity as set forth in New York University's ***Information System Activity Review operational specification*** (see 2.D).
13. Oversee the development and implementation of an effective security incident response policy and related procedures as set forth in New York University's ***Response and Reporting operational specification*** (see 7.A).
14. Confirm that adequate physical security controls exist to protect *EPHI*.
15. Create reports, as necessary, to inform the University administration of continuing compliance.

B. In addition to the University's *EPHI* Security Officer, each *covered component* will designate an *EPHI* security officer for the *covered component* with responsibility for ensuring the *confidentiality*, *integrity*, and *availability* of *EPHI* within the *covered component* in accordance with New York University's HIPAA Information Security Policies. The *EPHI* security officers of the *covered component*s shall provide reports to the University's *EPHI* Security Officer in such a manner and at such times as the University's *EPHI* Security Officer may direct from time to time. Such reports may include incident reports, quarterly reports, and others.

C. **HIPAA REGULATORY INFORMATION**

CATEGORY: Administrative Safeguards
TYPE: Standard
HIPAA HEADING: Assigned Security Responsibility
REFERENCE: 45 CFR 164.308(a)(2)
SECURITY REGULATION STANDARDS LANGUAGE: *"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."*

Policy Definitions

Availability
Business associate
Confidentiality
Covered component
*Electronic Protected Health Information (*or *EPHI)*
EPHI systems

HIPAA Security Regulations
Integrity
Workforce member

Related HIPAA Documents

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation
HIPAA Policy 2 – Security Management Process
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