


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-37	1 of 2
TITLE: WORK STATION SECURITY POLICY				

PURPOSE:

The purpose is to implement physical safeguards for all workstations that access electronic protected health information (ePHI) and to restrict access to authorized users. This is a standard required under the Physical Safeguards of the HIPAA Security Rule.

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 by Guam Memorial Hospital Authority. In addition, this policy applies to all workstations and other computing devices owned or operated by Guam Memorial Hospital Authority and any computing device allowed to connect to Guam Memorial Hospital Authority's internal network.

POLICY:

Physical safeguards will be implemented for all workstations that access ePHI to restrict access to authorized users only.

All members of the workforce will be trained on the appropriate and authorized use of workstations as part of the security awareness training.

Workstations will be positioned such that the monitor screens and keyboards are not within view of unauthorized individuals.

Users will logoff prior to leaving the workstation. Users will store any written passwords in secure locations only – under no circumstance must any password information be accessible on the workstation or its vicinity.

Workstations must be labeled to identify function and location and assist with compliance with access control procedures.

All workstations must be operated in a manner that ensures:

- Confidentiality of ePHI.
- Display of an appropriate warning banner prior to gaining operating system access.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

- Employment of a password protected screen saver and/or workstation locking mechanism when the workstation is unattended.
- Proper log off and shut down of workstations at the end of the business day.
- Routine back up of all critical data.
- Virus scanning of media prior to use on any workstation.
- Only approved software may be used on Guam Memorial Hospital Authority's systems.
- Workstations and said software is used in accordance with contract agreements and copyright laws.
- Procedures must be maintained that require users to run an up-to-date anti-virus program on all computing devices at Guam Memorial Hospital Authority.
- All unnecessary and unused services (or ports) must be disabled
- Measures will be taken to physically protect computers that are located in public areas and portable computers such as laptops and PDAs that can be taken off the premises.
- Computers located in public areas will be situated as to block unauthorized viewing and/or will have screen savers that black out the screen.

RESPONSIBILITIES:

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

- Using Guam Memorial Hospital Authority computing devices only for work related purposes
- Following all procedures implemented by the HIPAA Security Officer related to this policy.

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

- Maintaining procedures required to support this policy
- Supporting and ensuring compliance by workforce members

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.

Workstation Security is a standard (164.310 (c)) defined 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)).