University of Colorado
Denver | Anschutz Medical Campus

Office of Regulatory Compliance

13001 E. 17th Place, Suite W1124
Mail Stop F497
Aurora, CO 80045
Main Office: 303-724-1010
Main Fax: 303-724-1019

HIPAA Policy 9.7

Title:	**Contingency Planning**
Source:	**Office of Regulatory Compliance**
Prepared by:	**Assistant Vice Chancellor for Regulatory Affairs**
Approved by:	**Vice Chancellor for Research**
Effective Date:	**July 1, 2013**
Replaces:	**03/31/2005**
Applies:	**All UCD campuses**

Introduction

Purpose

To help meet UCD's goal of protecting the availability, integrity, and confidentiality of electronic protected health information (ePHI), UCD has developed policies and procedures for responding to an emergency or other unexpected negative event or occurrence that may damage any system containing ePHI.

Reference

45 C.F.R. § 164.308(a)(4)(ii)(B)

45 C.F.R. § 164.308(a)(7)

45 C.F.R. § 164.310(d)(2)(iv)

45 C.F.R. § 164.312(a)(2)(ii).

Applicability

This policy applies to every unit within UCD that administers computer systems containing ePHI.

Policy

UCD shall ensure that ePHI is protected and accessible after an event occurs that prevents normal business operations and access procedures. It is the responsibility of units that house ePHI to do the same at a unit-level.

Procedures

A. Contingency Planning

In order to assure that ePHI is available and secure during an emergency, every unit within UCD that administers systems containing ePHI shall maintain a comprehensive plan for responding to emergencies. This plan shall describe contingency mode operations as well as steps to be taken to ensure the ability to carry on business functions if there is a disaster.

EPHI held at a campus-level by the Information Systems Department (IS) is protected by and subject to the campus' contingency plan which is created and maintained by IS.

B. Contingency Plan

Specifically, each unit contingency plan should describe mechanisms to:

1. Avoid interruptions to critical functions even while undergoing or recovering from a loss of electricity, fire, system failure, vandalism, natural disaster, or other occurrence where systems and data are threatened;

2. Minimize impact on total business operations by minimizing interruptions to critical functions so that they occur only infrequently, are brief in duration, and do not result in loss of business functionality; and,

3. Address complications and consequences of normal lost processing time, operations degradation, lost equipment replacement processes, insurance funds, alternative processing sites, temporary office space, equipment, key personnel, telephones, and other business basic equipment.

C. Components of Contingency Plan

The unit security officer, working with other key administration personnel, must create, obtain management approval, implement, maintain, and periodically review a contingency plan which includes the following components:

1. Data Backup and Storage Plan

The Data and Storage Backup Plan must provide for the creation and maintenance of an exact retrievable copy of ePHI in the unit. Backups should also be made prior to movement of equipment hosting ePHI. The plan may include maintenance and retrieval of paper files of protected health information (PHI).

a. UCD requires that each unit create and maintain an exact retrievable copy of the organization's ePHI. Backups are to be created in the most appropriate form (zipped diskette, tape, CD-ROM, FTP copy, etc) and in a timely manner. Note that the frequency and methodology of the back-up is directly dependent on the importance of the data to the organization, system complexity, system configuration, resources and value of data. Regardless of the frequency or methodology, backup data should be created and rotated often enough to avoid disruption if current files are lost or damaged.

b. Scheduling, Labeling, and Off-Site Storage. One copy of ePHI (daily, weekly, or monthly version) must be labeled and maintained on the unit's premises in a secure manner. An additional copy of ePHI (daily, weekly or monthly version), or a duplicate of the backup, must be maintained off-site in a manner that is environmentally secure and limited by physical access controls to prevent improper modification and to limit access to appropriate users only. The off-site location should be geographically different from the unit's location so the backup data will not be affected by the same disaster but is close enough to retrieve in a timely manner.

2. Disaster Recovery Plan

The Disaster Recovery Plan must define unit procedures to restore any loss of data and equipment due to an emergency, such as power loss, fire, system failure, vandalism, natural disaster, or other occurrence.

The unit disaster recovery planning must start with advance preparation, including the establishment of comprehensive lists and identification of workforce members responsible for carrying out work after the disaster.

The unit security officer will work with others as necessary to compile and maintain the information below, which must be stored in multiple formats, on and off site, to be used in the event of an emergency. Depending on the nature of the work unit and the criticality of its operation, creation of the following documents may be appropriate:

a. Inventories;

b. Floor plans;

c. List of backup systems/data, location and contact information, and list of individuals who may access site;

d. Critical forms and supplies stocked off-site;

e. List of reliable resources for equipment replacement;

f. Contract for backup agreement for space, processing hardware and software and resources on an emergency basis, including method of retracting and utilizing data history;

g. Processing priorities pre-approved by unit management;

h. System application and documentation (current copies of all applications need to be located on and off site in a secure manner); see Emergency Access Controls section below;

i. Testing and revision plans as detailed below;

j. List of job categories and/or individuals responsible for recovery of computer and other systems. Job categories may include restore operations, and/or retrieval of previously backed-up data; and,

k. List of all critical business partners and emergency contact information.

3. Emergency Mode Operation Plan

The Emergency Mode Operation Plan must provide for continuation of critical business processes for the protection and security of ePHI even during emergency mode operations.

The unit security officer will work with others as necessary to develop a critical Emergency Mode Operation Plan that allows for an orderly resumption of activities and system recovery to the point of failure. The plan should include an outline of the business priorities for the unit, including related assumptions and a final base plan with activation criteria based on those business priorities.

4. Testing and Revision Plan

The Testing and Revision Plan must provide for routine testing of contingency plans as necessary in accordance with the unit's system complexity, and other factors reviewed during the risk analysis and risk management process as defined in the Security Management Policy: [insert link to policy here].

a. Each component of the unit's contingency plan must be identified, evaluated, and prioritized for routine testing and adjustment or revision based on test outcomes. Test plans must be clearly documented and include instruction to notify involved parties of the test, disaster simulation, and relocation as well as a defined timeline.

b. Different levels of testing can be performed ranging from complete mock disasters to simple desk checking of logical procedures. Any time a modification is made to a system, a corresponding plan revision should be considered and tested.

5. Applications and Data Criticality Plan

The Applications and Data Criticality Plan must provide for the prioritization of system applications and related data in order to support resumption of normal business and/or systems processing.

To determine the order of priority for restoring systems after a disaster and ensuring that the most critical application and/or data is restored first, the unit must consider and list computer software applications and databases in order of importance, criticality, and data sensitivity. System recovery and other contingency plan functions must be prioritized based upon this list.

6. Emergency Access Controls

Units must develop plans and procedures for accessing unit level ePHI in the event of an emergency. This may involve placing new computer equipment into service, restoring data from backup devices, or creation of new logons, passwords, or other access codes.

Some emergencies may result from an internal process that does not work or because an individual who has access control is not available. In these cases temporary access authorizations may be used to access systems. To be effective during an emergency, access codes must be communicated in advance to designated workforce members, documented in a standard manner, and securely maintained.

D. Approval of Plans

All unit-level contingency plans (and all components) must be submitted to the UCD HIPAA Security Officer for review and approval.

E. Documentation and Records Retention

1. All decisions made and plans created pursuant to this policy must be documented and maintained securely.

2. All documentation pursuant to this policy must be kept for a period of at least six (6) years from the date of creation of the document or the date when the document was last in effect, whichever is later.