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

Title:	Policy 8. Contingency Plan
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 taking reasonable and appropriate steps to establish and implement documented *emergency* response procedures in order to prepare for and respond to emergencies and *disaster*s that may damage or otherwise disable *EPHI Systems* and by taking reasonable and appropriate steps to ensure that critical data including applications, operating systems, database software, and other software supporting packages and tools will survive a *disaster* or other *emergency*. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

Purpose of this Policy

In order to safeguard *EPHI*, New York University and the *covered component*s must make efforts to plan for operational continuity in the event of *emergency* or *disaster* as required under the *HIPAA Security Regulations*. This policy reflects New York University's commitment to comply with such regulations. Only with effective business resilience will the University be able to avoid situations that may lead to increased *risk*s to *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. Through the combination of preventive and recovery controls and processes, New York University's and each *covered component*'s *disaster* and *emergency* response procedures will seek to reduce to an acceptable level the *risk* to the *confidentiality*, *integrity*, and *availability* of *EPHI Systems* by developing a Contingency Plan (commonly called Business Continuity Plan).

B. The Contingency Plan shall include:

1. A documented *disaster* and *emergency* recovery strategy that aligns with New York University's operational objectives and priorities.

2. A documented Data Backup Plan that aligns with the *disaster* and *emergency* recovery strategy. New York University or the *covered component*, as appropriate, shall back up and store copies of *EPHI,* as set forth in its ***Data Backup Plan operational specification*** (see 8.A).

3. A documented Disaster Recovery Plan that aligns with the *disaster* and *emergency* recovery strategy. New York University or the *covered component*, as appropriate, shall implement a documented Disaster Recovery Plan to recover *EPHI* if impacted by a *disaster* or other *emergency*, as set forth in its ***Disaster Recovery Plan operational specification*** (see 8.B)**.**

4. A documented Emergency Mode Operations Plan that aligns with the *disaster* and *emergency* recovery strategy. New York University or the *covered component*, as appropriate, shall implement a documented Emergency Mode Operations Plan to take reasonable steps to ensure the continuance of critical business processes that protect the security of *EPHI* during and immediately following a *disaster* or other *emergency,* as set forth in its ***Emergency Mode Operation Plan operational specification*** (see 8.C).

5. Testing, review, and revision of the Disaster Recovery Plan and Emergency Mode Operations Plan, as needed. New York University or the *covered component*, as appropriate, shall complete testing of its Disaster Recovery Plan and, if necessary, take reasonable steps to ensure that it is up-to-date and effective, as set forth in its ***Testing and Revision Procedure operational specification*** (see 8.D),.

6. Review and revision of the criticality analysis of *EPHI Systems*, as needed, and how such *EPHI Systems* are vulnerable to loss or other damage in the event of a *disaster* or other *emergency*. New York University or the *covered component*, as appropriate, shall have a process to identify and define the criticality of applications and data on *EPHI Systems*., as set forth in its ***Application and Data Criticality Analysis operational specification*** (see 8.E).

7. An annual test of the Contingency Plan conducted by New York University and its *covered component*s as set forth in its ***Testing and Revision Procedure operational specification*** (see 8.D) and retention of the documented results of the annual test.

C. New York University and each *covered component* shall provide periodic training about New York University's and/or the *covered component*'s *disaster* and *emergency* response procedures to *workforce member*s, as appropriate.

D. **HIPAA REGULATORY INFORMATION**

CATEGORY: Administrative Safeguards
TYPE: Standard
HIPAA HEADING: Contingency Plan
REFERENCE: 45 CFR 164.308(a)(7)(i)
SECURITY REGULATION STANDARDS LANGUAGE:
"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic *protected health information."*

Operational Specifications

8.A Data Backup Plan

1. Each *covered component* of New York University will take reasonable and appropriate steps to back up and store *EPHI* stored on *EPHI Systems* and to create exact and retrievable copies of *EPHI*.

