 <p style="text-align: center;">Heritage Provider Network & Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No.	Effective Date: 12/01/2002	Page - 1 -
	Authored by: Dave Pfafman	Date: 12/01/2002	Revised by: Dave Pfafman Date: 02/02/2015
	Approved by: Scott Bae	Date: 02/02/2015	
Title of Policy: Password Creation and Usage			

POLICY:

It is the policy of Heritage Provider Network and its Affiliated Groups (HPN) to establish a standard for the creation of strong passwords, the protection of password, and their frequency of change.

PURPOSE:


Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Heritage Provider Network's entire corporate network. As such, all Heritage Provider Network employees (including contractors and vendors with access to Heritage Provider Network systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. This policy establishes a standard for creation of strong passwords, the protection of passwords, and their frequency of change.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Heritage Provider Network facility, has access to the HPN network, or stores any non-public Heritage Provider Network information.

PROCEDURE:

1. All system-level passwords (e.g., root, enable, admin, application administration accounts (service accounts}, etc.) and all user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months; however, the recommended change interval is every three months.
2. Passwords must not be inserted into email messages or other forms of unencrypted electronic communication.
3. All user-level and system-level passwords must conform to the guidelines described below.
4. When setting up new accounts or if a password is forgotten, IS staff will set the account to a temporary password and the individual will be required to reset it at next login.
5. IS departments are specifically prohibited from maintaining a list of user passwords.

PROCEDURE (continued):

 <p>Heritage Provider Network & Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No.	Effective Date: 12/01/2002	Page - 2 -
	Authored by: Dave Pfafman	Date: 12/01/2002	Revised by: Dave Pfafman Date: 02/02/2015
	Approved by: Scott Bae	Date: 02/02/2015	
Title of Policy: Password Creation and Usage			


Guidelines

1. Passwords are used for various purposes at Heritage Provider Network. Some of the more common uses include: user level accounts, email accounts, EZCAP, Medic, voicemail or any other secure application. Everyone should be aware of how to select strong passwords.
2. Poor, weak passwords have the following characteristics:
 - a. The password contains less than eight characters
 - b. The password is a word found in a dictionary (English or foreign)
 - c. The password is a common usage word such as: names of family, pets, friends, co-workers, fantasy characters, etc.
 - d. Computer terms and names, commands, sites, companies, hardware, software.
 - e. The words with group abbreviations such as "HPN", "HDMG", "BFMC", "DOHC" or any derivation.
 - f. Birthdays, anniversaries and other personal information such as License #'s, addresses and phone numbers.
 - g. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - h. Any of the above spelled backwards.
3. Strong passwords have the following characteristics:
 - a. Contain both upper and lower case characters (e.g., a-z, A-Z)
 - b. Have digits and punctuation characters as well as letters e.g., 0-9,!@#\$\$%^&*()_+|~-=\ \{ \} [] : " ; ' < > ? , . /)
 - c. Are at least eight alphanumeric characters long.
 - d. Are not a word in any language, slang, dialect, jargon, etc.
 - e. Are not based on personal information, names of family, etc.
 - f. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

PROCEDURE (continued):

Password Protection Standards


 <p>Heritage Provider Network & Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No.	Effective Date: 12/01/2002	Page - 3 -
	Authored by: Dave Pfafman	Date: 12/01/2002	Revised by: Dave Pfafman Date: 02/02/2015
	Approved by: Scott Bae	Date: 02/02/2015	
Title of Policy: Password Creation and Usage			

1. Do not use the same password for Heritage Provider Network accounts as for other non-Heritage Provider Network access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Heritage Provider Network access needs. For example, select one password for the EZCAP systems and a separate password for the Medic system. Also, select a separate password to be used for an NT or an email account.
2. Do not share Heritage Provider Network passwords with **anyone, including administrative assistants or secretaries.** All passwords are to be treated as sensitive, confidential Heritage Provider Network information.
3. Here is a list of "don'ts":
 - a. Don't reveal a password over the phone to ANYONE
 - b. Don't reveal a password in an email message
 - c. Don't reveal a password to the boss
 - d. Don't reveal a password to a subordinate
 - e. Don't reveal passwords to MIS, If they need it, they will have you enter your password
 - f. Don't talk about a password in front of others
 - g. Don't hint at the format of a password (e.g., "my family name")
 - h. Don't reveal a password on questionnaires or security forms
 - i. Don't share a password with family members
 - j. Don't reveal a password to co-workers ever, even while on vacation
 - k. Don't use your network or EZCAP password to log on to external internet websites (always have a separate password for logging on to external websites)
4. If someone demands a password, refer them to this document or have them call someone in the Information Systems Department.

Do not use the "Remember Password" feature (e.g., windows desktop, OutLook, Internet Explorer or Netscape).

PROCEDURE (continued):

5. Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

 <p style="text-align: center;">Heritage Provider Network & Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No.	Effective Date: 12/01/2002	Page - 4 -
	Authored by: Dave Pfafman	Date: 12/01/2002	Revised by: Dave Pfafman Date: 02/02/2015
	Approved by: Scott Bae	Date: 02/02/2015	
Title of Policy: Password Creation and Usage			

Change passwords at least once every six months. The recommended change interval is every three months.

6. If an account or password is suspected to have been compromised, report the incident to the IS department and change all passwords.
7. Password cracking may be performed on a random basis by “Heritage Provider Network” or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Enforcement

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