


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/28/04	6420-3	1 of 4
TITLE: PASSWORD MANAGEMENT POLICY				

PURPOSE:

The purpose is to implement procedures for creating, changing and safeguarding passwords.

SCOPE:

This policy applies to Guam Memorial Hospital Authority in its entirety, including all workforce members and computer software business associates. Further, the policy applies to all computer systems, network, and applications that process, store or transmit electronic protected health information (ePHI).

POLICY:

The Guam Memorial Hospital Authority requires that:

- All passwords must be changed at least once every 180 days.
- All production system-level passwords must be part of the IT Administrator's (HIPAA Security Officer) administered global password management database.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where the Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system," and must be different from the passwords used to log in interactively. A keyed hash must be used where available (for example, SNMPv2).

Users must select strong passwords. Strong passwords have the following characteristics:

- Be at least six characters in length
- Be a mixture of letters and numbers
- Be changed at least every 180 days
- Be different from the previous 2 passwords
- Not contain 4 consecutive characters used from the previous password
- Not contain the user's User I.D.

Note that poor, weak passwords have the following characteristics:

- The password contains less than six characters
- The password is a word found in a dictionary (English or foreign)

Reviewed: 12/2004
Revised:
Approved: EMC 12/28/04

- The password 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 or number patterns 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)

Further, systems that authenticate must require passwords of users and must block access to accounts if more than three unsuccessful attempts are made.

Members of the workforce must strictly follow and adhere to these guidelines for passwords:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an e-mail message
- Don't talk about a password in front of others
- Don't hint at the format of a password, like, "my family name"
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers
- Don't reveal a password to business associates

If someone demands a password, refer them to this document or have them call the Information Technology (IT) Department or contact the HIPAA Security Officer.

Members of the workforce must not use the "Remember Password" feature of applications (Eudora, Outlook, Netscape Messenger, and so on).

Members of the workforce must not write down passwords and store them anywhere in your office. Further, passwords must not be stored on ANY computer system (including Palm Pilots or similar devices) without encryption.

RESPONSIBILITIES:

The IT Administrator (HIPAA Security Officer) is responsible for ensuring the implementation of the Password Management Policy.

Password cracking or guessing may be authorized to be performed on a periodic or random basis by the Security Officer. If a password is guessed or cracked during one of these scans, the user will be required to immediately change it.

Members of the workforce must not share their passwords with anyone, including administrative assistants or secretaries, unless otherwise justified and approved by the Hospital Administrator or the IT Administrator. All passwords are to be treated as sensitive, confidential information.

REMOTE ACCESS:

Access to the GMHA Network and Systems via remote access is to be controlled using both a one-time password authentication and a public/private key system with a strong passphrase. Only authorized users with very limited access will be given remote access to GMHA systems. Remote access usage will be closely monitored and logged on a daily basis.

COMPLIANCE:

Failure to comply with this policy or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws such as HIPAA.

Password Management is an addressable implementation specification defined within the Security Awareness and Training standard (164.308 (a)(5)) in the Administrative Safeguards category of the HIPAA Security Rule.

PROCEDURES:

The following are procedures for obtaining and activating authorized GMHA Staff and Business Associates with system access to include User ID and Password. Procedures for disabling and terminating authorized user system access are included.

I. GMHA STAFF:

- A. Department Head submits request to the Information Technology (IT) Department identifying and authorizing employee(s) to access what system and what application, and defining the job function and access limitations.
- B. Once activated, employee(s) will receive instructions from IT Department on how to change their passwords. Employee(s) should comply with this policy in the frequency of changing their Passwords.
- C. When employee(s) user account is not in use for more than 30 days, their account will be automatically disabled and suspended until they notify IT Department.
- D. When employee(s) terminate their employment and clear-out from the Hospital, IT Department will immediately remove the employee(s) user access account and password on their last day of work.

II. BUSINESS ASSOCIATE:

- A. As specified in the Business Associate (BA) Agreement, the authorized BA representative submits request to the IT Administrator identifying and authorizing BA employee(s) to access what system and what application, and defining the job function and access limitations.
- B. Once activated, BA employee(s) will receive instructions from IT Department on how to change their passwords. BA employee(s) should comply with this policy in the frequency of changing their Passwords.
- C. When BA employee(s) user account is not in use for more than 15 days, their account will be automatically disabled and suspended until they notify IT Department.
- D. When BA employee(s) terminate their employment with their company, the company should immediately notify the GMHA IT Department to remove the BA employee(s) user access account and password.
- E. When a member of the medical staff does not use his/her account for four months, his/her account be automatically disabled and suspended until he/she notifies IT Department.

III. GMHA IT DEPARTMENT:

- A. The IT Administrator reviews all requests for user access and approves or disapproves for assigning User ID and Password, and level of access limitations.

1. **If Approved:**

- a. Register User account based on the job function and limitations identified and authorized by requestor.
- b. Test User account to ensure access works as to authorized limitations and level of access.
- c. Inform Requestor when completed; inform User of their new User ID and Password and provide user with instructions on how to change their password.

2. **If Disapproved:**

- a. Notify Requestor on disapproval to include reasons why not approved.

B. IT Staff will perform periodic reviews of authorized users access to all systems at least twice annually.

C. IT Network Administrators will review the hardware firewall, software firewall, and web filtering logs on a daily basis as part of the network security procedures.

ENFORCEMENT:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any Business Associate found in violation with this policy will be immediately removed from accessing the GMHA system, and will be reported to his/her company's management.

-----Nothing Follows-----