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

Title: Policy 11. Facility Access Controls
Effective Date: January 1, 2005
Amended: October 3, 2016
Issuing Authority: Executive Vice President for Health; Vice President, Information Technology and Chief Information Officer
Responsible Officer: Executive Vice President for Health; Vice President, Information Technology and Chief Information Officer

Policy

New York University and each covered component will endeavor to protect the confidentiality, integrity, and availability of EPHI by taking reasonable and appropriate steps to protect EPHI Systems, as well as the facilities in which they are located, from unauthorized physical access, tampering, theft, and physical damage while taking reasonable and appropriate steps to ensure that access by properly authorized New York University workforce members is granted. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

Purpose of this Policy

In order to physically safeguard EPHI and EPHI systems, New York University recognizes its obligations under the HIPAA Security Regulations to provide security measures to protect its electronic information systems and the facilities in which they are housed from unauthorized access, while striving to ensure access by authorized workforce members. This policy reflects New York University’s commitment to comply with such Regulations.

Scope of this Policy

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 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 members in covered components.

Operational Requirements

A. New York University and each covered component will take reasonable and appropriate steps to locate EPHI Systems in locations where physical access can be reasonably controlled in order to minimize the risk of unauthorized access, including such steps as to:
   1. assess the exterior security of buildings that contain EPHI Systems and to include reasonable and appropriate protections where possible.
   2. provide a level of protection including protection from physical damage for EPHI Systems, as well as the facilities in which they are housed that is commensurate with that of identified threats and risks to the security of such EPHI Systems and its facilities.
3. create a facility security plan describing how it will protect its facilities in which EPHI Systems are located and equipment from unauthorized physical access, tampering, and theft, as set forth in its Facility Security Plan operational specification (see 11.B).

4. require workforce members to report loss or theft of any device, such as a key card, that allows them physical access to sensitive facilities or to areas having workstations that can access EPHI, as set forth in its Access Control and Validation Procedures operational specification (see 11.C).

5. document repairs and modifications related to the security of its sensitive facilities, as set forth in its Maintenance Records operational specification (see 11.D).

B. New York University and each covered component will establish and document procedures to:

1. provide physical access rights to specific areas where EPHI Systems are maintained. New York University will use reasonable efforts to provide physical access rights to a work area only to authorized workforce members.

2. review, on a periodic basis, the physical access controls used at its facilities to protect EPHI Systems and will review and revise physical access rights to New York University areas where EPHI Systems are maintained.

3. require New York University workforce members to carry or display New York University identification in accordance with procedures established by the applicable covered component.

4. require all visitors to show proper identification and authorization prior to gaining physical access to New York University areas where EPHI Systems are located.

C. New York University and each covered component will have a facility security plan detailing how it will protect its facilities in which EPHI Systems are located and equipment from unauthorized physical access, tampering, and theft, as set forth in its Facility Security Plan operational specification (see 11.B). Workforce members are required to report loss or theft of any device, such as a key card, that allows them physical access to sensitive facilities or to areas having workstations that can access EPHI, as set forth in its Access Control and Validation Procedures operational specification (see 11.C). Each covered component shall document repairs and modifications related to the security of its sensitive facilities, as set forth in its Maintenance Records operational specification (see 11.D).

D. HIPAA REGULATORY INFORMATION

CATEGORY: Physical Safeguards
TYPE: Standard
HIPAA HEADING: Facility Access Controls
REFERENCE: 45 CFR 164.310(a)(1)
SECURITY REGULATION STANDARDS LANGUAGE: “Implement policies and procedures to limit physical access to its [covered entity’s] electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.”

Operational Specifications

11.A Contingency Operations

1. Each covered component of New York University will take reasonable steps to ensure that in the event of a disaster or emergency, while operating in emergency mode, appropriate workforce members can enter its facilities to take the necessary actions as indicated in its respective procedures as set forth in the Disaster Recovery Plan operational specification (see 8.B) and Emergency Mode Operation Plan operational specification (see 8.C).

2. Based on its respective Disaster Recovery Plan, each covered component of New York University will develop, implement, and periodically review a documented procedure to allow authorized workforce members or business associates access to its facilities to support restoration of lost data. Each covered component of New York University shall define workforce members’ roles in its Disaster Recovery Plan, and address facilities, EPHI Systems and electronic media involved. Each covered component’s Disaster Recovery Plan should define how the actions taken by such workforce members are tracked and logged, and how unauthorized accesses can be detected and prevented.
3. Based on its respective Emergency Mode Operations Plan, each covered component of New York University will develop, implement, and periodically review a documented procedure to allow authorized workforce members to enter New York University’s facilities to enable continuation of processes and controls that protect the confidentiality, integrity and availability of EPHI while operating in emergency mode. Each covered component of New York University will define workforce members’ roles in its Emergency Mode Operations Plan. Its Emergency Mode Operations Plan should define how the actions taken by such workforce members are tracked and logged, and how unauthorized accesses can be detected and prevented.

4. In the event of an emergency, only authorized New York University workforce members shall be permitted to administer or modify processes and controls that protect the security of EPHI. New York University’s Emergency Mode Operations Plan shall define such workforce members and roles.

