

NEW YORK UNIVERSITY

HIPAA Information Security Policies, Specifications, and Definitions

Policy 2. Security Management Process

Responsible Officer: Associate Provost and Chief Information Technology Officer
Effective Date: January 1, 2005
Compliance Deadline: April 21, 2005
Date of Latest Revision: April 15, 2005

POLICY STATEMENT

New York University strives to ensure the *confidentiality, integrity, and availability* of *electronic protected health care information (EPHI)* by implementing a security management process that includes creating and maintaining appropriate and reasonable policies, procedures, and controls to prevent, detect, contain, and correct security violations. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

REASON FOR POLICY

New York University is required under the *HIPAA Security Regulations* to implement a security management process. This policy reflects New York University's commitment to comply with such regulations.

OPERATIONAL REQUIREMENTS

- A. New York University's security management process will include the following:
 - 1. New York University's commitment to take reasonable steps to ensure the *confidentiality, integrity, and availability* of *EPHI*.
 - 2. Institution of security controls, policies, and procedures that appropriately and reasonably prevent, detect, contain, and correct identified *risks* to the *confidentiality, integrity, and availability* of *EPHI*.
 - 3. Periodic reviews and revisions of security controls, policies, and procedures.
 - 4. Ongoing training and awareness for New York University's *workforce members* on these security controls, policies, and procedures.
- B. A *risk analysis and risk management* program shall be used as the basis for New York University's ***Security Management Process*** administered as set forth in New York University's ***Risk Analysis operational specification*** (see 2.A) and ***Risk Management operational specification*** (see 2.B).
- C. New York University administration, including the University's *EPHI Security Officer*, shall be responsible for security management. These responsibilities shall include:
 - 1. Approving New York University's information security policies, procedures, and controls.
 - 2. Approving, supporting, and, as appropriate, implementing New York University's ***Security Sanctions operational specification*** (see 2.C).
 - 3. Approving and supporting New York University's security awareness and training programs.
 - 4. Creating and enforcing policies that require appropriate clearance and training before a *workforce member* is permitted to access any *EPHI*.
- D. New York University's *EPHI Security Officer* shall oversee New York University's security management process.

- E. Certain supervisors and managers at New York University have stewardship responsibilities for *EPHI* which include the following security management responsibilities:
1. Protecting the *confidentiality, integrity, and availability* of *EPHI* for which they are responsible.
 2. Identifying and approving the use of security policies, procedures, and controls for the *EPHI* for which they are responsible.
 3. Authorizing appropriate access by New York University's *workforce members* to the *EPHI* for which they are responsible.
 4. Immediately reporting *risks, security incidents, and violations* of New York University's policies, procedures, and controls relating to the *EPHI* for which they are responsible.
 5. Supporting investigations of security violations with respect to the *EPHI* for which they are responsible.
 6. Contributing to New York University security training and awareness programs for *workforce members*.
- F. New York University's *workforce members* shall be responsible for protecting *EPHI* within their control from unauthorized access, modification, destruction, and disclosure, are expected to comply with these security policies and procedures, and are responsible for doing so. Responsibilities of *workforce members* who have access to *EPHI* include:
1. Using New York University data processing resources that contain *EPHI* only for appropriate purposes and consistent with their approved level of access and authorization.
 2. Being aware of and using New York University-approved security controls.
 3. Complying with New York University security policies, procedures, and standards.
 4. Immediately reporting any security violation to his/her supervisor, the *EPHI* security officer of the *covered component*, or the University's *EPHI* Security Officer.
 5. Attending appropriate New York University security training and awareness programs.

G. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards

TYPE: Standard

HIPAA HEADING: Security Management Process

REFERENCE: 45 CFR 164.308(a)(1)(i)

SECURITY REGULATION STANDARDS LANGUAGE: "Implement policies and procedures to prevent, detect, contain and correct security violations."

