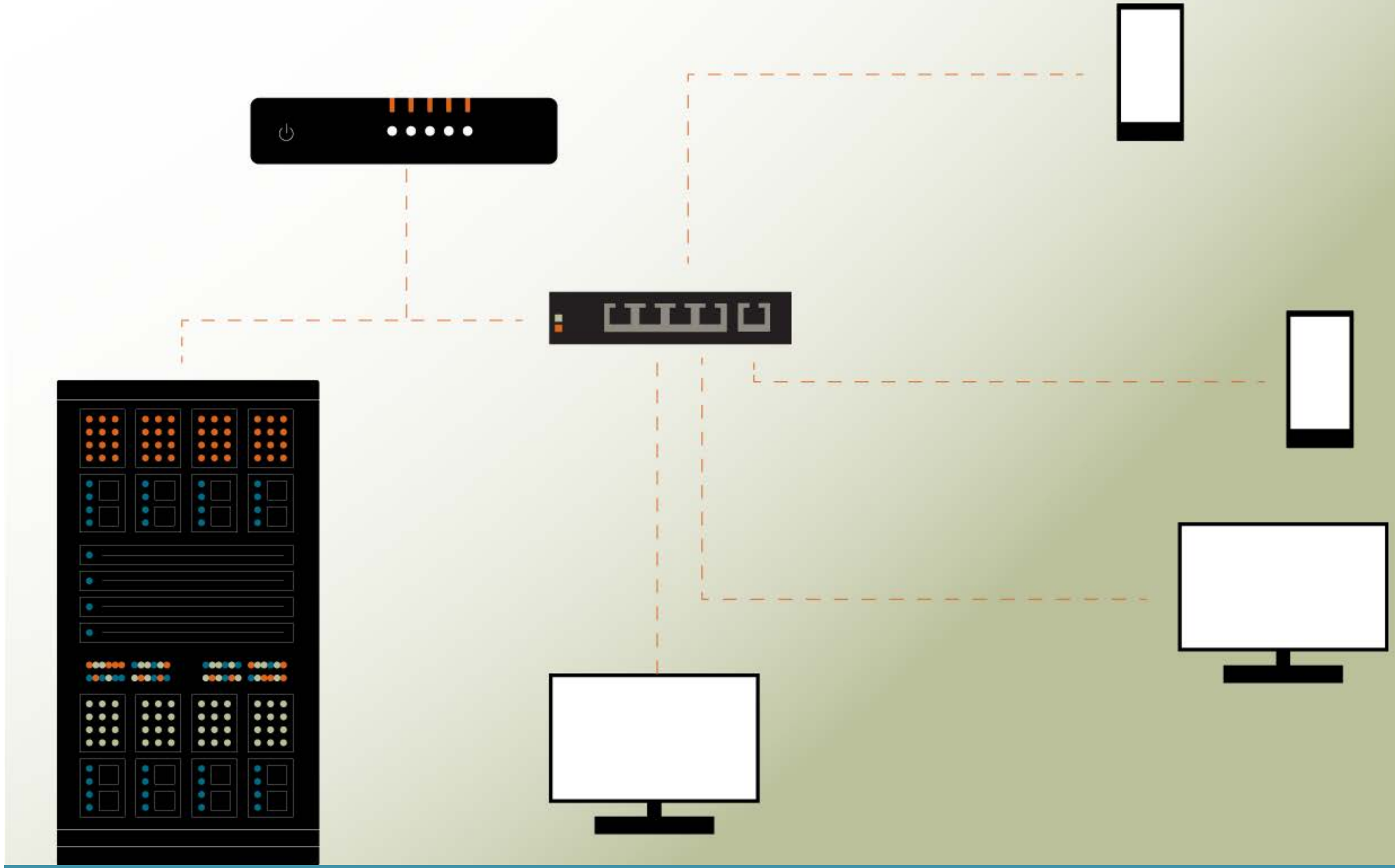
DTO Doctors Technology Office

A GPSC initiative



CLINIC IT SUPPORT COMMUNITY

GPSC

General Practice Services Committee

OVERVIEW

Topic: Clinic Security Overview (Checklist Review)

Speakers: Jesse Zacharias, Health Technology Consultant, DTO
Ralph Buschner, Senior IT Analyst, DTO
Ram Kodali, IMITS Information Security, PHSA
Naomi Monaster, Clinical Lead, eHealth Projects, IMITS, PHSA

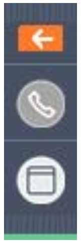
Agenda: 05 min – Introductions and Housekeeping
05 min – Clinic Security Overview
05 min – Provincial eHealth Viewer (CareConnect)
05 min – Declaration and Acknowledgements
40 min – Review of Security Checklist w/ Q&A

HOUSEKEEPING:

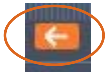
Control Panel:

By default the control panel is set to auto-hide.

