

NEW YORK UNIVERSITY

HIPAA Information Security Policies, Specifications, and Definitions

Policy 1. Overview: Policies, Procedures, and Documentation

Responsible Officer: Associate Provost and Chief Information Technology Officer
Effective Date: January 1, 2005
Compliance Deadline: April 21, 2005
Date of Latest Revision: May 31, 2005

WHO IS AFFECTED BY THESE POLICIES

Affected by these policies are all *covered components* that may be designated by the University from time to time, including the NYU School of Medicine, NYU College of Dentistry, and the University 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, including the Bursar's Office, Controller's Division, including Accounts Payable, Information Technology Services, Insurance Department, Internal Audit, Office of the Chief Compliance Officer, Office of Legal Counsel, Office of Sponsored Programs, Press Office/Public Affairs, Public Safety, Treasurer's Office, and University Development and Alumni Relations. These policies affect all NYU *workforce members* in *covered components*.

POLICY STATEMENT

New York University strives to protect the *confidentiality, integrity, and availability of electronic protected health information (EPHI)* by taking reasonable and appropriate steps to address the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. These policies guide the University's efforts to comply with the requirements of the Security Regulations. The University does not intend for these policies and specifications to form a contract of any kind, including an employment contract. The University intends these policies and specifications to augment and reinforce the HIPAA Privacy policies and procedures of the University and its *covered components*. The University reserves the right to modify any or all of these policies and specifications without notice and at its discretion or as otherwise may be required by law. New York University maintains documentation of the policies and procedures that it implements to comply with the *HIPAA Security Regulations* in written (paper or electronic) format. All defined terms are noted in *italics*. The material below in this Policy 1 applies to all HIPAA policies.

REASON FOR POLICY

New York University is designated a hybrid organization under HIPAA. As such, its *covered components* are required to safeguard *EPHI* in accordance with the Security Regulations promulgated pursuant to HIPAA. These policies reflect New York University's commitment to comply with such Regulations.

OPERATIONAL REQUIREMENTS

A. Policy Authority and Enforcement

In regard to the authority and enforcement of New York University's security policies and procedures:

1. New York University's *EPHI* Security Officer has general responsibility for and will oversee the development and documentation of the University's security policies and procedures required by the *HIPAA Security Regulations*. The *EPHI* security officer of each *covered component* of New York University has responsibility for implementation of the policies and procedures required by the *HIPAA Security Regulations* at the *covered component*.
2. Members of the New York University workforce who violate any of the HIPAA security policies or specifications, or the procedures established thereunder, may be subject to disciplinary action, up to and including the termination of employment or contract with the University. Anyone who knows or has reason to believe that another person has violated the policies or specifications, or the procedures established thereunder, shall report the matter promptly to his or her supervisor, the *EPHI* security officer at the *covered component*, or the University's *EPHI* Security Officer. Any attempt to retaliate against a person for reporting a violation will itself be considered a violation of the policies and specifications and the procedures established thereunder, and may result in disciplinary action up to and including the termination of employment or contract with the University.
3. All alleged violations, or reports of violations, of the policies and specifications, and the procedures established thereunder, will be investigated and, where appropriate, steps will be taken to remedy the situation.

B. Policy Considerations

In determining the reasonableness and appropriateness of New York University's security policies and procedures, New York University will take into consideration its own and/or the *covered component's* characteristics related to its:

1. Size, complexity and capabilities
2. Technical infrastructure, hardware, and software capabilities
3. Costs of implementing security controls
4. Probability and criticality of risks to *EPHI*
5. Culture and strategic planning objectives

C. Policy Implementation

1. New York University and each *covered component* will implement its security policies, specifications, and procedures in accordance with its organizational process for policy implementation, and will be particularly aware of the documentation requirements concerning time limits, *availability*, and review.
2. New York University and each *covered component* will inform its *workforce members* about the security policies and procedures that apply to New York University generally, to the appropriate *covered component*, and to the *workforce members* in their individual roles.
3. If the *HIPAA Security Regulations* require an action, activity, or assessment to be documented, New York University or the *covered component*, as appropriate, will maintain a written record of the action, activity, or assessment.
4. New York University and the *covered component* will retain such documentation for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.
5. New York University and each *covered component* will make such documentation available as appropriate to *workforce members* who are responsible for implementing the procedures to which the documentation pertains.

D. Policy Review and Modification

New York University's *EPHI* Security Officer will perform periodic reviews of its security policies and procedures and revise them as necessary; each *covered component's* *EPHI* security officer will perform periodic reviews of its security procedures and revise them as necessary. New York University and each *covered component* will inform the *workforce members* of these updates. New York University's *EPHI* Security Officer and the *covered component's* *EPHI* security officer, as

appropriate, will review the policies and procedures and the required documentation periodically and revise them as necessary to respond to environmental or operational changes affecting the *confidentiality, integrity, or availability* of EPHI. In the event that a significant regulatory change occurs, the policies, specifications, and the *covered component's* procedures will be reviewed and updated as needed. Questions for clarification and suggestions about these policies can be sent to hipaa.policies@nyu.edu.

E. HIPAA REGULATORY INFORMATION

CATEGORY: Policies and Procedures and Documentation Requirements

TYPE: Standard

HIPAA HEADING: Policies and procedures

REFERENCE: 45 CFR 164.316(a)

SECURITY REGULATION STANDARDS LANGUAGE: *“Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart taking into account those factors specified in § 164.306(b)(2)(i),(ii),(iii), and (iv)[Security Standards: Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.”*

TYPE: Standard (Implementation Specifications are included in the body of the policy).

HIPAA HEADING: Documentation

REFERENCE: 45 CFR 164.316(b); 164.316(b)(i); 164.316(b)(ii); 164.316(b)(iii)

SECURITY REGULATION STANDARDS LANGUAGE: *“(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.”*

SECURITY IMPLEMENTATION SPECIFICATION LANGUAGE:

- (i) *Time limit (Required). “Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.”*
- (ii) *Availability (Required). “Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.”*
- (iii) *Updates (Required). “Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.”*

DEFINITIONS

Availability

Confidentiality

Covered component

Electronic Protected Health Information (or EPHI)

HIPAA Security Regulations

Integrity

Protected health information

Workforce member

RELATED HIPAA DOCUMENTS

HIPAA Policy 9 – Evaluation

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://aspe.os.dhhs.gov/admsimp/pl104191.htm>>.

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/admsimp/FINAL/FR03-8334.pdf>>.