


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-54	1 of 2
TITLE: ENCRYPTION POLICY				

PURPOSE:

The purpose is to implement a mechanism to encrypt electronic protected health information (ePHI) whenever deemed appropriate. This is a standard required under the Technical Safeguards of the HIPAA Security Rule

The Encryption Policy is intended to assist employees of Guam Memorial Hospital Authority when making decision about purchasing or developing software and other systems that make use of encryption technologies as a method of protecting "data in motion".

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. More specifically, this policy applies to employees of Guam Memorial Hospital Authority that have the authority to evaluate, purchase (or develop), and implement systems that store or process sensitive information.

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 protects "data in motion" by implementing a combination of solutions that may include Virtual Private Networks (VPNs), Secure Sockets Layer (SSL) and other technologies.

Guam Memorial Hospital Authority will identify systems that require ePHI to be encrypted for the purpose of transmission.

Guam Memorial Hospital Authority will identify members of the workforce who require encryption capabilities for transmission purposes.

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

Symmetric cryptosystem key lengths must be at least 128 bits.

Asymmetric crypto-system keys must be of a length that yields equivalent strength.

Guam Memorial Hospital Authority's key length requirements will be reviewed annually and upgraded as technology allows. All keys generated will be securely escrowed.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Security Officer.

Guam Memorial Hospital Authority will test encryption and decryption capabilities of products and systems to ensure proper functionality.

RESPONSIBILITIES:

All workforce members are responsible for:

- Understanding and following all security related policies and procedures

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

- Ensuring all workforce members understand and follow security related policies and procedures

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.

Encryption is an addressable implementation specification defined within the Transmission Security standard (164.312 (e)(1)) in the Technical Safeguards category of the HIPAA Security Rule.

PROCEDURES:

Procedures developed in support of the Encryption Policy include:

- Encryption and Decryption Procedure
- Transmission Security 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)).