Creating and Maintaining Strong Passwords

Last Modified on 05/23/2019 12:19 pm EDT

Version 14.19

Overview

It is critical that Practices adopt and maintain policies and procedures for protecting Practice data and patient-related data. This begins with using Strong Passwords. Not only is this a requirement for protecting PHI and to maintain compliance with HIPAA guidelines, it is also a sound business practice. This article discusses the recommendations that OP provides to all of our Practices to help them create and maintain Strong Passwords. A Strong Password is one that is constructed in such a way as to make it as difficult as possible for anyone who is not supposed to have access to a password to figure out what the password is.

Protecting the passwords in your Practice involves two critical considerations:

- Creating strong passwords.
- Maintaining strong passwords by adopting and maintaining Strong Passwords policies.

Creating Strong Passwords

OP recommends the following guidelines for creating a Strong Password for each member of your staff:

Do:

- **Enforce Minimal Length:** In general, the longer the password, the stronger it is. OP recommends that passwords have a minimum of eight of characters.
- **Use a Variety of Character Types:** OP recommends that each password include at least one alphabetic, numeric, and special (for example, !@#? character.
- **Use Upper and Lower Case** OP recommends that each password include a variety of upper- and lower-case characters. Use of upper- and lower-case characters does not need to follow standard grammar rules. Using upper- and lower-case characters where they do not occur grammatically actually helps to build Strong Passwords.
- **Use Phrases**: OP also recommends the use of phrases. In general, phrases (especially longer phrases) with a variety of characters and upper- and lower-case letters are more difficult to

figure out than single words or even a string of random characters.

Do Not:

- **Use Personal Information**: OP strongly recommends**against** using any type of personal information (such as staff names, family names, birth dates, residential streets, or pet names) no matter how remotely related to the staff member that information may be.
- **Use Easily Identifiable Information**: OP strongly recommends**against** using any type of information that can be easily guessed (such as the Practice name, address, phone number, or the extension or titles of staff member).

Policies for Maintaining Strong Passwords

OP recommends the following policies for maintaining Strong Passwords for your Practice:

- Prohibit staff from writing down passwords either on paper (regardless of how safely they believe they are hiding it) or in files on workstations (even if stored in a password-protected file).
- Never allow staff to share IDs or passwords with anyone.
- Do not allow staff to leave their logged-on workstation unattended. Not only is this a violation of HIPAA policy, it could allow others to access or change passwords.
- Do not allow staff to log on to a workstation and then allow others to use that station with their logon. Not only is this a violation of HIPAA policy, it could allow others to access or change passwords.
- HIPAA requires covered entities to provide periodic privacy and security reminders to their office staff, so use this time to remind employees to change passwords.
- Set a policy to change passwords often. OP recommends changing passwords monthly. Please review the **Adding, Modifying Passwords** article for details.
- Enable the Strong Passwords feature in OP 14. Please review the**Enabling Strong Passwords** article for details.

Version 14.10

Overview

It is critical that Practices adopt and maintain policies and procedures for protecting Practice data and patient-related data. This begins with using Strong Passwords. Not only is this a requirement for protecting PHI and to maintain compliance with HIPAA guidelines, it is also a sound business practice. This article discusses the recommendations that OP provides to all of our Practices to help them create and maintain Strong Passwords. A Strong Password is one that is constructed in such a way as to make it as difficult as possible for anyone who is not supposed to have access to a

password to figure out what the password is.

Protecting the passwords in your Practice involves two critical considerations:

- Creating strong passwords.
- Maintaining strong passwords by adopting and maintaining Strong Passwords policies.

Creating Strong Passwords

OP recommends the following guidelines for creating a Strong Password for each member of your staff:

Do:

- **Enforce Minimal Length:** In general, the longer the password, the stronger it is. OP recommends that passwords have a minimum of eight of characters.
- **Use a Variety of Character Types:** OP recommends that each password include at least one alphabetic, numeric, and special (for example, !@#? character.
- **Use Upper and Lower Case** OP recommends that each password include a variety of upper- and lower-case characters. Use of upper- and lower-case characters does not need to follow standard grammar rules. Using upper- and lower-case characters where they do not occur grammatically actually helps to build Strong Passwords.
- **Use Phrases**: OP also recommends the use of phrases. In general, phrases (especially longer phrases) with a variety of characters and upper- and lower-case letters are more difficult to figure out than single words or even a string of random characters.

Do Not:

- **Use Personal Information**: OP strongly recommends**against** using any type of personal information (such as staff names, family names, birth dates, residential streets, or pet names) no matter how remotely related to the staff member that information may be.
- **Use Easily Identifiable Information**: OP strongly recommends**against** using any type of information that can be easily guessed (such as the Practice name, address, phone number, or the extension or titles of staff member).

Policies for Maintaining Strong Passwords

OP recommends the following policies for maintaining Strong Passwords for your Practice:

- Prohibit staff from writing down passwords either on paper (regardless of how safely they believe they are hiding it) or in files on workstations (even if stored in a password-protected

file).

- Never allow staff to share IDs or passwords with anyone.
- Do not allow staff to leave their logged-on workstation unattended. Not only is this a violation of HIPAA policy, it could allow others to access or change passwords.
- Do not allow staff to log on to a workstation and then allow others to use that station with their logon. Not only is this a violation of HIPAA policy, it could allow others to access or change passwords.
- HIPAA requires covered entities to provide periodic privacy and security reminders to their office staff, so use this time to remind employees to change passwords.
- Set a policy to change passwords often. OP recommends changing passwords monthly. Please review the **Adding, Modifying Passwords** article for details.
- Enable the Strong Passwords feature in OP 14. Please review the **Enabling Strong Passwords** article for details.