


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-11	1 of 2
TITLE: WORKFORCE SECURITY POLICY				

PURPOSE:

The purpose of this policy is to implement policies and procedures to ensure that all members of the workforce have appropriate access to electronic protected health information (ePHI) and to prevent those workforce members who should not have access from obtaining access to ePHI. 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:

Members of the workforce as well as contractors and others shall access only those systems and information to which they are authorized.

Access will be provided on the basis of the Information Access Management Policy 6420-15.

The termination of any member of the workforce will result in the immediate implementation of the activities identified in Termination Procedures.

All members of the workforce will be appropriately trained so they understand Guam Memorial Hospital Authority's policies related to accessing authorized information only.

The Guam Memorial Hospital Authority will continually assess potential risks and vulnerabilities to ePHI in its possession and develop, implement, and maintain appropriate security measures so that access is only provided to authorized members of the workforce and all such information access is restricted to the minimum necessary to accomplish their job role or function.

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for determining the appropriate classification of information, such as ePHI and maintains a list that details the type of access for each individual.

Reviewed:
Revised:

Approved: EMC 2/15/06

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.

PROCEDURES:

Procedures related to the Workforce Security Policy include:

- Workforce Clearance Procedure
- Termination Procedure
- Password Management Policy

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)).