HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

TECHNICAL BULLETIN - MULTI-FACTOR AUTHENTICATION

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

What is Multi-factor Authentication?

Multi-factor authentication (MFA), also including **2-factor authentication (2FA),** is a method in which access to a system is only granted when two or more pieces of evidence (factors/credentials) are provided and successfully verified. The credentials must be from different types of factors: something you know (eg. password or pin), something you are (eg. fingerprint), or something you have (token or code from MFA app). Common examples are remote access tokens that generate a one-time code that you use in combination with your own set password to log in or a using bank card and associated PIN code.

MFA is an important method to use for clinics to appropriately secure staff accounts that have access to patient information. It can be used to create a powerful layer of extra security for computer / workstation logins, mobile devices access, online services such as Gmail or Microsoft Office and more. While accounts secured with MFA may still be vulnerable to some types of cyberattacks, the use of MFA will drastically reduce the risk that would otherwise be present when just using a strong password alone.

Using MFA at a Clinic

It is recommended to use multi-factor authentication (MFA) whenever you have an account that accesses personal health information or other sensitive data. Access to clinic workstations, mobile devices, email, EMR or other health portals are some prime examples of areas that should be considered for MFA protections.

Choosing an MFA Solution

A big challenge to using MFA is that different services and products use or support different MFA solutions. One strategy to deal with this is to prioritize which systems in your clinic are the most sensitive and apply MFA solutions appropriate to those services first.

Using an MFA solution from a mobile device, while having its advantages and disadvantages from a security standpoint, is generally the most convenient platform to use. Hardware tokens are also common and can work similar to the MFA mobile apps with One-time password generation (OTP). They can also work more like a physical key that gets plugged in or swiped instead of manually entering a generated code and supports some level of single-sign on ability (SSO).

Some electronic medical record (EMR) vendors support MFA for logging in. Check with your vendor directly to confirm if they support this feature and/or recommend any specific MFA solutions to use. This can be a good starting point in determining if a single MFA solution can be used for all sensitive logins at the clinic. Working with both the EMR vendor and qualified IT support will help ensure a good choice of solution is made and a smooth transition to using MFA security can occur at the clinic.

MFA Solution Examples

Below are some examples of common MFA solutions available. While DTO does not endorse any particular vendor, reviewing these options below can provide some understanding of the products and features available for securing your accounts with multi-factor authentication:

- **Google 2-Step Verification:** How to add 2-step verification to your Google account.
  https://www.google.ca/landing/2step/index.html
- **Microsoft 2-Step Verification:** How to add 2-step verification to your Microsoft account.
  https://support.microsoft.com/en-ca/help/12408/microsoft-account-how-to-use-two-step-verification
- **Authy:** A popular MFA application with multiple device support.
  https://authy.com/
- **Yubico's Yubikey:** Hardware token, 2-factor / passwordless authentication.
  https://www.yubico.com/

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).

Related Materials

National Institute of Standards and Technology (NIST) - Trusted Identities Group (TIG) Blog Post
Back to basics: Multi-factor authentication (MFA)
https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication

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