If it disappears, check the top, right-hand corner of your screen for the minimized control panel. →



Click on the orange arrow to expand to control panel. →



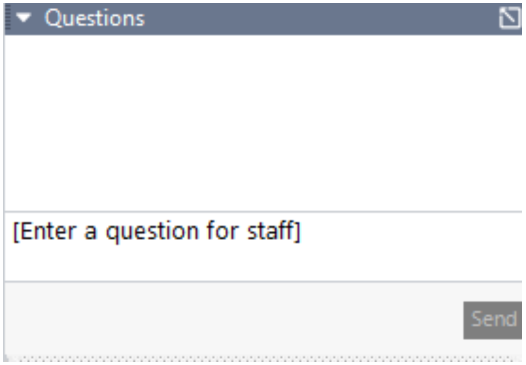
Mute:

By default, you will be put on Mute when you join the Webinar.

Questions:

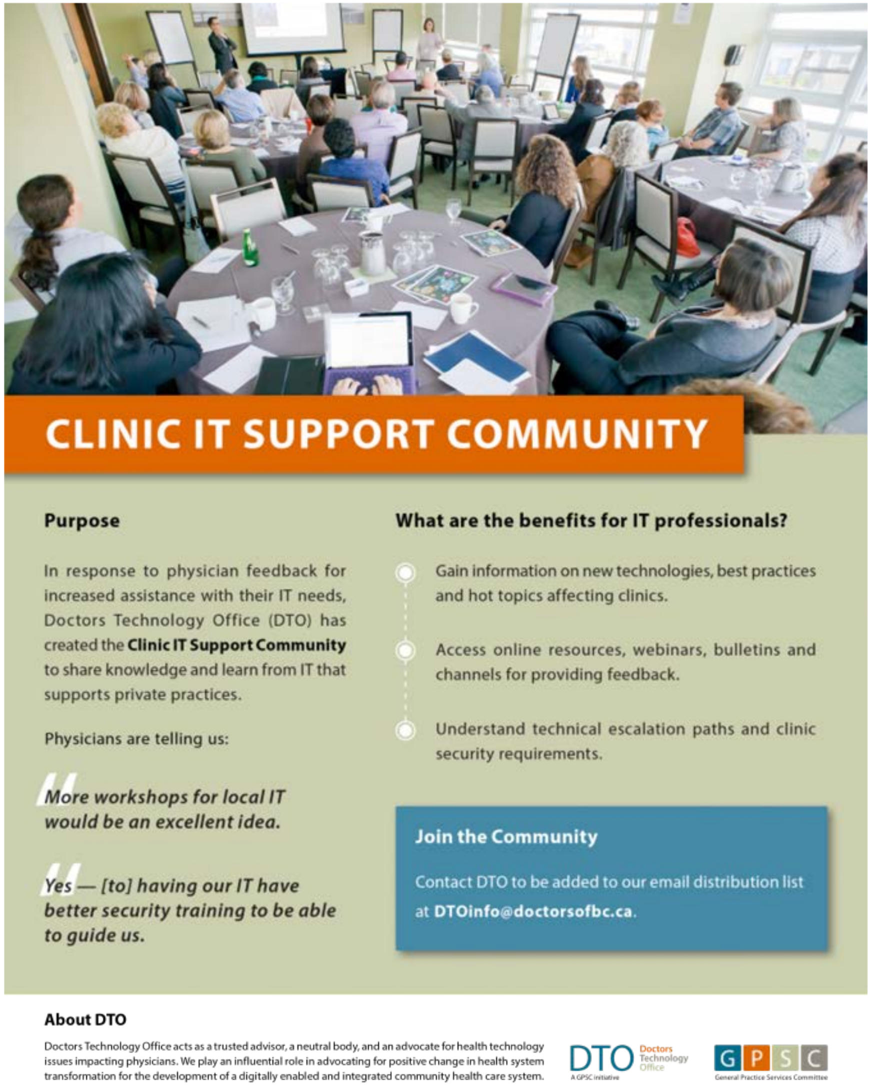
The question box feature is found at the bottom of the GoTo Webinar control panel.

If you have a question or comment, please write in the question box. →



Your question will automatically go to the presenters.

CLINIC IT SUPPORT COMMUNITY



CLINIC IT SUPPORT COMMUNITY

Purpose

In response to physician feedback for increased assistance with their IT needs, Doctors Technology Office (DTO) has created the **Clinic IT Support Community** to share knowledge and learn from IT that supports private practices.

Physicians are telling us:

> *More workshops for local IT would be an excellent idea.*

> *Yes — [to] having our IT have better security training to be able to guide us.*

What are the benefits for IT professionals?