OPERATIONAL SPECIFICATIONS

2.A Risk Analysis

1. Each *covered component* of New York University will take reasonable steps to identify and prioritize the *risks* to the *confidentiality, integrity, and availability* of *EPHI* on a periodic basis. A documented *risk* analysis process as approved by the *covered component's EPHI* security officer shall be used as the basis for the identification, definition, and prioritization of *risks* to *EPHI*. The *risk* analysis shall include, where appropriate, the judgments used, such as assumptions, defaults, and uncertainties, and explicitly state and document them. The *risk* analysis shall be based on the following steps:
 - a. Inventory – A periodic inventory of *EPHI Systems* and the *security measures* implemented to protect those systems will be conducted by the *covered components*.
 - b. Security measures analysis – The *security measures* that have been implemented to protect *EPHI Systems* shall be analyzed, including preventive and detective controls.

- c. Risk likelihood determination – The identified *risks* shall be rated by assigning a ratio or percentage or by some other appropriate means that indicates the probability that a *vulnerability* is exploited by an actual *threat*. Three factors shall be considered when assigning the rating: 1) type of *vulnerability*, 2) existence and effectiveness of current security controls, and 3) *threat* motivation and capability.
 - d. Vulnerability identification – *Vulnerabilities* of *EPHI* shall be identified and prioritized by reviewing *vulnerability* sources and performing security assessments on a periodic basis.
 - e. Threat identification – Potential *threats* to the *confidentiality*, *integrity*, and *availability* of *EPHI* shall be identified, such as natural, human or environmental *threats*, and prioritized.
 - f. Impact analysis – The impact analysis shall determine the effect on the *confidentiality*, *integrity*, or *availability* of *EPHI* that results if a *threat* successfully exploits a *vulnerability*.
 - g. Risk determination – The information obtained in the six steps above shall be used to identify the level of *risk* to *EPHI*. The *risk* determination shall be based on:
 - i. The likelihood a certain *threat* attempts to exploit a *vulnerability*.
 - ii. The likely level of impact should the *threat* successfully exploit the *vulnerability*.
 - iii. The adequacy of planned or existing *security measures*.
2. Each *covered component* shall update the *risk* analysis on a periodic basis and shall use the *risk* analysis to inform its *risk* management process as set forth in New York University’s ***Risk Management operational specification*** (see 2.B). In addition to the periodic *risk* analysis updates that New York University completes, the *risk* analysis shall be updated when environmental or operational changes arise that impact the *confidentiality*, *integrity*, or *availability* of *EPHI*. Such changes include:
- a. New *threats* or *risks* that impact *EPHI*.
 - b. A *security incident* that impacts *EPHI*.
 - c. Changes to New York University’s or the *covered component*’s information security requirements or responsibilities that impact *EPHI*. (e.g., new state or federal regulation, new role defined in New York University, new or modified security control has been implemented).
 - d. Changes to New York University’s or the *covered component*’s organizational or technical infrastructure that impact *EPHI*. (e.g., addition of a new network, new hardware/software standard implemented, new method of creating, receiving, maintaining, or transmitting *EPHI*).
 - e. Hardware and software upgrades.
3. The documented *risk* analysis results shall be reviewed by New York University’s *EPHI* Security Officer, the *EPHI* security officer of the *covered component*, and appropriate members of the New York University administration, and shall be maintained in a secure fashion.

4. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards

TYPE: REQUIRED Implementation Specification for Security Management Standard

HIPAA HEADING: Risk Analysis

REFERENCE: 45 CFR 164.308(a)(1)(ii)(A)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity.”

