Good Samaritan Health and Wellness Center

Policies and Procedures

Subject: Password Management Policy	Policy #: 4.9.3
Prepared by: Teri Craig	Revision #:
Approved by: Board of Directors	Effective Date: 4/22/2016

4.9.3 Password Management Policy

Purpose:
To protect Good Samaritan Health and Wellness Center (GSHWC) information assets from unauthorized access, use, disclosure, modification, and destruction by establishing a standard for creating, protecting and changing passwords. Passwords are an important aspect of computer security because they are the front line of protections for protecting against unauthorized access to protected information.

Policy:
In order to ensure that only authorized users are gaining access to GSHWC information assets, GSHWC workforce members are responsible for taking the appropriate steps to select and secure their passwords. These steps are outlined in the Standards and Guidelines section in this policy.

Procedure:
GSHWC is committed to the security of its electronic data. This data is stored on the e-Clinical Works EMR, Computer Rx pharmacy system, Med Services (previous EMR) and includes patient, and billing data as well as other types of data that must remain confidential in accordance with State and Federal laws. The first level of security to systems such as e-Clinical Works, that contain Protected Health Information (PHI), is the employee's login ID and its association with a unique password.

All GSHWC workforce members whose job role requires access to systems containing PHI will be assigned a unique individual ID and initial password after access authorization has been confirmed. Login IDs for departmental applications and systems will be requested by the team leaders or executive staff according to the department's login ID creation and maintenance procedures.

Once approved by the Executive Director, or Chief Financial Officer, login IDs to systems containing PHI will be created by IT, or the Chief Financial Officer and will adhere to GSHWC's published standards.

Removal of access to these systems will be initiated and acted upon promptly by the Executive Director, Chief Financial Officer, or Security Officer when it is determined to be no longer appropriate.

STANDARDS:

- Passwords must be six or more characters.
- Use at least 2 different character types: upper case, lower case, numerals, or keyboard symbols when possible.
- Use words that cannot be found in the dictionary and are not based on personal information (family names, pet names, birthdays, anniversaries, etc.)
- User IDs and passwords should never be the same. Do not use any variation of your user ID in the password.
- Don't use duplicate letters/numbers like aa1122bb.
- Individuals must use their own ID and password to access a system.
- Do not share your password with anyone.
- Posting passwords on systems that contain protected health information (PHI) on monitors or placing them where others can access them is prohibited.
- Passwords must be immediately changed if there is any possibility it was disclosed, regardless of whether or not it was intentional.
- When changing passwords, create one that has not been previously used.
- Passwords should be changed every 6 months.
- Keep your network password different from other passwords on external personal accounts.
- To prevent password guessing attacks, the number of consecutive unsuccessful logins must be limited to 5 attempts whenever possible. After 5 unsuccessful logins, the user login ID must be suspended until reset by the "Security Officer" or Chief Information Officer.

SUGGESTIONS FOR CREATING STRONG PASSWORDS:

- Use a mixture of upper case, lower case, special characters, and numbers when possible, e.g. Bcre8tive!
- Use several words or parts of a word together. If possible, substitute a number or special character for a letter, e.g. UrAGen$us.
- Choose a phrase from a favorite song or poem and use only the first letter of every word in the password. Substitute numbers or special characters for some letters. E.g. Mary had a little lamb whose fleece was white as snow:
  Mha11wfwwa$
- Invent phrases for a vanity plate, e.g. 2Fst4u

GUIDELINES:

- Treat all passwords as sensitive, confidential GSHWC information.
- Do not store passwords in a file on ANY computer system (including smart phones, tablets, or similar devices) without encryption.
- If one suspects an account or password has been compromised, report the incident to Compliance and change all passwords.

Implementation:

It is the responsibility of all employees/contractors/volunteers to read and acknowledge their obligations under this policy.