


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-6	1 of 2
TITLE: RISK ANALYSIS POLICY				

PURPOSE:

The purpose is to conduct an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) held by the Guam Memorial Hospital Authority. 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 facilities and systems that process ePHI. Such risk analysis activities will be conducted at least once a year and must result in a comprehensive Risk Analysis Report that summarizes the risks, vulnerabilities to the confidentiality, integrity and availability of ePHI. This report must also identify recommended safeguards and prioritize all such risks and vulnerabilities.

POLICY:

Risk is defined as the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence.

The Guam Memorial Hospital Authority will conduct an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the Guam Memorial Hospital Authority.

All risk analysis activities that are to be implemented are organized into three phases. These phases are:

- Phase I: ePHI Documentation Phase
- Phase II: ePHI Risk Assessment Phase
- Phase III: ePHI Safeguards Determination Phase

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

Phase I: ePHI Documentation Phase

- Identify systems with ePHI
- Document the purpose of these systems
- Document the flow of ePHI

Reviewed: 01/2006
Revised: 02/2006

Approved: EMC 2/15/06

Phase II: ePHI Risk Assessment Phase

- Identify vulnerabilities and threats to ePHI
- Describe the risks
- Identify controls
- Describe the level of risk

Phase III: ePHI Safeguards Determination Phase

- Recommend safeguards for ePHI
- Determine residual risk to ePHI

The results of all identified risk analysis activities along with the safeguard and other recommendations must be summarized with supporting documentation in a Risk Analysis Report.

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for coordinating all activities associated with risk analysis. All involved employees who assist with risk analysis activities will be trained in the HIPAA Security Rule and Guam Memorial Hospital Authority's security policies with the objective that they understand their responsibilities and duties to reduce the risk of security violations.

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 Analysis 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.

FORM(S):

Forms related to the risk analysis policy include:

- Risk Assessment Survey

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)).