HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

PASSWORD MANAGEMENT GUIDE

Summary

This guide helps private practice clinics in the implementation of effective practices for password management. Privacy Officers can adopt this guide and attached *Password Management Checklist* for their clinics. It provides minimum requirements for proper password management and can be adopted by clinics as training and monitoring tool.

Why Clinics Need a Password Management System

Adequate and documented password practices allow clinics to ensure staff is clear on their responsibilities. Accurate audit trails documenting what records have been accessed by whom will assist clinics in investigation and prevention of possible issues or security threats. Should the privacy breach occur, due diligence will protect clinic's reputation.

Guiding Principles

1. All clinical information systems must require secure authentication methods such as log in and password, token (e.g. for remote EMR access), or electronic certificate allowing to exchange digital information.

2. Passwords must be sufficient and strong:

    a. unique (not used in any other situations),

    b. kept strictly confidential and never shared between individual users,

    c. adhering to policies of the organizations granting access to their clinical information systems or provincial patient record viewers (eHealth viewers such as CareConnect or Uniform Clinical Information known as UCI),

    d. exceeding minimum complexity recommendations: see *Password Management Checklist* attached to this guide.

3. All users at the clinic should be trained on password management practices and aware of their responsibilities for the protection of their passwords to ensure unauthorized access is not allowed.

4. Individual users who are provided with an account to any computer or information system at the clinic are responsible for the managing of their own passwords.

5. When logging in to a computer or information system for the first time, individuals should create a new and unique password immediately to ensure confidentiality.

6. Software or hardware technology solutions may be used to help manage passwords and provide additional security authentication if appropriate. Examples include password manager software, multi-factor authentication services.

Related Materials

Physician Office IT Security Guide	User-friendly guide focusing on key safeguards for private practices to ensure their compliance with regulatory requirements. Concise (35 pages) reference for technical terminology and concepts.

DISCLAIMER

This document provides general guides and approaches only. We strongly recommend that you retain a knowledgeable and qualified IT professional to regularly assess and maintain your clinic's technology.

For more information, guidance, or support contact:

Doctors Technology Office
604 638-5841
DTOinfo@doctorsofbc.ca
www.doctorsofbc.ca/doctors-technology-office

Checklist for Implementing Password Management

- ☐ Passwords are secure, never shared, or posted to be visible to others.
- ☐ If passwords are digitally stored, they must be protected with a strong master password or multi-factor authentication where possible.
- ☐ Passwords are set to expire every ____ months.*
- ☐ Passwords are unique. The same or similar passwords are not re-used or used on different accounts.
- ☐ Password do not include dictionary words or identifiable terms such as a name or clinic address.
- ☐ Passwords include a minimum of 9 characters which are a combination of uppercase characters, lowercase characters, numerals, and symbols (! $ # %).
- ☐ Temporary passwords meet minimum password complexity and are changed upon first login.
- ☐ Clinic staff completes is educated about the password management practice and aware of their responsibilities.

Note: Password expiry time frames and complexity requirements should align with any external clinical access agreements in place such as for Physician's Private Network (PPN) or CareConnect access.