- Gain information on new technologies, best practices and hot topics affecting clinics.
- Access online resources, webinars, bulletins and channels for providing feedback.
- Understand technical escalation paths and clinic security requirements.

Join the Community

Contact DTO to be added to our email distribution list at **DTOinfo@doctorsofbc.ca**.

About DTO

Doctors Technology Office acts as a trusted advisor, a neutral body, and an advocate for health technology issues impacting physicians. We play an influential role in advocating for positive change in health system transformation for the development of a digitally enabled and integrated community health care system.

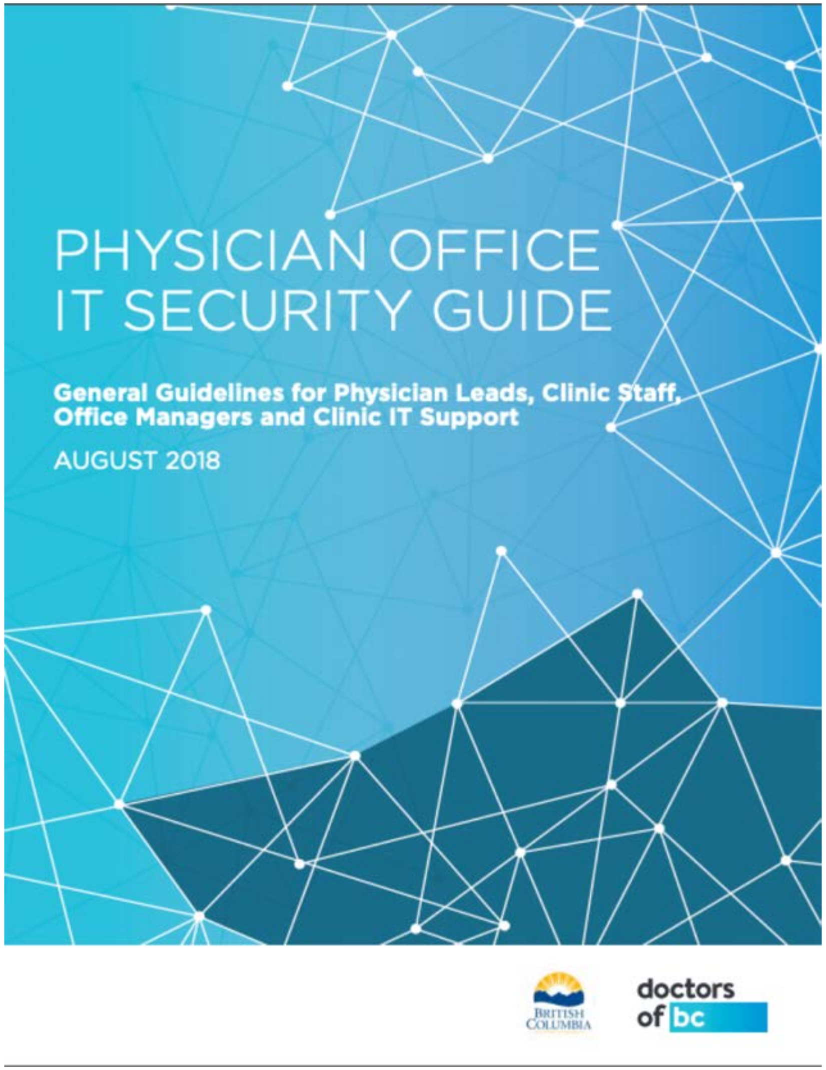
CLINIC SECURITY OVERVIEW

- Provincial Requirements
  - PIPA - Personal Information Protection Act
  - PIPEDA – Personal Information Protection and Electronic Documents Act
  - FIPPA – Freedom of Information and Protection of Privacy Act

- Public vs Private Organizations
  - PIPA – Private, Provincial
  - PIPEDA – Public, Federal
  - FIPPA – Public, Provincial

- Preparing for the Future
  - New technology and threats require healthcare to adapt
  - Alignment of privacy and security requirements expected

PHYSICIAN OFFICE IT SECURITY GUIDE



PHYSICIAN OFFICE
IT SECURITY GUIDE

General Guidelines for Physician Leads, Clinic Staff, Office Managers and Clinic IT Support

