


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-15	1 of 2
TITLE: INFORMATION ACCESS MANAGEMENT POLICY				

PURPOSE:

The purpose is to implement policies and procedures for authorizing access to electronic protected health information (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 are to be granted access only to that ePHI to which they are authorized in order to perform their job role or associated job function.

All members of the workforce will be trained regarding appropriate access to ePHI, including the awareness of information access controls.

Safeguards such as role-based access control or context-based access control or mandatory access control or discretionary access control will be used as appropriate to control access to ePHI.

The Guam Memorial Hospital Authority will develop security policies to identify core activities in the areas of isolating health care clearinghouse function, access authorization, access establishment and modification.

RESPONSIBILITIES:

The Functional Application System Manager is responsible for determining the appropriate access for users to their system and the ePHI and will submit documented request to the HIPAA Security Officer.

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for assessing and granting the appropriate access to ePHI. The security officer is responsible for leading compliance activities that bring the Guam Memorial Hospital Authority into compliance with the HIPAA Security Rule implementation specifications of the Information Access Management standard:

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

- Isolating health care clearinghouse function
- Access authorization
- Access establishment and modification

Members of the workforce shall be guided by the HIPAA Privacy Rule's standard on Minimum Necessary and obtain only the type and amount of health information necessary to carry out the job role or function.

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.

Information Access Management is a standard (164.308 (a)(4)) defined in the Administrative Safeguards category of the HIPAA Security Rule.

PROCEDURES:

Department Heads and Supervisors must submit a request to the Information Technology (IT) department identifying the employee(s) they authorize to have access to ePHI and functional system application(s).

Procedures related to the Information Access Management Procedure include:

- Access Authorization Procedure
- Access Establishment and Modification Procedure
- Pass word Management Procedure

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)).