2.B Risk Management

1. Each *covered component* of New York University, in order to protect the *confidentiality, integrity, and availability* of *EPHI*, will implement *security measures* designed to reduce the *risks* to *EPHI* to a reasonable and appropriate level.
2. The *risk* management process implemented by each *covered component* and conducted periodically shall be based on a documented process that is used as a basis for selection and implementation of the *security measures*. The *risk* management process will include the following:
 - a. Assessment and prioritization, on the basis of *risks*, of *EPHI Systems*.
 - b. Selection and implementation of reasonable, appropriate, and cost-effective *security measures* to manage, mitigate, or accept identified *risks*.
 - c. Security training and awareness on implemented *security measures* to *covered component workforce members*.
 - d. Periodic evaluation and revision, as necessary, of the *covered component's security measures*.
3. The *risk* management process, as an implementation process, is led by the *covered component's EPHI* security officer in consultation with the University's *EPHI* Security Officer and shall be based on the following:
 - a. Risk analysis – The *covered component's risk* analysis is the basis of its *risk* management activities, as set forth in New York University's ***Risk Analysis operational specification*** (see 2.A).
 - b. Risk prioritization - *Risks* identified in the *covered component's risk* analysis shall be prioritized on a scale from high to low based on the potential impact to *EPHI Systems*. Information on the probability of occurrence shall be based upon the *covered component's risk* analysis. The highest priority shall be given to those *risks* with unacceptably high *risk* ratings. Resources, as available, shall be allocated according to the identified *risks*.
 - c. Method identification – The appropriate security methods to minimize or eliminate identified *risks* to *EPHI* shall be identified. Security methods shall be identified based on the nature, feasibility, and effectiveness of the specific security method.
 - d. Cost-benefit analysis – The *covered component* shall identify and define the costs and benefits of implementing or not implementing the identified security methods.
 - e. Security method selection – Based on the cost-benefit analysis, the *covered component* shall select the most appropriate, reasonable, and cost-effective security methods for reducing identified *risks* to *EPHI*.
 - f. Assignment of responsibility – The selected security methods shall be implemented by the *covered component's EPHI* security officer and other *workforce members* who have assigned security responsibility and the appropriate expertise.
 - g. Security method implementation – The selected security methods shall be properly implemented by the responsible *workforce members*. The *covered component's EPHI* security officer is responsible for overseeing this implementation.
 - h. Security method evaluation – The selected and implemented security methods shall be evaluated and revised, as necessary, by the *covered component's EPHI* security officer.
4. The *covered component's* strategies for managing *risk* shall be proportionate with the *risks* to and sensitivity of *EPHI*. The *covered component's security measures* shall reasonably protect the *confidentiality, integrity, and availability* of *EPHI* and the *risk* will be managed on a continuous basis. The following methods are used to manage *risk*:
 - a. *Risk* acceptance
 - b. *Risk* avoidance
 - c. *Risk* limitation
 - d. *Risk* transference
5. The results of the *risk* management process shall be documented in writing, reviewed by New York University's *EPHI* Security Officer, and maintained by New York University and by the *covered component*.

6. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards

TYPE: REQUIRED Implementation Specification for Security Management Standard

HIPAA HEADING: Risk Management

REFERENCE: 45 CFR 164.308(a)(1)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

“Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306 (a) [Risk analysis].”

2.C Security Sanctions

1. New York University is committed to applying appropriate sanctions against New York University *workforce members* who fail to comply with the security policies and procedures of New York University and of the relevant *covered component*.
2. Each *covered component* of New York University will take reasonable steps to ensure that applicable security policies and procedures are adhered to by New York University *workforce members*. Reasonable compliance with these security policies and procedures is necessary to safeguard the *confidentiality, integrity, and availability* of *EPHI*.
3. Each *covered component* will provide periodic security training for *workforce members* about the applicable New York University and *covered component* security policies and procedures.
4. Each *covered component* shall impose appropriate sanctions against *workforce members* who do not comply with applicable New York University and *covered component* security policies and procedures. The imposition of those appropriate sanctions shall be a documented process.
5. Sanctions shall be proportionate to the severity of the non-compliance with the applicable security policies and procedures and may reflect, among other things, the extent to which the non-compliance affects the *confidentiality, integrity, and availability* of *EPHI*, and the employee’s awareness or knowledge of the non-compliance.
6. New York University’s *EPHI Security Officer*, the *EPHI security officer* at the *covered component*, the Human Resources and Legal departments, and other departments or personnel, all as applicable and appropriate, shall be involved in identifying and defining appropriate sanctions. Sanctions may include, but are not limited to:
 - a. Oral warnings
 - b. Suspension or limitation of access to New York University’s and/or the *covered component’s information systems*, repositories, and conduits that contain *EPHI*
 - c. Required re-training
 - d. Letter of warning
 - e. Suspension from work
 - f. Termination

7. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards

TYPE: REQUIRED Implementation Specification for Security Management Standard

HIPAA HEADING: Sanction Policy

REFERENCE: 45 CFR 164.308(a)(1)(ii)(C)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

“Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.”

2.D Information System Activity Review

1. New York University is committed to take reasonable and appropriate steps to review, on a periodic basis, records of activity on its *information systems* that create, receive, maintain, or transmit *EPHI*.
2. Each *covered component* of New York University will take reasonable and appropriate steps to ensure that *EPHI Systems* have the appropriate hardware, software, or procedural auditing mechanisms installed on them to enable review of *information system* activity on a periodic basis. The *covered component's risk* analysis shall determine the level and type of auditing mechanisms that will be implemented on *EPHI Systems*. Examples of generated reports of *information system* activity *auditable events* include:
 - a. Failed authentication attempts
 - b. Use of audit software programs or utilities
 - c. Access of particularly designated *EPHI* (e.g., *EPHI* regarding VIPs)
 - d. *Information system* start-up or shutdown
 - e. Use of privileged accounts (e.g., system administrator account)
 - f. *Security incidents*
3. When feasible, these *information system* activity auditing mechanisms will generate the following information about *information systems* activity:
 - a. Date and time of activity
 - b. Description of attempted or completed activity
 - c. Identification of user performing activity
 - d. Origin of activity (e.g., I/P address, workstation ID)
4. The *covered component* shall review logs of *information system* activity audit mechanisms implemented on *EPHI Systems* on a periodic basis. Findings from the *risk* analysis shall be used to help determine the frequency of such reviews; however, each *covered component* should review the audit mechanism on a periodic basis. The following factors should be considered with respect to the frequency of reviews of audit mechanisms:
 - a. The merit or sensitivity of the *EPHI* on the *EPHI Systems*.
 - b. The importance of the applications operating on the *information systems*.
 - c. The degree to which the *information systems* are connected to other *EPHI Systems* and the degree to which that connection poses a *risk* to the *EPHI*.
5. The *information system* activity audit mechanism review process shall include:
 - a. Definition of what activity is significant.
 - b. Procedures for defining how significant activity will be identified and, if appropriate, reported.
 - c. Procedures for maintaining the *integrity* of records of significant activity.
 - d. Identification of which *workforce members* will review records of activity.
 - e. Definition of which activity records need to be archived and for what duration.
6. For each of the *EPHI Systems*, the *covered component* shall maintain and follow a specific procedure for conducting *information systems* activity review, including review of *information systems* activity and review of *auditable events* on a periodic basis. These procedures shall identify the *information systems* activity to be reviewed and the auditing mechanism to be used to capture the *information systems* activity. The audit results shall be retained for six years.

7. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards

TYPE: REQUIRED Implementation Specification for Security Management Standard

HIPAA HEADING: Information System Activity Review

REFERENCE: 45 CFR 164.308(a)(1)(ii)(D)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

“Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.”

DEFINITIONS

Auditable event

Availability

Confidentiality

Covered component

Data steward

Electronic Protected Health Information (or EPHI)

EPHI systems

HIPAA Security Regulations

Information system

Integrity

Protected health information

Risk

Security incident

Security measures

Threat

Vulnerability

Workforce member

RELATED HIPAA DOCUMENTS

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation

HIPAA Policy 7- Security Incident Procedures

HIPAA Operational Specification 7.A - Response and Reporting

HIPAA Policy 16 - Audit Controls

HIPAA Operational Specification 17.A – Mechanism to Authenticate Electronic Protected Health Information

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>>.