H.1.G.v
HIPAA Security Regulations

Title: Applications and Data Criticality Analysis

Security Rule: 164.308(a)(7)

Purpose: The purpose of this criticality analysis is to document the impact to services, processes, and operating objectives if a disaster or other emergency causes ePHI Systems to become unavailable for a period of time. The criticality analysis will serve as the basis for the prioritization of restoration of ePHI and ePHI Systems.

Requirements:

1. All owners of systems containing ePHI must work with a HIPAA Security designee to build an inventory of all information systems containing ePHI.
2. All systems containing ePHI must be prioritized by criticality of the application. Prioritization must be based on an analysis of the impact to the entity’s services, processes and business objectives if disasters or emergencies cause specific information systems to be unavailable for particular periods of time.
3. Prioritization must also include an analysis of the system’s criticality to the entity’s ability to function at normal levels.
4. The criticality analysis must be conducted with significant involvement from the administrators, users and other ePHI system owners within the entity.
5. The criticality analysis must be conducted at least annually and immediately after significant changes to the system or changes to business processes involving the use of the system.

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: January 14, 2009

Review Date: April 21, 2011