


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-28	1 of 2
TITLE: APPLICATIONS AND DATA CRITICALITY ANALYSIS POLICY				

PURPOSE:

The purpose is to assess the relative criticality of specific applications and data in support of other contingency plan components. This is a standard required under the Administrative Safeguards of the HIPAA Security Rule.

SCOPE:

This policy applies to Guam Memorial Hospital Authority in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit ePHI.

POLICY:

It is the policy for the Guam Memorial Hospital Authority to periodically assess the "critical" areas of the business systems, which would include:

- Critical business systems functions
- Critical storage and networking infrastructure
- Critical ePHI or records

The specific components of business systems applications and data criticality analysis include:

- Network architecture diagrams and system flowcharts that show current structure, equipment addresses, communication providers and system interdependencies.
- Identification and analysis of critical business processes surrounding ePHI.
- Identification and analysis of key applications and systems used to support critical business processes.
- A prioritized list of key applications and systems and their recovery time objectives.
- Documented results of an analysis of the internal and external interfaces with key applications and systems.
- Adequate redundancies within the network infrastructure to reduce or eliminate single points of failure.

Mitigating controls or work-around procedures in place and tested for single points of failure that are unable to be eliminated.

Reviewed: 01/2006
Revised: 02/2006
Approved: EMC 2/15/06

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, will be responsible for ensuring the implementation of the requirements of Applications and Data Criticality Analysis.

COMPLIANCE:

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy 6420-8. Legal actions also may be taken for violations of applicable regulations and laws such as HIPAA.

Applications and Data Criticality Analysis is an addressable implementation specification defined within the Contingency Plan standard (164.308 (a)(7)) in the Administrative Safeguards category of the HIPAA Security Rule.

PROCEDURES:

Procedures related to the Applications and Data Criticality Analysis standard include:

- Contingency Plan
- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operations Plan
- Testing and Revision Procedures

REFERENCES:

- HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>, February 20, 2003.
- CMS, "CMS Information Systems Security Policy, Standards and Guidelines Handbook", CMS, February 2002.
- International Standards Organization (ISO/IEC 17799:2000(E)).