


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-7	1 of 3
TITLE: RISK MANAGEMENT POLICY				

PURPOSE:

The purpose is to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule. This is a standard required under the Administrative Safeguards of the HIPAA Security Rule.

The objective of performing risk management is to enable Guam Memorial Hospital Authority to accomplish its mission by:

- Better securing systems that store, process or transmit electronic Protected Health Information (ePHI).
- Enabling management to make well-informed risk management decisions to justify the expenditures that are a part of the Information Technology (IT) and other budgets.
- By assisting management in authorizing or evaluating systems on the basis of supporting documentation resulting from the performance of risk management.

SCOPE:

This policy applies to Guam Memorial Hospital Authority in its entirety, including all facilities and systems that process ePHI.

POLICY:

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce the risk to an acceptable level.

Risk management related activities are essential to help identify critical resources needed to support the Guam Memorial Hospital Authority and the likely threat to all such resources.

The principal goal of the Guam Memorial Hospital Authority's risk management policy is to protect the organization, especially its ePHI, and its ability to perform its mission.

Risk management consists of three phases:

- Phase I: Risk Assessment
- Phase II: Risk Mitigation
- Phase III: Evaluation and Assessment (Residual Risk)

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

The activities that the Guam Memorial Hospital Authority will conduct in each phase are as follows:

Phase I: Risk Assessment

- System characterization
- Threat identification
- Vulnerability identification
- Safeguard analysis
- Likelihood determination
- Impact analysis
- Risk Determination
- Safeguard recommendations
- Results documentation

Phase II: Risk Mitigation

- Prioritize actions
- Evaluate recommended safeguard options
- Conduct cost-benefit analysis
- Select safeguards
- Assign responsibility
- Develop safeguard implementation plan
- Implement selected safeguards

Phase III: Evaluation and Assessment (Residual Risk)

- Evaluate safeguards deployed
- Evaluate security policies

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, has the responsibility to:

- Ensure that appropriate risk analysis covering at a minimal all ePHI are performed at a frequency of at least once a year
- Approve risk mitigation plans, risk prioritization, and the elimination or minimization of risks
- Facilitate timely actions, decisions and remediation activities

The HIPAA Security Officer must be supported by all system owners, data owners and other managers to identify and prioritize risks to ePHI. Risk management is an essential management function at Guam Memorial Hospital Authority.

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.

Risk Management is a required implementation specification defined within the Security Management Process standard (164.308 (a)(1)) in the Administrative Safeguards category of the HIPAA Security Rule.

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)).