


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-31	1 of 2
TITLE: FACILITY ACCESS CONTROLS POLICY				

PURPOSE:

The purpose is to implement policies and procedures to limit physical access to Guam Memorial Hospital Authority's electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. This is a standard required under the Physical Safeguards of the HIPAA Security Rule.

SCOPE:

This policy applies to Guam Memorial Hospital Authority in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications, as well as all facilities, which process, store or transmit electronic protected health information (ePHI).

POLICY:

Guam Memorial Hospital Authority will launch activities to ensure compliance with the Facility Access Control standard and its associated implementation specifications of contingency operations, facility security plan, access control and validation procedures, and maintenance records.

Guam Memorial Hospital Authority will safeguard the facility and equipment from unauthorized physical access, tampering and theft.

Guam Memorial Hospital Authority will continually assess potential risks and vulnerabilities to ePHI and develop, implement and maintain appropriate safeguards to ensure compliance with the requirements of the HIPAA Security Rule.

All repairs and modifications to the physical components of the facility shall be documented and maintained by the Hospital Chief of Security and reported to the HIPAA Security Officer.

All repairs and maintenance, including installation, of hardware and software will be documented and maintained by the HIPAA Security Officer.

The Facility Security Plan shall be reviewed by the Hospital Chief of Security and the HIPAA Security Officer and updated at least once a year.

Maintenance of all hardware and software will be reviewed on an annual basis.

Tests on the security attributes of all hardware and software will be conducted on an annual basis.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, will be responsible for ensuring the implementation of the requirements of the Facility Access Control standard and its associated implementation specifications of contingency operations, facility security plan, access control and validation procedures, and maintenance records.

The Hospital Chief of Security, under the delegated authority of the Hospital Administrator, will be responsible for reviewing and updating the Hospital Entire Facility (Campus) Access Control Policy other than the secured electronic information systems computer room and office area.

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.

Facility Access Controls is a standard (164.310 (a)(1)) defined in the Physical Safeguards category of the HIPAA Security Rule.

PROCEDURES:

Access Control and Validation Procedures

FORMS:

Maintenance Records

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)).