Policy: Password Guidelines

Policy Details

Creation Date: _____ Revision Date:_____

Applies to: All Employees and Contractors

Approved by:

Purpose

To ensure that privacy and security of our computer systems are maintained by using strong password standards.

Scope

1. All clinic electronic information system users are assigned a unique identifier (user ID) that restricts access to systems that may contain sensitive personal information and health information required for the employee to carry out their job duties (e.g., windows login).
    a. Access to electronic systems are password protected.
    b. Access to phone voicemail is password protected.
    c. Access to iPhone/tablets devices are password protected.
    d. Access to the wireless network is password protected.
2. All remote access sessions are password protected.
3. All clinic user-level passwords must be changed every 90 days.
4. All system-level passwords (e.g., Windows Administrator, application administration accounts, etc.) must be changed on at least an annual basis.
5. All clinic-issued mobile devices must be password protected with a minimum six digit PIN.
6. All clinic employees must follow appropriate use guidelines including
    a. Passwords are to be kept confidential at all times and should not be written down or posted publicly or shared with other staff except for security purposes. Do not reveal a password in email, chat, or other electronic communication.
    b. Do not reveal a password on questionnaires or security forms.
    c. Always decline the use of the "remember password" feature of applications (e.g., Outlook, internet browsers, etc.).
    d. If an account or password compromise is suspected, report the incident to your manager or clinic lead physician immediately and follow the breach management policy.

7. All monitors used to display identifying health information will time out after a short period of inactivity and require the entry of a password to reactivate the screen.
    a. Selected time-out periods must reflect the level of risk of exposure of workstations (set to lock after one hour of inactivity for local computers and 30 minutes for remote access sessions)

Passwords must be:

- Minimum length of 8 characters
- Cannot contain user's name
- Must contain an alpha-upper case, alpha-lower case, numeric, special character
- Only valid for 90 days
- New passwords must be unique (e.g. never used before)
- Maximum of 5 invalid attempts before account lockout

Suggestions:

- It is strongly suggested to use long passphrases (up to 64 characters with no spaces)
- All users with administration privileges should enable multi-factor authentication

Group	Example
Lowercase letters	a, b, c, ...
Uppercase letters	A, B, C, ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Non-alphanumeric (symbols)	( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /