


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-33	1 of 2
TITLE: FACILITY SECURITY PLAN POLICY				

PURPOSE:

The purpose is to implement policies and procedures to safeguard the facility housing the computer equipment and electronic protected health information (ePHI) therein from unauthorized physical access, tampering, and theft. 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 develop a Facility Security Plan with the objective of safeguarding main computer and data facilities and premises from unauthorized physical access, tampering or theft including the equipment present in all such facilities.

The Facility Security Plan must define the security perimeter of all buildings and sites. Further, the Plan should ensure that all external doors are adequately secured against unauthorized access by installing locks, alarms, or other access control devices.

Internally, within buildings and facilities, all doors and windows must be locked by default. Further, intrusion detection capabilities must be evaluated to secure privileged internal areas. Also, physical barriers must be in place from the floor to the ceiling.

The Facility Security Plan will be reviewed, and if necessary, updated at least once a year.

Controls will need to be deployed to protect against theft as well guard against fire, water or other damage. To the extent possible power and communications cabling must be located underground.

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 Security Plan. The HIPAA Security Officer is responsible for reviewing and updating the plan as necessary.

Reviewed: 01/2006
Revised: 02/2006
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.

Facility Security Plan is an addressable implementation specification defined within the Facility Access Controls standard (164.310 (a)(1)) in the Physical 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)).