5. HIPAA REGULATORY INFORMATION

 CATEGORY: Physical Safeguards
 TYPE: ADDRESSABLE Implementation Specification for Facility Access Controls Standard
 HIPAA HEADING: Contingency Operations
 REFERENCE: 45 CFR 164.310(a)(2)(i)
 SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: “Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.”

11.B Facility Security

1. New York University is committed to take reasonable and appropriate steps to protect facilities and EPHI Systems from unauthorized access, tampering, or theft in order to protect the confidentiality, integrity, and availability of EPHI.

2. Each covered component of New York University shall develop, document, and implement a facility security plan that describes how it seeks to protect its facilities and EPHI Systems from unauthorized access, tampering, or theft in order to protect the confidentiality, integrity, and availability of EPHI, including appropriate physical safeguards for EPHI Systems. This risk analysis shall be the basis of the facility security plan.

3. Each covered component’s facility security plan should address such elements as the following:
   a. Identification of EPHI Systems to be protected from unauthorized access, tampering or theft.
   b. Identification of processes and controls used to protect EPHI Systems from unauthorized access, tampering or theft.
   c. Actions to be taken if unauthorized access, tampering or theft attempts have been made against EPHI Systems.
   d. Identification of the covered component’s workforce members’ responsibilities within the facility security plan.
   e. Maintenance schedule that specifies and documents how and when the plan will be reviewed and tested and a process for maintaining and revising the facility security plan. Such documentation should be made available to New York University’s EPHI Security Officer who will be responsible for taking reasonable steps to ensure the plan is tested and maintained appropriately.

4. Each covered component of New York University shall distribute the facility security plan to the necessary workforce members, provide appropriate training, and maintain an appropriate number of copies of the facility security plan off-site.

5. HIPAA REGULATORY INFORMATION

 CATEGORY: Physical Safeguards
 TYPE: ADDRESSABLE Implementation Specification for Facility Access Controls Standard
 HIPAA HEADING: Facility Security Plan
11.C Access Control and Validation Procedures

1. New York University is committed to take reasonable and appropriate steps to control and validate physical access to facilities containing EPHI Systems. Each covered component will define, document, and implement a procedure for controlling and validating physical access to facilities that house EPHI Systems, to include the following elements:
   a. provide workforce member access rights to highly sensitive areas only as needed in order to accomplish a legitimate business task.
   b. define and document roles or functions that require physical access rights to the facilities.
   c. periodically review and, where necessary, revise access rights to the facilities and EPHI Systems.
   d. track, log, and maintain in a secure manner physical access to the facilities.

2. Each covered component shall instruct workforce members
   a. not to attempt to gain physical access to sensitive facilities containing EPHI Systems for which they have not been given proper authorization to access.
   b. immediately to report to an appropriate authority, such as the University’s EPHI Security Officer or an EPHI security officer at the covered component, the loss or theft of any device (e.g., card, token) that enables physical access to facilities.
   c. to carry or display an identification badge when at facilities containing EPHI Systems. Visitors to sensitive facilities shall show proper identification and state their reasons for needed access prior to gaining access.

3. HIPAA REGULATORY INFORMATION

   CATEGORY: Physical Safeguards
   TYPE: ADDRESSABLE Implementation Specification for Facility Access Controls Standard
   HIPAA HEADING: Access Control and Validation Procedures
   REFERENCE: 45 CFR 164.310(a)(2)(iii)

   SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: “Implement procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.”

11.D Maintenance Records

1. Each covered component shall document repairs and modifications to the physical elements of its facilities that are related to the physical security of the facility and EPHI Systems and store the documentation in a secure manner. Such documentation should include such elements as:
   a. date and time of repair or modification,
   b. description of physical component prior to repair or modification,
   c. reason(s) for repair or modification (including any damage and any related security incident),
   d. person(s) performing repair or modification,
   e. outcome of repair or modification.

2. New York University or the covered component, as appropriate, shall provide training to the building maintenance personnel regarding this Maintenance Records operational specification in order that those workforce members take reasonable steps to inform the University’s EPHI Security Officer or other workforce member, as designated, when a repair or modification is made that impacts the physical security of New York University’s facilities.

3. REGULATORY INFORMATION

   CATEGORY: Physical Safeguards
Policy Definitions

Access
Availability
Business associate
Confidentiality
Covered component
Disaster
Electronic media
Electronic Protected Health Information (or E PHI)
Emergency
E PHI systems
Facility
HIPAA Security Regulations
Information system
Integrity
Risk
Workforce member

Related HIPAA Documents

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation
HIPAA Operational Specification 2.A - Risk Analysis
HIPAA Policy 5- Information Access Management
HIPAA Operational Specification 5.B - Access Establishment and Modification
HIPAA Policy 8 - Contingency Plan
HIPAA Operational Specification 8.B - Disaster Recovery Plan
HIPAA Operational Specification 8.C- Emergency Mode Operation Plan
HIPAA Policy 9 - Evaluation
HIPAA Policy 13 – Workstation Security
HIPAA Privacy Regulations covered component’s Minimum Necessary Policy

