Network passwords – How to create a strong password

This document provides general information about password requirements and how to go about creating a strong password.

What is a strong password?

A strong password is the first line of defense in protecting ePHI and the overall health and security of Legacy's computer systems.

The strength of a password is a function of length, complexity (use of varied characters), and unpredictability. Passwords that are "strong' are very resistant being breached by others through guessing or more sinister attacks.

Use of strong passwords is Legacy policy. All new passwords must meet Legacy security requirements for configuration and complexity.

- Minimum of eight (8) characters.
- Must contain ALL of the following:
  - At least one lower-case letter (a-z)
  - At least one upper-case letter (A-Z)
  - At least one number (0-9).
  - At least one special character (punctuation or symbols.)
- Should not include words found in a dictionary (English or foreign)
- May not include names, birth dates, SSNs, pet's names, etc.

How do I create a strong password?

There are many approaches to creating a strong password. To help you get started, here's a sample methodology for designing a strong password. (Be careful not to use the exact suggestions from this document!)

1. Think of something such as thing, place or phrase that has some kind of personal meaning to you but is not something that would be easily known or guessed by others.

   Examples: Avocados
   Venezuela
   Made in Oregon

2. Identify some techniques to strengthen the word(s) you chose. Here are some examples to give you the idea:

    - Substitute letters with numbers. For example, replace each letter O with a zero or each letter E with a number 3.
    - Substitute letters with special characters. For example, change each letter T to a + or each letter S to a $.
    - Substitute spaces with a special character such as %.
    - Add punctuation.
    - Mix up capital letters and lowercase letters

3. Apply the selected techniques to your chosen password or passphrase.

    Examples: Av0cad0$
    Ven3zu3la!
    Mad3%In%Or3gon

4. Verify that your new password meets requirements for strength.

    - Does it have at least eight characters?
    - Does it include at least one upper-case letter, one lower-case letter, one number and one symbol?
    - Does it include any words found in a dictionary (English or foreign)?
    - Does it include any names, birth dates, SSNs, pet's names, etc.?

The final result must:

1. Be at least 8 characters long. (Longer is even more secure!)
2. Include at least one capital letter, one number, and one special character (punctuation.)
3. Not include any words that can be found in the dictionary.
4. Not be the same as any of the past twelve passwords used.

Some tips for helping to keep your password(s) safe:

- Create unique password every time you create a new account. Never keep the same password for more than one use. It is very tempting to create one password to use for all the systems you log in to, but try to avoid this temptation and keep unique passwords for all your accounts.
- Change passwords for all your accounts regularly. Schedule a recurring appointment on your calendar to remind you.
- Don't share with anyone. Anyone includes your friends and family.
- Never write down passwords. Creating a very strong password and writing it down on a paper is as bad as creating an easy to remember weak password and not writing it down anywhere.
- Don't type your password when someone is looking over your shoulder. This is especially very important if you type slowly and search for the letters in the keyboard and type with one finger, as it is very easy for someone looking over your shoulder to figure out the password.
- Never send your password to anybody in an email. Legitimate website or organization will ***never*** ask you for your user name and password either via email or over telephone.
- Change password immediately when it either has or may have been compromised. Even if you have the slightest doubt that someone might have stolen your password, change it immediately. Don't even waste a minute.
- Be careful typing your password into computers that are not assigned to you. Be sure to uncheck "Remember Me" and similar checkboxes.