HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

TECHNICAL BULLETIN - PASSWORD MANAGEMENT SOLUTIONS

This document is intended as a brief introduction and informational bulletin on **password management solutions** for clinic IT staff, vendors, or self-supporting physicians with IT experience.

How Password Managers Work

Password management software provides a place where you can securely store your individual digital credentials under one single login. A strong "master" password, often secured additionally with a **multi-factor authentication method (MFA)**, is used to store and access all of your other passwords and login information.

There are generally two main types of password manager, online and offline. Online password managers are software that provide service from a cloud and require a subscription (free or paid). The security encryption standard expected for all online connections from a password manager is AES 256. Offline password managers may be free and store encrypted credentials on your local system instead of in the cloud.

Choosing a Password Manager

Choosing which password manager software to use at a clinic is largely a personal preference and business requirement specific choice. The major vendors offer industry standard security methods and so the main factors in selecting one is based on desired features and preference for the general look and feel (or ease of use) of the application. Most offer a free or trial service option and it is recommended to test out a few options before making your final decision.

Password management software typically offers several related features beyond basic password and credential management including: password generation, user vaults, sharing, file storage, MFA/SSO/VPN integrations, credit/dark web/identify theft monitoring and insurance. These features will vary from vendor to vendor and you may begin to learn more about each from the individual vendor websites (see examples below).

Password Management Solution Examples

Below are a few examples of common password management software vendors available. While DTO does not endorse any particular vendor, reviewing these options below can provide some understanding of the products and features available from popular password managers:

- **LastPass:** https://www.lastpass.com/
- **Dashlane:** https://www.dashlane.com/
- **1Password:** https://1password.com/
- **Enpass:** https://www.enpass.io/

DTO Resources

DTO Technical Centre	Doctors Technology Office (DTO) resources including a knowledge-sharing community for clinic IT support and other resources to educate and share best practices related technical challenges experienced by clinics.
Physician Office IT Security Guide	Doctors Technology Office (DTO) guide detailing best practices for clinic privacy and security based on requirements and information from the Personal Information Protection Act (PIPA), College of Physicians and Surgeons of BC, and the Office of the Information and Privacy Commissioner for British Columbia (OIPC).

DISCLAIMER

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

For more information, guidance, or support please contact:

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