


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-18	1 of 3
TITLE: SECURITY AWARENESS AND TRAINING POLICY				

PURPOSE:

The purpose is to implement a security awareness and training program for all members of the Guam Memorial Hospital Authority's workforce, including management. This is a standard required under the Administrative Safeguards of the HIPAA Security Rule.

Guam Memorial Hospital Authority understands that "people", not necessarily technology, are often the largest threat to the security of sensitive information, such as electronic protected health information (ePHI) in the organization.

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, and anyone else granted access to sensitive information, such as ePHI, by Guam Memorial Hospital Authority.

POLICY:

Guam Memorial Hospital Authority will ensure that all workforce members have been trained in and understand the security policies and procedures. In addition, all workforce members will be trained how to identify, report, and prevent potential security incidents.

Security training will be an ongoing activity at Guam Memorial Hospital Authority. Periodic security reminders will keep workforce members up to date with new threats, such as computer viruses or "scams" to watch out for. The frequency and form these reminders take will be determined by the HIPAA Security Officer but should include things like security-related flyers or posters in break rooms, attached to paycheck stubs, broadcast through emails or system messages, and verbal updates at staff meetings.

Guam Memorial Hospital Authority will run anti-virus software on all computers that connect to the Internet and/or are networked together. Members of the workforce must be trained how to use the software and how to spot unusual activity that might indicate the presence of a virus. The anti-virus software must be kept up to date with live updates, as new viruses (and other types of malicious code) are discovered daily.

Reviewed: 01/2006
Revised: 02/2006
Approved: EMC 2/15/06

The Guam Memorial Hospital Authority will develop security policies to identify core activities in the areas of security reminders, protection from malicious software, log-in monitoring, and password management.

RESPONSIBILITIES:

All workforce members are responsible for:

- Understanding and following all security related policies and procedures

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

- Ensuring all workforce members understand and follow security related policies and procedures
- Maintaining an ongoing security awareness program at Guam Memorial Hospital Authority
- Ensuring all workforce members understand and use the installed anti-virus software
- Keeping all anti-virus software up to date

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for leading compliance activities that bring the Guam Memorial Hospital Authority into compliance with the HIPAA Security Rule implementation specifications of:

- Security reminders
- Protection from malicious software
- Log-in monitoring
- Password management

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.

Security Awareness and Training is a standard (164.308 (a)(5)) defined in the Administrative Safeguards category of the HIPAA Security Rule.

PROCEDURES:

Procedures related to the Security Awareness and Training Procedure includes:

- Workforce Security Procedure
- Information Access Management Procedure
- Access Authorization Procedure
- Access Establishment and Modification Procedure
- Password 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)).