AUGUST 2018

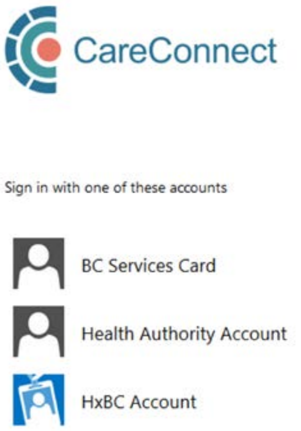
BRITISH COLUMBIA

doctors of bc

PROVINCIAL EHEALTH VIEWER

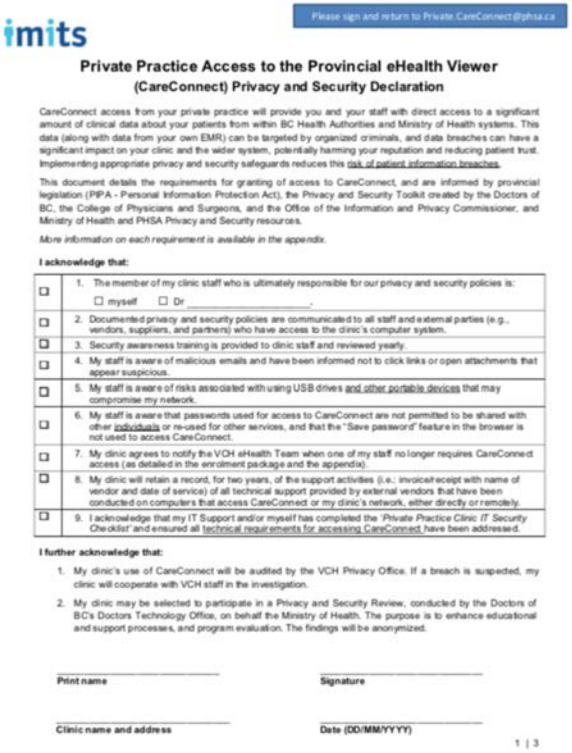
CareConnect is the Provincial eHealth Viewer for B.C.

- A secure, read-only Electronic Health Record (EHR) that delivers patient-centric information to support healthcare providers in their delivery of patient care
- Each Health Authority is responsible for the information that is sent to CareConnect (e.g, ADT information, Encounters, Documents)
- Ministry of Health is responsible for provincial information that is sent from health information banks (e.g., PLIS, Pharmanet)



Sign in with one of these accounts

CARECONNECT AGREEMENT



Please sign and return to Private.CareConnect@phsa.ca

Private Practice Access to the Provincial eHealth Viewer (CareConnect) Privacy and Security Declaration

CareConnect access from your private practice will provide you and your staff with direct access to a significant amount of clinical data about your patients from within BC Health Authorities and Ministry of Health systems. This data (along with data from your own EMR) can be targeted by organized criminals, and data breaches can have a significant impact on your clinic and the wider system, potentially harming your reputation and reducing patient trust. Implementing appropriate privacy and security safeguards reduces this risk of patient information breaches.

This document details the requirements for granting of access to CareConnect, and are informed by provincial legislation (PIPA - Personal Information Protection Act), the Privacy and Security Toolkit created by the Doctors of BC, the College of Physicians and Surgeons, and the Office of the Information and Privacy Commissioner, and Ministry of Health and PHSA Privacy and Security resources.

More information on each requirement is available in the appendix.

I acknowledge that:

☐	1. The member of my clinic staff who is ultimately responsible for our privacy and security policies is: ☐ myself ☐ Dr ____________________.
☐	2. Documented privacy and security policies are communicated to all staff and external parties (e.g., vendors, suppliers, and partners) who have access to the clinic's computer system.
☐	3. Security awareness training is provided to clinic staff and reviewed yearly.
☐	4. My staff is aware of malicious emails and have been informed not to click links or open attachments that appear suspicious.
☐	5. My staff is aware of risks associated with using USB drives and other portable devices that may compromise my network.
☐	6. My staff is aware that passwords used for access to CareConnect are not permitted to be shared with other individuals or re-used for other services, and that the "Save password" feature in the browser is not used to access CareConnect.
☐	7. My clinic agrees to notify the VCH eHealth Team when one of my staff no longer requires CareConnect access (as detailed in the enrolment package and the appendix).
☐	8. My clinic will retain a record, for two years, of the support activities (i.e.: invoice/receipt with name of vendor and date of service) of all technical support provided by external vendors that have been conducted on computers that access CareConnect or my clinic's network, either directly or remotely.
☐	9. I acknowledge that my IT Support and/or myself has completed the *'Private Practice Clinic IT Security Checklist'* and ensured all technical requirements for accessing CareConnect have been addressed.

