


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-43	1 of 3
TITLE: ACCESS CONTROL POLICY				

PURPOSE:

The purpose is to implement technical policies and procedures for electronic information systems that maintain electronic protected health information (ePHI) to allow access only to those persons or software programs that have been granted access rights as specified by the HIPAA Security Rule. This is a standard required under the Technical 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, some third parties such as support contractors may be required to abide by parts of this policy if required by Guam Memorial Hospital Authority in a Business Associate Contract (BAC).

Further, the policy applies to all systems, network, and applications, as well as all facilities, which process, store or transmit ePHI.

POLICY:

- Guam Memorial Hospital Authority will control access to its information assets and systems. Only individuals that have been formally authorized to view or change sensitive information will be granted access to that information.
- Each individual that accesses sensitive information via computer at Guam Memorial Hospital Authority will be granted some form of unique user identification, such as a login ID. At no time will any workforce member allow anyone else to use their unique ID. Likewise, at no time will any workforce member use any other user's access ID and password.
- Guam Memorial Hospital Authority will establish an Emergency Access Procedure for gaining access to sensitive information during an emergency. Extraordinary care in safeguarding and documenting the use of the information will be exercised during this procedure.

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

- The fundamental principal of “need to know” will be applied within Guam Memorial Hospital Authority to determine access privileges. Access to sensitive information will be granted only if that individual has a legitimate business need for the information. Reasonable efforts will be made to limit the amount of information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.
- Where ever reasonable and appropriate, Guam Memorial Hospital Authority will establish role-based categories that identify types of information necessary for employees to do their jobs. Access to sensitive information will be granted based on these roles or functions that the individual performs within the organization.
- Guam Memorial Hospital Authority will maintain procedures for Automatic Logoff of systems that contain sensitive information after a period of inactivity. The length of time that a user is allowed to stay logged on while idle will depend on the sensitivity of the information that can be accessed from that computer and the relative security of the environment that the computer is located.
- Guam Memorial Hospital Authority will evaluate and implement encryption and decryption solutions as an additional form of access control, where deemed reasonable and appropriate. These solutions will be implemented when they are found to be:
 - Technically sound and useable
 - Financially reasonable

RESPONSIBILITIES:

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

- Ensuring no other individual uses their unique ID
- Never using another individual’s unique ID
- Abiding by the terms of this policy
- The Guam Memorial Hospital Authority HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for:
 - Ensuring workforce members have access to only the sensitive information they need to do their jobs
 - Creating and maintaining role-based access control based on the roles and functions workforce members perform in the organization
 - Ensuring each workforce member has a unique user ID for access systems that contain sensitive information
 - Maintaining Emergency Access Procedures
 - Maintaining Automatic Logoff Procedures
 - Evaluating and implementing (when reasonable appropriate) encryption and decryption solutions as a form of access control

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.

Access Control is a standard (164.312 (a)(1)) defined in the Technical Safeguards category of the HIPAA Security Rule.

PROCEDURES:

Procedures developed in support of the Access Control Policy include:

- Access Authorization Procedure
- Access Establishment and Modification Procedure
- Pass Management Procedure
- Access Control and Validation Procedures
- Emergency Access Procedure
- Automatic Logoff 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)).