


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-36	1 of 2
TITLE: WORK STATION USE POLICY				

PURPOSE:

The purpose is to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific computer workstation or class of workstation and computer equipment that can access electronic protected health information (ePHI). 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, such as ePHI, 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:

The workstations and other computing devices at Guam Memorial Hospital Authority are to be used for work related purposes only. This includes, but is not limited to, Internet and Web access as well as the use of e-mail at Guam Memorial Hospital Authority. Workforce members should not expect any level of privacy as their activities, e-mails, files, and logs may be viewed at any time by the HIPAA Security Officer or other members of management in support of this and other policies and procedures.

Guam Memorial Hospital Authority may revoke the access rights of any individual at any time in order to protect or secure the confidentiality, integrity, and availability of sensitive information or to preserve the functionality of electronic information systems. Guam Memorial Hospital Authority will implement reasonable and appropriate measures to secure its computer workstations and computing devices that could be used to access sensitive information. These measures will include, but are not limited to the following:

- All user and administrator accounts must be protected by some form of authentication. If passwords are used, they must follow the guidelines set forth in the GMHA Password Management Policy 6420-3 and Person or Entity Authentication Policy 6420-51.
- All users accessing Guam Memorial Hospital Authority computing devices must have and use a unique user ID as set forth in the GMHA Password Management Policy 6420-3 and Person or Entity Authentication Policy 6420-51.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

- Procedures must be maintained that implement security updates and software patches in a timely manner.
- 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.
- No food or drinks are allowed to be consumed or placed on, near or around Computer Equipment.
- No personal games, music or video are allowed to be installed and played Hospital computers.
- Only software licensed to Guam Memorial Hospital Authority can be installed and used on Hospital computers in accordance with GMHA Computer Software Policy 6420-4.
- Maintain media backup of computer contents such as data, programs, documents and files for recovery and restoration purposes. This should be done as frequently as possible.
- Computer equipment should not be moved within or removed from the Hospital without approval from the HIPAA Security Officer and the Hospital Administrator.
- Use of Personally owned Computer equipment at or within the Hospital is prohibited until approved by the Hospital Administrator and the HIPAA Security Officer.

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 Workstation Use standard.

Hospital staff will be responsible for ensuring the requirements of this policy are followed and adhered to when using Hospital computer equipment.

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 Use is a standard (164.308 (b)) 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)).