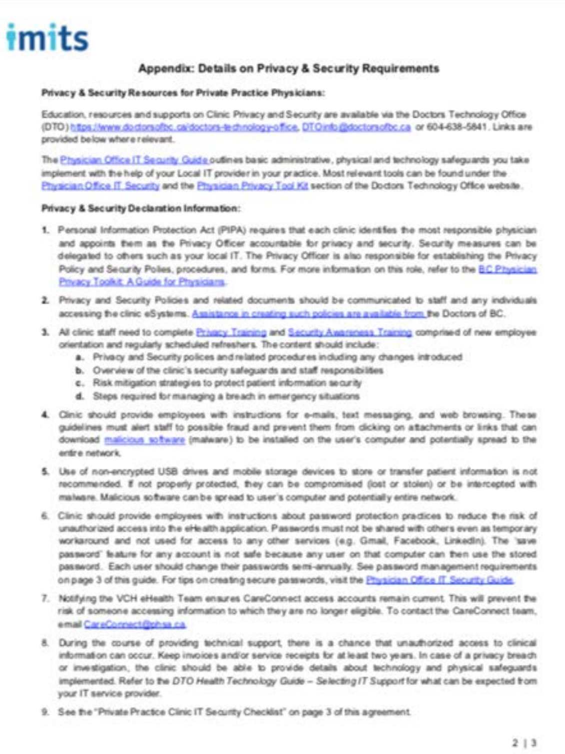
I further acknowledge that:

1. My clinic's use of CareConnect will be audited by the VCH Privacy Office. If a breach is suspected, my clinic will cooperate with VCH staff in the investigation.
2. My clinic may be selected to participate in a Privacy and Security Review, conducted by the Doctors of BC's Doctors Technology Office, on behalf the Ministry of Health. The purpose is to enhance educational and support processes, and program evaluation. The findings will be anonymized.

______________________ ______________________
Print name **Signature**

______________________ ______________________
Clinic name and address **Date (DD/MM/YYYY)**

1 | 3



Appendix: Details on Privacy & Security Requirements

Privacy & Security Resources for Private Practice Physicians:

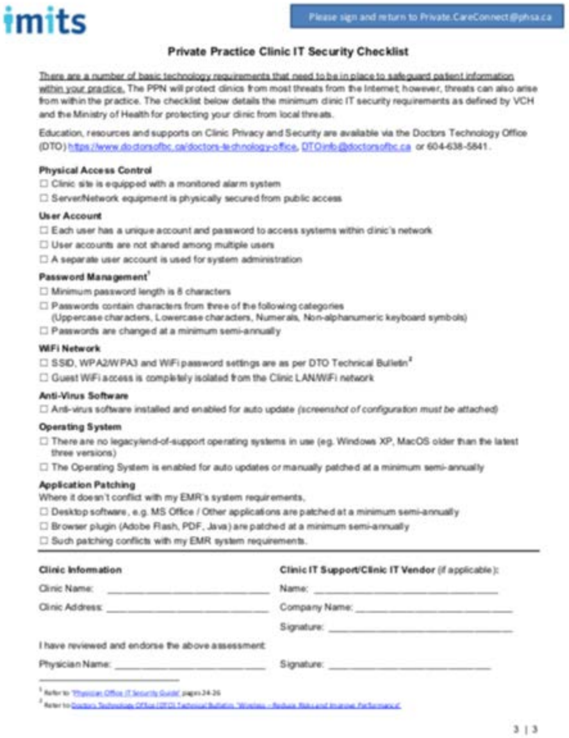
Education, resources and supports on Clinic Privacy and Security are available via the Doctors Technology Office (DTO) https://www.doctorsofbc.ca/doctors-technology-office, DTOinfo@doctorsofbc.ca or 604-638-5841. Links are provided below where relevant.

The Physician Office IT Security Guide outlines basic administrative, physical and technology safeguards you take implement with the help of your Local IT provider in your practice. Most relevant tools can be found under the Physician Office IT Security and the Physician Privacy Tool Kit section of the Doctors Technology Office website.

Privacy & Security Declaration Information:

