# CONTINGENCY PLAN POLICY

**Latest Revision: May 1, 2017**
**Original Effective Date: April 18, 2005**

**HIPAA Security Rule 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."* Standard 45 CFR 164.308(a)(7)(i)

*"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."* Required Implementation Specification for Contingency Plan Standard 45 CFR 164.308(a)(7)(ii)(A)

*"Establish (and implement as needed) procedures to restore any loss of data."* Required Implementation Specification for Contingency Plan Standard 45 CFR 164.308(a)(7)(ii)(B)

*"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*." Required Implementation Specification for Contingency Plan Standard 45 CFR 164.308(a)(7)(ii)(C)

*"Implement procedures for periodic testing and revision of contingency plans."* Addressable Implementation Specification for Contingency Plan Standard 45 CFR 164.308(a)(7)(ii)(D)

*"Assess the relative criticality of specific applications and data in support of other contingency plan components."* Addressable Implementation Specification for Contingency Plan Standard 45 CFR 164.308(a)(7)(ii)(E)

**Purpose:**

This policy reflects Cu Medicine's commitment to effectively prepare for and respond to emergencies or disasters in order to protect the confidentiality, integrity, and availability of its information systems.

**Policy:**

1. Cu Medicine must have a process for both preparing for and effectively responding to emergencies and disasters that damage the confidentiality, integrity, or availability of its information systems.

2. Cu Medicine's disaster and emergency response process must reduce the disruption to Cu Medicine's information systems to an acceptable level through a combination of preventative and recovery controls and processes. These controls and processes must identify and reduce risks to Cu Medicine's information systems and processes, and must be commensurate with the value of the information systems being protected or recovered.

3. Cu Medicine must have a backup plan for its information systems. Backup copies of all electronic protected health information (ePHI) on Cu Medicine information systems must be made regularly.

4. Cu Medicine must have adequate backup systems that ensure that all ePHI can be recovered following a disaster or media failure.

5. Backup of ePHI on Cu Medicine information systems, together with documented restoration procedures, must be stored in a secure remote location, at a sufficient distance from the facility to escape damage from a disaster at or near Cu Medicine.

6. Backup copies of ePHI stored at a secure, remote location must be accessible to authorized Cu Medicine employees for retrieval of the information and it must be given an appropriate level of physical and environmental protection consistent with the standards applied to ePHI physically located at Cu Medicine.

7. The retention period for backup of ePHI on Cu Medicine information systems and any requirements for archive copies to be permanently retained must be defined and documented.

8. Cu Medicine must create and document a disaster recovery plan to recover its information systems if they are impacted by a disaster.

9. Cu Medicine must have an emergency mode operations plan for protecting its information systems containing ePHI during and immediately after a crisis situation.

10. Cu Medicine must conduct regular testing of its backup, disaster recovery, and emergency mode operations plans to ensure they are current and operative. Restoration procedures for Cu Medicine's information systems containing ePHI must be regularly tested to ensure that they are effective.

11. The results of such tests must be documented and presented to appropriate Cu Medicine management. The backup, disaster recovery, and emergency mode operations plans must be revised as necessary to address issues or gaps identified in the testing process.

12. Cu Medicine's backup, disaster recovery, and emergency mode operation plans must be kept current. All appropriate Cu Medicine workforce members must have a current copy of the plan and an appropriate number of current copies of the plan must be kept off-site.

13. Cu Medicine must have a process for defining and identifying the criticality of its information systems and the data contained within them.

14. The prioritization of Cu Medicine information systems must be based on an analysis of the impact to Cu Medicine services, processes and business objectives if disasters or emergencies cause specific information systems to be unavailable for particular periods of time.

**Procedures:** Contingency Plan Documentation Table of Contents

**Scope/Applicability:** This policy is applicable to all departments that use or disclose electronic protected health information for any purpose.

This policy's scope includes all electronic protected health information.

**Regulatory Category:** Administrative Safeguards

**Definitions:** See glossary for key terms and acronyms used in this policy.
(On file with Security Officer)

**Policy Authority/ Enforcement:** Enforcement of this policy will reside with the Security Officer or appropriate Management.

**Related Policies:** Facility Access Controls Policy
Device and Media Controls Policy

**Renewal/Review:** This policy is to be reviewed periodically to determine if the policy complies with current HIPAA Security regulations. In the event that significant related regulatory changes occur, the policy will be reviewed and updated as needed.

| MM/DD/YYYY | COMMENT |
|---|---|
| **05/01/2017** | **Updated and reviewed for CU Medicine name change** |
| **9/20/13** | **Reviewed and updated for Omnibus Rules; Senior Security/Project Manager.** |
| **7/24/12** | **Reviewed; Senior Security/Project Manager.** |

**Governance:** Responsibility for adoption and/or implementation of this policy is as follows:

| Approving Body | | Executive Approval | |
|---|---|---|---|
| **Security Officer:** | **05/01/17** | **Chief Financial Officer:** | **05/01/17** |
| **Signature on file.** | **Date** | **Signature on file.** | **Date** |