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

Title:	Policy 7. Security Incident Procedures
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 instituting and documenting reasonable and appropriate safeguards to identify, report, track, and respond to *security incident*s promptly. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

Purpose of this Policy

Awareness of, response to, and creation of reports about *security incident*s in the context of its operations are integral parts of New York University's efforts to comply with the *HIPAA Security 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 implement a documented process for promptly identifying, reporting, tracking, and responding to *security incident*s, and will conduct training awareness on those *security incident* procedures.

B. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards
TYPE: Standard
HIPAA HEADING: Security Incident Procedures
REFERENCE: 45 CFR 164.308(a)(6)(i)
SECURITY REGULATION STANDARDS LANGUAGE: *"Implement policies and procedures to address security incidents."*

Operational Specifications

7.A Response and Reporting

1. New York University and each *covered component* shall include, as appropriate, in its documented process for promptly identifying *security incident*s, the following:
   a. Risk analysis of *EPHI Systems*, as set forth in New York University's ***Risk Analysis operational specification (***see 2.A).
   b. On the basis of the risk analysis, identify what events constitute a *security incident* in the context of New York University's and the *covered component*'s operations.
   c. Process for identifying a *security incident*.

2. New York University and each *covered component* shall organize a *Security Incident* Response Team (SIRT) that is primarily responsible for *security incident* reporting and response will perform an investigation when evidence shows that a *security incident* has occurred and will respond promptly to the *security incident*. New York University and each *covered component* shall document its process for promptly responding to *security incident*s.

3. New York University and each *covered component* shall include, as appropriate, in its documented process for promptly reporting *security incident*s, a procedure for New York University *workforce member*s to report a *security incident* to the appropriate identified management personnel. A New York University *workforce member* will not prohibit or otherwise attempt to hinder or prevent another New York University *workforce member* from reporting a *security incident* to the SIRT and shall cooperate fully with *security incident* investigations.

4. New York University and each *covered component* shall include training and awareness for *workforce member*s, as appropriate, in its documented process for promptly identifying, reporting, tracking, and responding to *security incident*s in accordance with New York University's and the *covered component*'s security policies and procedures.

5. New York University and each *covered component* shall mitigate, to the extent practicable, harmful effects of *security incidents* that are known to the covered entity and document those *security incidents* and their outcomes.

6. When performing a risk assessment, New York University and each *covered component* shall assess the probability that the *electronic protected health information* has been compromised based on considerations that include at least the following four factors:
   a. the nature and extent of the *protected health information* involved, including the types of identifiers and the likelihood of re-identification;
   b. the unauthorized person who used the *protected health information* or to whom the disclosure was made;
   c. whether the *protected health information* was actually acquired or viewed; and
   d. the extent to which the risk to the *protected health information* has been mitigated.

7. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards
TYPE: REQUIRED Implementation Specification for *Security Incident* Procedures Standard
HIPAA HEADING: Response and Reporting
REFERENCE: 45 CFR 164.308(a)(6)(ii)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: *"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."*

Policy Definitions

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

Related HIPAA Documents

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation
HIPAA Operational Specification 2.A – Risk Analysis
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