1. Personal Information Protection Act (PIPA) requires that each clinic identifies the most responsible physician and appoints them as the Privacy Officer accountable for privacy and security. Security measures can be delegated to others such as your local IT. The Privacy Officer is also responsible for establishing the Privacy Policy and Security Polies, procedures, and forms. For more information on this role, refer to the BC Physician Privacy Toolkit: A Guide for Physicians.
2. Privacy and Security Policies and related documents should be communicated to staff and any individuals accessing the clinic eSystems. Assistance in creating such policies are available from the Doctors of BC.
3. All clinic staff need to complete Privacy Training and Security Awareness Training comprised of new employee orientation and regularly scheduled refreshers. The content should include:
   a. Privacy and Security polices and related procedures including any changes introduced
   b. Overview of the clinic's security safeguards and staff responsibilities
   c. Risk mitigation strategies to protect patient information security
   d. Steps required for managing a breach in emergency situations
4. Clinic should provide employees with instructions for e-mails, text messaging, and web browsing. These guidelines must alert staff to possible fraud and prevent them from clicking on attachments or links that can download malicious software (malware) to be installed on the user's computer and potentially spread to the entire network.
5. Use of non-encrypted USB drives and mobile storage devices to store or transfer patient information is not recommended. If not properly protected, they can be compromised (lost or stolen) or be intercepted with malware. Malicious software can be spread to user's computer and potentially entire network.
6. Clinic should provide employees with instructions about password protection practices to reduce the risk of unauthorized access into the eHealth application. Passwords must not be shared with others even as temporary workaround and not used for access to any other services (e.g. Gmail, Facebook, LinkedIn). The 'save password' feature for any account is not safe because any user on that computer can then use the stored password. Each user should change their passwords semi-annually. See password management requirements on page 3 of this guide. For tips on creating secure passwords, visit the Physician Office IT Security Guide.
7. Notifying the VCH eHealth Team ensures CareConnect access accounts remain current. This will prevent the risk of someone accessing information to which they are no longer eligible. To contact the CareConnect team, email CareConnect@phsa.ca.
8. During the course of providing technical support, there is a chance that unauthorized access to clinical information can occur. Keep invoices and/or service receipts for at least two years. In case of a privacy breach or investigation, the clinic should be able to provide details about technology and physical safeguards implemented. Refer to the *DTO Health Technology Guide – Selecting IT Support* for what can be expected from your IT service provider.
9. See the "Private Practice Clinic IT Security Checklist" on page 3 of this agreement.

2 | 3



Please sign and return to Private.CareConnect@phsa.ca

Private Practice Clinic IT Security Checklist

There are a number of basic technology requirements that need to be in place to safeguard patient information within your practice. The PPN will protect clinics from most threats from the Internet; however, threats can also arise from within the practice. The checklist below details the minimum clinic IT security requirements as defined by VCH and the Ministry of Health for protecting your clinic from local threats.

Education, resources and supports on Clinic Privacy and Security are available via the Doctors Technology Office (DTO) https://www.doctorsofbc.ca/doctors-technology-office, DTOinfo@doctorsofbc.ca or 604-638-5841.

Physical Access Control

☐ Clinic site is equipped with a monitored alarm system

☐ Server/Network equipment is physically secured from public access

User Account

☐ Each user has a unique account and password to access systems within clinic's network

☐ User accounts are not shared among multiple users

☐ A separate user account is used for system administration

Password Management[1]

☐ Minimum password length is 8 characters

☐ Passwords contain characters from three of the following categories (Uppercase characters, Lowercase characters, Numerals, Non-alphanumeric keyboard symbols)

☐ Passwords are changed at a minimum semi-annually

WiFi Network

☐ SSID, WPA2/WPA3 and WiFi password settings are as per DTO Technical Bulletin[2]

☐ Guest WiFi access is completely isolated from the Clinic LAN/WiFi network

Anti-Virus Software

☐ Anti-virus software installed and enabled for auto update *(screenshot of configuration must be attached)*

Operating System

☐ There are no legacy/end-of-support operating systems in use (e.g. Windows XP, MacOS older than the latest three versions)

☐ The Operating System is enabled for auto updates or manually patched at a minimum semi-annually

Application Patching

Where it doesn't conflict with my EMR's system requirements.

☐ Desktop software, e.g. MS Office / Other applications are patched at a minimum semi-annually

☐ Browser plugin (Adobe Flash, PDF, Java) are patched at a minimum semi-annually

☐ Such patching conflicts with my EMR system requirements.

Clinic Information

Clinic Name: ______________________

Clinic Address: ______________________

Clinic IT Support/Clinic IT Vendor (if applicable):

Name: ______________________

Company Name: ______________________

Signature: ______________________

I have reviewed and endorse the above assessment:

Physician Name: ______________________

Signature: ______________________

[1] Refer to 'Physician Office IT Security Guide' pages 24-26

[2] Refer to Doctors Technology Office (DTO) Technical Bulletin "Wireless – Reduce Risk and Improve Performance"

3 | 3

ACKNOWLEDGEMENTS & DECLARATIONS

- Agreements must be signed as part of the sign-up process to access an eHealth viewers that contain a number of acknowledgements and declarations.
- Summary of acknowledgements:
  - Physician assigned as responsible for privacy and security policies
  - Policies are documented and communicated to all parties with access to systems
  - Clinic staff are trained on various security risks
  - eHealth portal provider is notified when access is to be revoked
  - 2 year log of all support activities that have been conducted on computers that have access to eHealth viewer (remote and local)
  - Private Practice IT Security Checklist has been completed
  - Agreement to allow use of eHealth viewer audited and cooperation if a breach occurs

PRIVATE PRACTICE IT SECURITY CHECKLIST

The Private Practice IT Security Checklist is provided with the CareConnect access agreement and contains the following sections:

