H.1.G.iv

HIPAA Security Regulations

Title: Testing and Revision Plan

Security Rule: 164.308(a)(7)

Purpose: All contingency and disaster recovery plans are tested on a periodic basis to ensure that business processes will continue in the event of system failures, natural disasters or other serious events.

Requirements:

1. Owners of systems containing ePHI will need to, as part of contingency and disaster recovery planning, build test and revision procedures to ensure that plans do not contain any weaknesses or shortcomings.

2. Test plans should contain the following elements:
   a. Scope of test
   b. Test objectives
   c. Type of test
   d. Assumptions
   e. Impact of disaster recovery testing on operations
   f. Test schedule
   g. Test team
   h. Training requirements as necessary

3. Each ePHI system owner will work with entity security designees to determine the appropriate testing methods. Tests may be accomplished in a number of ways, such as: walkthroughs or document reviews, simulation test at disaster recovery site or full interruption test, which results in activation of the disaster recovery plan with the original site shut down and the alternate site is responsible for all processing to test readiness.
   a. Tests and exercises will be performed on an annual basis.
   b. Test results will be documented and must indicate
      i. whether the test was successful or not
      ii. any deficiencies identified
      iii. a remediation plan that addresses all identified deficiencies
c. Test results will be retained for 6 years.

4. This policy and its procedures must be reviewed and evaluated on a periodic basis to ensure that they maintain their technical viability and effectiveness.

5. 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

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