H.1.G.ii

HIPAA Security Regulations

Title: HIPAA Security Disaster Recovery Planning Policy

Security Rule: 164.308(a)(7)

Purpose: To ensure that each covered component can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting systems containing ePHI.

Requirements:

1. All ePHI system owners must establish and implement disaster recovery plans for all systems, which addresses restoration and recovery of ePHI, and the systems required to make that ePHI available.

2. The disaster recovery plan must include the following:
   a. A data backup plan
   b. Manual downtime procedures to ensure continuity of care as well as continuity of business processes in the event of short-term and long-term outages.
   c. Procedures to restore ePHI from data backups in the event of a disaster resulting in data loss
   d. Procedures to enable the continuation of business critical functions and processes for the protection of ePHI during emergency or disaster situations
   e. Procedures to periodically test data backup and disaster recovery plans
   f. Procedures to periodically perform an application and data criticality analysis, establishing the specific applications and ePHI that are necessary to maintain operation in an emergency mode. To maintain business continuity, the critical ePHI needed to operate should be a priority.
   g. Procedures for logging system outages, failures, and data loss to critical systems.
   h. Procedures for training the appropriate personnel in implementation of the disaster recovery plan.

3. The disaster recovery plan must be documented and easily available to the necessary personnel at all times. A copy of the disaster recovery plan must be securely stored offsite with the disaster recovery backups.
This policy and its procedures must be reviewed and evaluated on a periodic basis to
ensure that they maintain their technical viability and effectiveness.

Non-compliance with this policy may result in disciplinary action, up to and including
termination of employment and/or criminal prosecution.

See: HIPAA Security Regulations: Sanction Policy

   HIPAA Security Regulations: Emergency Mode operation Plan

**Recommended By:** Emory HIPAA Security Working Group

**Effective Date:** April 20, 2005

**Authorized By:** Emory HIPAA Security Steering Committee

**Date of Last Edit:** January 14, 2009

**Review Date:** April 21, 2011