2. Each *covered component* of New York University will create and implement a documented and detailed plan for creating and maintaining *backup data* from all electronic media associated with *EPHI* that:
    a. Defines who is responsible for taking reasonable steps to ensure the *backup* of *EPHI*.
    b. Defines a *backup* schedule.
    c. Specifies the *EPHI Systems* that are to be backed up.

d. Defines where *backup* media is to be stored and New York University *workforce member*s who may *access* the stored *backup* media.
e. Defines where *backup* media is to be kept secure before it is moved to storage.
f. Defines who may remove the *backup* media and transfer it to storage.
g. Defines *restoration* procedures to restore *EPHI* from *backup* media to the appropriate *EPHI Systems*.

3. Each *covered component* will implement a *backup* procedure that will
    a. generate up-to-date copies of *EPHI* that can be recovered in the event that *EPHI Systems* are damaged by or during a *disaster* or other *emergency*.
    b. complete periodic testing of its *restoration* procedures for *EPHI Systems* to confirm the effectiveness of those procedures and that the *EPHI* can be restored in the time set forth in the *covered component*'s ***Disaster Recovery Plan operational specification*** (see 8.B).
    c. document the retention period for *backup* media that contain *backup* copies of *EPHI*.
    d. store *backup* copies of *EPHI*, complete records of the *backup* copies, and document *restoration* procedures in a remote and secure location, within sufficient distance from the site.
    e. provide *access* to authorized *workforce member*s for timely retrieval of the *backup* information stored at the remote location.
    f. provide physical, environmental, and technical security for the *backup* media stored at the remote location that will be consistent with the security provided to *EPHI* onsite.

4. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards
TYPE: REQUIRED Implementation Specification for Contingency Plan Standard
HIPAA HEADING: Data Backup Plan
REFERENCE: 45 CFR 164.308(a)(7)(ii)(A)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."

8.B Disaster Recovery Plan

1. Each *covered component* of New York University will take reasonable and appropriate steps to maintain a documented and detailed Disaster Recovery Plan to recover *EPHI* that is lost, damaged, or corrupted in the event of a *disaster* or other *emergency*.

2. The Disaster Recovery Plan will include:
    a. The conditions under which the Disaster Recovery Plan may be activated.
    b. New York University *workforce member*s' roles and responsibilities in executing the Disaster Recovery Plan.
    c. Recommended procedures that contain the actions to be taken to restore *EPHI*, and to return *EPHI Systems* to normal operations, within a defined timeframe.
    d. Documented order in which *EPHI* will be restored and the *EPHI Systems* will be returned to operation.
    e. Documented reporting and notification procedures to the *covered component*'s *EPHI* security officer or designated *workforce member*s.
    f. In the event of a *disaster* or other *emergency*, procedures for permitting appropriate specified *workforce member*s physical *access* to the *covered component*'s facilities, and to any *backup* media on which *EPHI* is stored whether onsite or offsite, in order to carry out the recovery plan.
    g. Procedures that specify how and when the plan will be tested and maintained.
    h. An Emergency Mode Operation Plan as set forth in the ***Emergency Mode Operation Plan operational specification*** (see 8.C).

3. Each *covered component* will provide periodic training and awareness on the Disaster Recovery Plan to New York University *workforce member*s. The *covered component*'s *EPHI* security officer will determine

the frequency of the training and awareness in accordance with New York University's ***Security Training and Awareness policy*** (HIPAA Policy 6).

4. Each *covered component* will provide current copies of the Disaster Recovery Plan and training and awareness on that plan to the New York University *EPHI* Security Officer and to the appropriate New York University *workforce member*s on a periodic basis, as well as keep copies of the plan off-site.

5. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards
TYPE: REQUIRED Implementation Specification for Contingency Plan Standard
HIPAA HEADING: Disaster Recovery Plan
REFERENCE: 45 CFR 164.308(a)(7)(ii)(B)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Establish (and implement as needed) procedures to restore any loss of data."

8.C Emergency Mode Operation Plan

1. In an effort to enable continuation of critical operational procedures, New York University is committed to take reasonable and appropriate steps to ensure the *confidentiality*, *integrity*, and *availability* of *EPHI* by continuing operations and protecting *EPHI* during and immediately following an *emergency*.

