H.1.G.iii

HIPAA Security Regulations

Title: Emergency Mode Operation Plan

Security Rule: 164.308(a)(7)

Purpose: To enable 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.

Requirements:

1. Each owner of a system containing ePHI will work with their covered entity’s security designee 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.

2. 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 they will react to emergencies that impact ePHI systems.
   c. Include a procedure to follow during and immediately following an emergency that outlines how to maintain security processes and controls.
   d. Include a procedure authorizing appropriate workforce members to enter onsite and/or any offsite location where backup storage media are stored to maintain the security processes and controls.
   e. Identify and document processes and controls that protect the confidentiality, integrity, and availability of ePHI while the entity is functioning in emergency mode.

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

Recommended By: Emory HIPAA Security Working Group

Effective Date: April 20, 2005
Authorized By: Emory HIPAA Security Steering Committee
Date of Last Edit:
Review Date: April 21, 2011