


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

| APPROVED | RESPONSIBILITY | EFFECTIVE DATE | NUMBER | PAGE |
|---|---|-----------------------|---------------|-------------|
|  | Information Technology Administrator (HIPAA Security Officer) | 12/2004 | 6420-58 | 1 of 2 |
| TITLE: EMAIL SECURITY POLICY | | | | |

PURPOSE:

The purpose of this policy is to protect the confidentiality and integrity of sensitive information such as electronic protected health information (ePHI) that may be sent or received via email. This is a required standard 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 electronic protected health information (ePHI) by Guam Memorial Hospital Authority.

POLICY:

Guam Memorial Hospital Authority recognizes that using email without the use of an encryption mechanism is an insecure means of sending and receiving messages. Guam Memorial Hospital Authority will evaluate emerging encryption solutions for email and implement them when one is found that is:

- Technically sound
- Reasonable to implement and use by workforce members
- Financially reasonable

Until a workable encryption mechanism is implemented, Guam Memorial Hospital Authority will utilize the following guidelines regarding sending sensitive information via email:

- Emails containing sensitive information are permitted only when both the sender and receiver are members of Guam Memorial Hospital Authority's workforce and the e-mail stays within the confines of Guam Memorial Hospital Authority's local network. That is, both email addresses must end with "GMHA.org". When sending ePHI via email, care should be taken to send only the minimum necessary.
- Emails containing sensitive information may not be sent to any other person outside of Guam Memorial Hospital Authority's network.
- Emails being sent need to have the GMHA Email Disclaimer imbedded as a signature file in accordance with GMHA Policy 6100-29.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

Guam Memorial Hospital Authority provided e-mail systems are intended for official and authorized purposes only. E-mail messages are considered by Guam Memorial Hospital Authority to be company property. Therefore, e-mail equipment operated by or for Guam Memorial Hospital Authority staff are subject to the same restrictions on their use as any other company furnished resource provided for use by members of the workforce.

Electronic information about an individual, such as a client or a patient, in an organized set of records, should be protected to the extent that a hard copy record is protected, and disclosed only when required for authorized purposes.

E-mail system administrators and others with special system-level access privileges are prohibited from reading electronic messages of others unless authorized by appropriate Guam Memorial Hospital Authority management officials. However, Guam Memorial Hospital Authority officials will have access to e-mail messages whenever there is a legitimate purpose for such access, e.g., technical or administrative problems.

When e-mail is not in use, users are to exit the software to prevent unauthorized access.

RESPONSIBILITIES:

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

- Abide by the terms and guidelines set forth by this policy

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

- Evaluate, on a periodic basis, emerging encryption solutions for email and implementing them when one is found that meets the criteria described in the policy section of this document
- Maintaining procedures and forms in support of this policy
- Monitoring and enforcing workforce compliance with this policy

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.

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)).