


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-8	1 of 2
TITLE: SANCTION POLICY				

PURPOSE:

The purpose of this policy is to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the Guam Memorial Hospital Authority. This is a standard required under the Administrative Safeguards of the HIPAA Security Rule.

Guam Memorial Hospital Authority will ensure all members of its workforce comply with the security policies or the organization as well as state and federal regulations such as HIPAA by applying sanction and disciplinary actions appropriate for the breach of policy.

SCOPE:

This policy applies to all Guam Memorial Hospital Authority workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers.

POLICY:

Guam Memorial Hospital Authority will appropriately discipline employees and other workforce members for any violation of security policy or procedure to a degree appropriate for the gravity of the violation. These sanctions include, but are not limited to, re-training, verbal and written warnings and immediate dismissal from employment.

In addition, workforce members who knowingly and willfully violate state or federal law for improper use or disclosure of an individual's information are subject to criminal investigation and prosecution or civil monetary penalties.

Guam Memorial Hospital Authority will record all disciplinary actions taken in the employment records of the employee.

Guam Memorial Hospital Authority will investigate any security incidents or violations and mitigate to the extent possible any negative effects that the incident may have had in a timely manner.

Guam Memorial Hospital Authority and its workforce members will not intimidate or retaliate against any workforce member or individual that reports the incident.

Reviewed: 01/2006
Revised: 02/2006

Approved: EMC 2/15/06

RESPONSIBILITIES:

All individuals identified in the scope of this policy are responsible for:

- Compliance with any sanction that is applied to them under this policy

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for:

- Reviewing reported security incidents and violations of security policy and levying, based on the gravity of the breach, appropriate sanctions upon the workforce member.

COMPLIANCE:

Failure to comply with this or any other security policy will result in disciplinary actions as per this Sanction Policy 6420-8. Legal actions also may be taken for violations of applicable regulations and laws such as HIPAA.

Sanction Policy is a required implementation specification defined within the Security Management Process standard (164.308 (a)(1)) 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)).