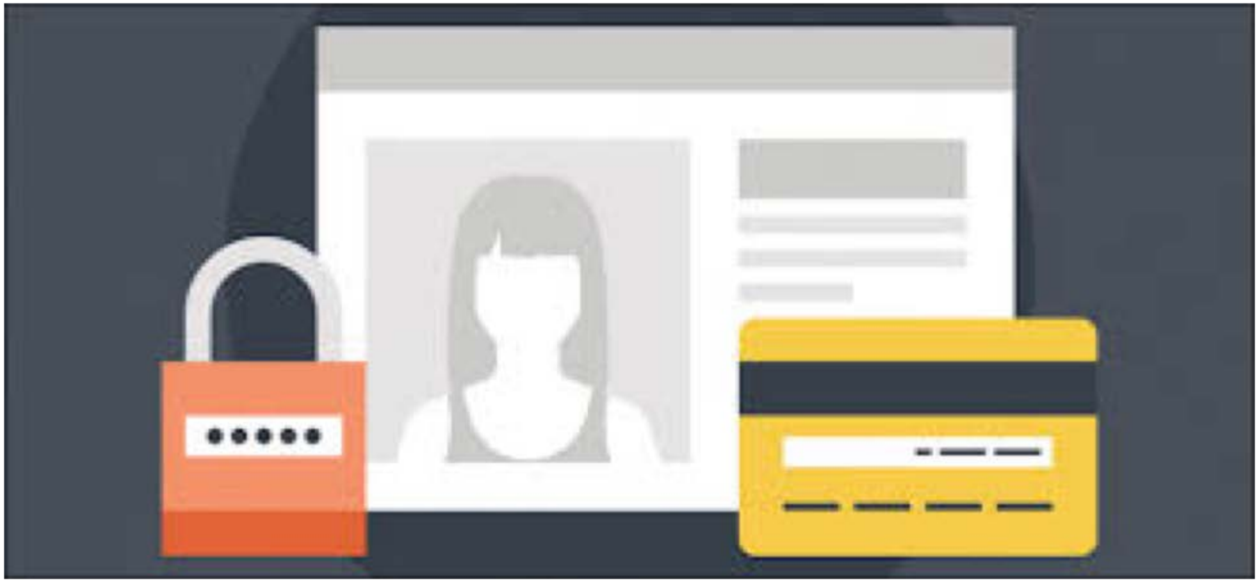
- Physical Access Control
- User Account
- Password Management
- Wi-Fi Network
- Anti-Virus Software
- Operating System
- Application Patching

PHYSICAL ACCESS CONTROL

- ❑ Clinic site is equipped with a monitored alarm system
- ❑ Server / network equipment is physically secured from public access

USER ACCOUNT

- ❑ Each user has a unique account and password to access your network
- ❑ User accounts are not shared among multiple users
- ❑ A separate account is used for system administration



PASSWORD MANAGEMENT

- ❑ Minimum password length is 8 characters, preferred length is 9-10
- ❑ Password contain characters from three of the following categories: Uppercase, lowercase, numerals, non-alphanumeric symbol
- ❑ Passwords are changed at least semi-annually

WI-FI NETWORK

- ❑ SSID, WPA2/WPA3 and Wi-Fi password settings are as per DTO technical bulletin ”Wireless – Reduce Risks and Improve Performance”
  - ❑ SSID is masked or disguised
  - ❑ WPA2/WPA3 minimum with a complex password
  - ❑ Default credentials for router reset to custom
- ❑ Guest Wi-Fi access is completed isolated from LAN

ANTI-VIRUS SOFTWARE

- ❑ Anti-virus software installed and enabled for auto-update (screenshot of configuration must be provided)

OPERATING SYSTEM

- ❑ There are no legacy / end-of-support operating systems in use (Windows XP, Mac OS older than latest few versions)
- ❑ Operating system is enabled for auto-updates and patched regularly

APPLICATION PATCHING

Where it doesn’t conflict with my EMR’s system requirements:

❑ Desktop software, eg. MS Office, is patched regularly

❑ Browser plugins are patched regularly

❑ Such patching conflicts with my EMR system requirements

RESOURCE LINKS

Provincial Health Services Authority (PHSA)

Care Connect Team
Email: careconnect@phsa.ca

Private Physician Network Administration

Email: ppnadmin@phsa.ca

Doctors Technology Office Technical Centre

https://www.doctorsofbc.ca/technical-centre

Physician's Office IT Security Guide (DTO)
https://www.doctorsofbc.ca/resource-centre/physicians/doctors-technology-office-dto/physician-office-it-security/

Doctors of BC Privacy Toolkit Website
https://www.doctorsofbc.ca/resource-centre/physicians/managing-practice/privacy-toolkit/

