GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-38	1 of 2

TITLE: DEVICE AND MEDIA CONTROLS POLICY

PURPOSE:

The purpose is to implement policies and procedures that govern the use, receipt and removal of hardware and electronic media that contain electronic protected health information (ePHI) into, within and out of the Guam Hospital Authority. 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, business associates such as payors, support contractors, and other associated healthcare providers. Further, the policy applies to all systems, network, applications, servers, and workstations as well as all facilities, which process, store or transmit ePHI.

POLICY:

Guam Memorial Hospital Authority will launch activities to ensure compliance with the Device and Media Controls standard and its associated implementation specifications of disposal, media re-use, accountability and data backup and storage.

Only authorized personnel will have access to ePHI. A backup copy of all ePHI and other critical software and applications will be stored in a secure location. A secure log will be maintained to document the request, release, copying, scanning and disposal of any ePHI or other sensitive information.

Removable data storage devices and media such as external backup devices, zip drives, flash drives, thumb drives, magnetic tapes, optical compact disks, floppy diskettes and the like are prohibited for use with ePHI without adequate safeguards in place. Exceptions can be considered under documented need and extenuating circumstances and with approval by the Hospital Administrator and the HIPAA Security Officer and Privacy 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 Device and Media Controls standard and its associated implementation specifications of disposal, media re-use, accountability and data backup and storage.

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

All workforce members, business associates such as payors, support contractors, and other associated healthcare providers will be responsible to comply with this policy.

COMPLIANCE:

Failure to comply with this or any other security policy may 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.

Device and Media Controls is a standard (164.310 (d)(1)) 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)).