


**GUAM MEMORIAL HOSPITAL AUTHORITY  
ADMINISTRATIVE MANUAL**

<b>APPROVED</b>	<b>RESPONSIBILITY</b>	<b>EFFECTIVE DATE</b>	<b>NUMBER</b>	<b>PAGE</b>
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-47	1 of 2
<b>TITLE: ENCRYPTION AND DECRYPTION POLICY</b>				

**PURPOSE:**

The purpose is to implement a mechanism to encrypt and decrypt electronic protected health information (ePHI). 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 the use of encryption technologies as a method of protecting data stored on systems that process ePHI.

**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 such as ePHI.

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 identify systems that require ePHI to be encrypted.

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

The Guam Memorial Hospital Authority will need to balance the challenge of protecting "data at rest" such as that defined in the Access Control standard of the HIPAA Security Rule against the increase in security technology complexity and administrative overhead including performance considerations and usability.

The Guam Memorial Hospital Authority will seriously review the viability of securing critical database, file servers as well as ePHI on mobile devices such as laptops and PDAs.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

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.

Symmetric cryptosystem key lengths must be at least 56 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 HIPAA Security Officer.

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

### **RESPONSIBILITIES:**

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, will be responsible for ensuring the implementation of the Encryption and Decryption 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.

Encryption and decryption is an addressable implementation specification defined within the Access Control standard (164.312 (a)(1)) in the Technical 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)).