2. Each *covered component* of New York University will implement a documented and detailed Emergency Mode Operation Plan designed to allow the continuation of critical operations processes, while permitting necessary *access* to and use of *EPHI*, during and immediately following an *emergency*.

3. The Emergency Mode Operation Plan will:
    a. Define and categorize reasonably foreseeable emergencies that could have an impact on the *confidentiality*, *integrity*, and *availability* of *EPHI Systems*.
    b. Include a procedure that specifies how the *covered component* will react to emergencies that impact the *confidentiality*, *integrity*, and *availability* of *EPHI*.
    c. Include a procedure for the *covered component* to follow during and immediately following an *emergency* that outlines how the *covered component* will maintain security processes and controls to ensure the *confidentiality*, *integrity*, and *availability* of *EPHI*.
    d. Include a procedure authorizing New York University *workforce member*s to enter New York University and any offsite location where *backup* storage media are stored to maintain the security processes and controls that protect the *confidentiality*, *integrity*, and *availability* of *EPHI* while the *covered component* is functioning in *emergency* mode.
    e. Identify and document processes and controls that protect the *confidentiality*, *integrity*, and *availability* of *EPHI* while New York University is functioning in *emergency* mode.

4. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards
TYPE: REQUIRED Implementation Specification for Contingency Plan Standard
HIPAA HEADING: Emergency Mode Operation Plan
REFERENCE: 45 CFR 164.308(a)(7)(ii)(C)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: *"Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of* electronic *protected health information while operating in emergency mode*."

8.D Testing and Revision Procedure

1. New York University and each *covered component* of New York University will take reasonable and appropriate steps to perform testing of its Contingency Plan to assess its sufficiency and determine whether it is accurate and up-to-date, and by making necessary revisions on a periodic basis.

2. New York University's *EPHI* Security Officer will receive the documented testing results. The *EPHI* security officer of the *covered component* will review and recommend revisions, as necessary, to the Contingency Plan to address any issues identified in the testing of the *disaster* recovery.

3. New York University and each *covered component* will use a change control process to modify its Disaster Recovery Plan to make it sufficient and keep it accurate and up-to-date. Events that result in a revision of the plan will include:
    a. *Disaster* recovery role and responsibility changes, including changes to contact information.
    b. Changes to New York University's and/or each *covered component*'s physical or technical infrastructure.
    c. Changes in *threat*s to *EPHI Systems*.
    d. Results of testing that indicate that the plan needs to be modified to ensure that it is sufficient, accurate, and up-to-date.

4. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards
TYPE: ADDRESSABLE Implementation Specification for Contingency Plan Standard
HIPAA HEADING: Testing and Revision Procedure
REFERENCE: 45 CFR 164.308(a)(7)(ii)(D)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures for periodic testing and revision of contingency plans."

8.E Applications and Data Criticality Analysis

1. Each *covered component* will analyze and document the criticality of *EPHI* and *EPHI Systems*. The purpose of this criticality analysis is to document the impact to its services, processes, and operating objectives if a *disaster* or other *emergency* causes *EPHI Systems* to become unavailable for a documented amount of time. The criticality analysis will serve as the basis for the prioritization of *EPHI* and *EPHI Systems*.

2. **REGULATORY INFORMATION**

CATEGORY: Administrative Safeguards
TYPE: ADDRESSABLE Implementation Specification for Contingency Plan Standard
HIPAA HEADING: Applications and Data Criticality Analysis
REFERENCE: 45 CFR 164.308(a)(7)(ii)(E)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Assess the relative criticality of specific applications and data in support of other contingency plan components."

Policy Definitions

Access
Availability
Backup
Business associate
Confidentiality
Covered component
Disaster
*Electronic Protected Health Information (*or *EPHI)*
Emergency
EPHI systems
HIPAA Security Regulations
Integrity

Restoration
Risk
Threat
Workforce member

Related HIPAA Documents

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation
HIPAA Operational Specification 2.A – Risk Analysis
HIPAA Policy 6 – Security Training and Awareness
HIPAA Operational Specification 14.D - Data Backup and Storage
HIPAA Policy 15 – Access Control
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