


**GUAM MEMORIAL HOSPITAL AUTHORITY  
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-51	1 of 3
<b>TITLE: PERSON OR ENTITY AUTHENTICATION POLICY</b>				

**PURPOSE:**

The purpose is to implement procedures to verify that the person or entity seeking access to electronic protected health information (ePHI) is the one claimed. This is a standard required under the Technical Safeguards of the HIPAA Security Rule.

Authentication is the mechanism that verifies that an individual is who they claim to be. It is the first step in gaining access to any secured computing environment and is the basis for allowing or denying access to sensitive information. Authentication is based on one or more of the three following factors:

- Something that the person knows such as a password
- Something that the person has such as a smart card or token
- Something the person is such as a fingerprint.

This policy sets a minimum acceptable level of authentication for users or entities at Guam Memorial Hospital Authority.

**SCOPE:**

This policy applies to Guam Memorial Hospital Authority in its entirety, including all workforce members. 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 recognizes that the use of passwords as an authentication method is inherently insecure and intends to use strong authentication solutions for workforce members that have access to sensitive information where reasonable and appropriate. Strong authentication solutions use a combination of two or more factors (described above) when granting or denying access; such as the presence of a smart card (something you have) combined with a pin number (something you know).

Guam Memorial Hospital Authority will evaluate emerging strong authentication technologies on a periodic basis and implement them when one is found that is:

- Technically sound and useable
- Financially reasonable
- Meets business objectives

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

Guam Memorial Hospital Authority will give strong authentication preference to users that pose a higher risk to the organization. High risk users include (but are not limited to):

- Users that have administrator rights to systems that contain sensitive information
- Users that connect to the network remotely
- Users that have portable computing devices such as laptops or PDAs that may be carried off the premises

All workforce members that use passwords will make efforts to keep those passwords safe and secure. At no time will any workforce member:

- Write down their password, either on paper or in an electronic file
- Share or otherwise disclose their password to anyone else for any reason including technical support, managers, and supervisors.
- Keep the same password for longer than 90 days
- Use a password that is the same as or a variation of any password has been used before
- Use the "remember password" option on any program that supplies the password for the user
- Use a "weak" password as described below

Weak passwords will not be used at Guam Memorial Hospital Authority for any reason. Weak passwords have the following characteristics:

- It contains less than six characters
- It is a word found in a dictionary (English or foreign)
- It is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, and so on
  - Computer terms and names, commands, sites, companies, hardware, software
  - Birthdays and other personal information such as addresses and phone numbers
  - Word and/or number patters like aaabbb, qwerty, zyxwvuts, 123321, and so on
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (for example, secret1, 1secret)

If a password is suspected to have been compromised (or if anyone requests or demands a password), it shall be treated as a security incident and reported to the Security Officer.

#### **RESPONSIBILITIES:**

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

- Using, as instructed, any authentication method required by the HIPAA Security Officer
- Abiding by all requirements set forth for the protection of passwords at Guam Memorial Hospital Authority.

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

- Evaluating and implementing strong (two factor) authentication solutions when appropriate, while giving preference to high risk users as described above
- Ensuring the password administration options of all software packages are set to reflect the password requirements outlined above
- Monitoring compliance of the workforce to this policy and responding to any security incidents which may arise from it

**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.

Person or Entity Authentication is a standard (164.312 (d)) defined 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)).