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

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
**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)
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 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 to prevent data victimisation is therefore crucial.

This document details the requirements for granting access to CareConnect and, as informed by provincial legislation (PIPA - Personal Information Protection Act), the Privacy and Security Rules enacted by the Doctors of BC, the College of Physicians and Surgeons, and its Office of the Information and Privacy Commissioner, and Ministry of Health and PHSA Privacy and Security rules. Further information on each requirement is available in the appendix.

I acknowledge that:

1. The member of my clinic staff who is/are responsible for our privacy and security policies is/are:
   - [ ] myself
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
   - [ ] ________________
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
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)
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)

Doctors of BC Privacy Toolkit Website

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

Doctors Technology Office (DTO)

Contact: 604 638-5841 or DTOinfo@doctorsofbc.ca
<table>
<thead>
<tr>
<th>Question Asked</th>
<th>Summarized Answers</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th>Question Asked</th>
<th>Summarized Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does &quot;Public = Patients&quot; or &quot;Public = clinic staff&quot; in reference to checklist</td>
<td>Public would be referring to people external to the organization, such as the patients.</td>
</tr>
<tr>
<td>item “server / network equipment is physically secured from public access”</td>
<td></td>
</tr>
<tr>
<td>Regarding semi-annual password changes and password complexity, some of these</td>
<td>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.</td>
</tr>
<tr>
<td>requirements exceed EMR password policies. Will DTO ask EMR vendors to align</td>
<td></td>
</tr>
<tr>
<td>their password policies with these requirements?</td>
<td></td>
</tr>
<tr>
<td>Med Access EMR never requires password changes. Same password used for years.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>CareConnect agreement includes declaration that password policy exists. MedAccess CareConnect-specific integration access will have password policy that reflects the agreement.</td>
</tr>
<tr>
<td>Question Asked</td>
<td>Summarized Answers</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>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?</td>
<td>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. <a href="https://www.doctorsofbc.ca/doctors-technology-office">https://www.doctorsofbc.ca/doctors-technology-office</a></td>
</tr>
<tr>
<td>MOAs open visits for physicians in EMRs and then Dr continues with notes. That won’t work with multiple log ins?</td>
<td>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.</td>
</tr>
<tr>
<td>Since I missed the 1st presentation is it possible to get a copy</td>
<td>PDF copies of any past learning sessions may be obtained by emailing <a href="mailto:DTOinfo@doctorsofbc.ca">DTOinfo@doctorsofbc.ca</a></td>
</tr>
<tr>
<td>Question Asked</td>
<td>Summarized Answers</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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. |