


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-5	1 of 2
TITLE: SECURITY MANAGEMENT PROCESS POLICY				

PURPOSE:

The purpose is to implement policies and procedures to prevent, detect, contain, and correct security violations. 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.

POLICY:

Security management process refers to the creation, administration, and oversight of policies to address the full range of security issues and to ensure the prevention, detection, containment and correction of security violations.

The Guam Memorial Hospital Authority will create, administer and oversee policies to ensure the prevention, detection, containment and correction of security violations. The Guam Memorial Hospital Authority will develop security policies to identify core activities in the areas of risk analysis, risk management, sanctions and information system activity review.

RESPONSIBILITIES:

The HIPAA security officer, under the delegated authority of the Hospital Administrator, is responsible for the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of its Information Technology assets including electronic protected health information.

The HIPAA security officer, , under the delegated authority of the Hospital Administrator, is responsible for leading compliance activities that bring the Guam Memorial Hospital Authority into compliance with the HIPAA Security Rule implementation specifications of:

- Risk analysis
- Risk management
- Sanction policy
- Information system activity review

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

PROCEDURE(S):

Procedures related to the Security Management Process standard include but are not limited to:

- Information system activity review procedure

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.

Security Management Process is a standard (164.308 (a) (1)) defined 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)).