Office of the Information & Privacy Commissioner Website (PIPA, FIPPA)

https://www.oipc.bc.ca/about/legislation/

Office of the Privacy Commissioner of Canada (PIPEDA)

https://www.priv.gc.ca/

DTO TECHNICAL TEAM

Contact: 604 638-5841 or DTOinfo@doctorsofbc.ca

Q&A

Question Asked	Summarized Answers
Are you going to be collecting vendor financial information and why?	In terms of the 2yr log requirement of the CareConnect agreement – the log is intended to record what specific action was performed as part of the support activity. Financial information is not suggested to be recorded. Examples of potential details to capture in a log are invoice # (if exists), date of service, vendor name, and activity. Basically, an itemized account of the work.
Just a note from the password complexity side, it is significantly harder to break a password that is longer than more complex (passphrases vs. passwords). We've been recommending a string of 2 - 3 words with numbers and/or symbols padding. These have typically been 12 - 20 characters long	Agreed, this is a good point. Establishing password policies that provide complex passwords is key to clinic security.
Will there be any check in to make sure that these checklists are being met on an ongoing basis? It's not uncommon for standards to be set at the initial deployment of a clinic but they can slide over time.	There is not currently a clear, defined periodic review but a clinic should be able to plan for some type of check-in or re-assessment eventually. CareConnect agreement does have an acknowledgement that a clinic could be audited. Ministry of Health collaborated with VCH privacy office in developing this agreement and VCH may perform an audit. This is an example of the wave of the future as more information is being shared between Health Authorities and private practices.

Q&A

Question Asked	Summarized Answers
Does "Public = Patients" or "Public = clinic staff" in reference to checklist item “server / network equipment is physically secured from public access”	Public would be referring to people external to the organization, such as the patients.
Regarding semi-annual password changes and password complexity, some of these requirements exceed EMR password policies. Will DTO ask EMR vendors to align their password policies with these requirements?	EMRs have suggested guidelines for passwords but ultimately the policy is controlled by the clinic. DTO cannot dictate to an EMR vendor on their password policies but does share all suggested guidelines with the EMR vendors.
Med Access EMR never requires password changes. Same password used for years.	Password policy should be managed at the clinic level and enforce their own policies. The clinic password policy should be used at all access levels, workstation and EMR. CareConnect agreement includes declaration that password policy exists. MedAccess CareConnect-specific integration access will have password policy that reflects the agreement.

Q&A

Question Asked	Summarized Answers
I would guess IT support community understands PPN security protection and password policies but a fairly hard sell to private physicians, mainly due to cost implications. Is DTO or Doctors of BC offering learning for physicians on these topics and the value of implementing proper IT security?	Yes, DTO has a physician security training program that is currently providing privacy and security education to physicians across BC. This training also applies to CME credits for the physicians. DTO shares a lot of resources to the physicians in addition to the training mentioned, most of which can be found on our website. https://www.doctorsofbc.ca/doctors-technology-office
MOAs open visits for physicians in EMRs and then Dr continues with notes. That won't work with multiple log ins?	Should be addressed within EMR workflow. EMR can support MOA using their own workstation and EMR account to start an encounter note and doctor can finish with their own.
Since I missed the 1st presentation is it possible to get a copy	PDF copies of any past learning sessions may be obtained by emailing DTOinfo@doctorsofbc.ca

Q&A

Question Asked	Summarized Answers
Do you recommend that all clinics be on the PPN even if the EMR vendor doesn't require	PPN substantially improves security of but does not protect from things like human error, for example clicking on a malicious email link. If you are on the PPN, there are 3 layers of security; you will be protected from the internet by antivirus, intrusion detection and a firewall. PPN also has service level agreements, and can provide better support in terms of outages than another carrier. PPN access is a prerequisite for CareConnect access. You have access for millions of records and being on the PPN is a requirement to help have additional security to have access to the Provincial eHealth Viewer, CareConnect. PHSA is working to put in fiber-optic in most clinics and address all previous bandwidth issues. Performance on the PPN should not be an issue moving forward. An example recent clinic transition and had no noticeable performance issues. The considerations were a few clinic workflow changes and IT practices to adjust to when moving on to the PPN.
I do have one question regarding the logging of support activities on clinic infrastructure. All our support is provided in-house so there are no external vendors that perform services. Is this requirement about logging external vendors that gain access to provide support or logging all support services completed in the clinic in general? Obviously, we do not generate any invoices for the services performed.	While the CareConnect declaration currently refers to external vendor support activities, it is a good practice to keep the log of support activities performed on clinic systems even by internal it. The checklist may be updated in the future to reflect this. The key is logging the activity or event, so if an invoice # is not relevant, then using another reasonable piece of data to identify it would be expected.