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**.

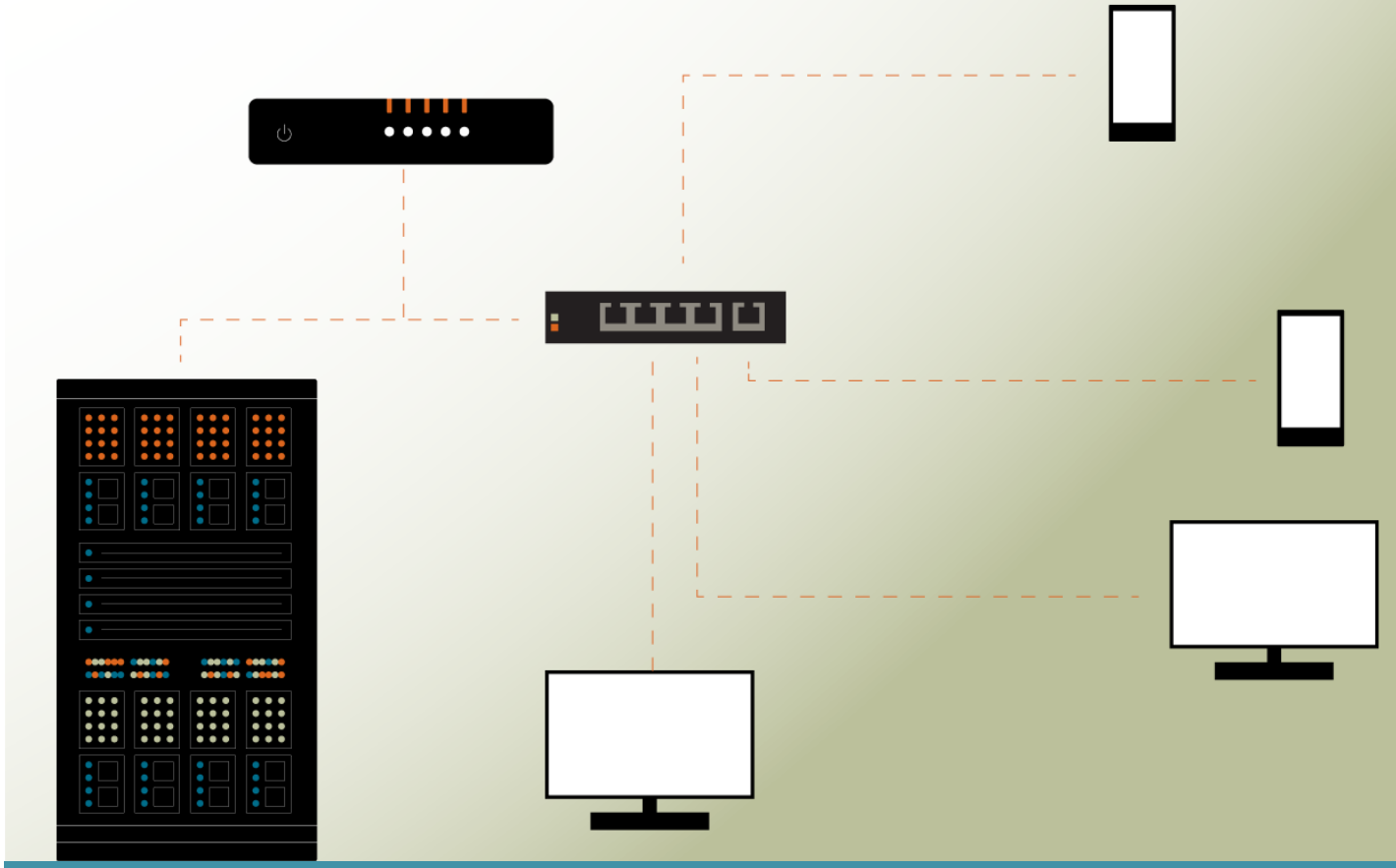
About DTO

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.

DTO Doctors Technology Office
A GPSC initiative

GPSC General Practice Services Committee

DTO Doctors Technology Office
A GPSC initiative



CLINIC IT SUPPORT COMMUNITY LEARNING SESSION WEBINAR 4: IT SUPPORT ROLE IN CLINIC SECURITY

GPSC General Practice Services Committee

LEARNING SESSION OVERVIEW

Topic: **IT Support Role in Clinic Privacy & Security**

Speakers: **Jesse Zacharias**, Health Technology Consultant, DTO
Ralph Buschner, Senior IT Analyst, DTO
Mauree Matsusaka, Health Technology Advisor, DTO
Agata Wodzynska, Virtual Care Specialist, DTO

Agenda:

- **Introductions & Updates**
- **OIPC Audit**
- **Provincial eHealth Viewers**
- **DTO Physician Office Security Course & Toolkit**
  - **Security Culture & Role Responsibilities**
  - **IT Support Selection**
  - **Clinic Security Self-Assessment**
  - **Asset Management**
  - **Role-Based Access**
  - **Password Management**
  - **Documentation & Resources**
  - **Hot Topic Questions / Q&A**

HOUSEKEEPING

Control Panel:

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

By moving your curser to the bottom of the screen the control panel will appear. The control panel includes the mute, chat, raise hand and Q&A functions.

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

Hand raising:

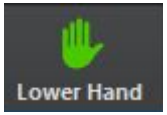
The hand raising feature is found on the middle of the Zoom control panel.

By default, your hand will not be raised.

When your hand is down, the button look like this:

Click on the button to raise your hand if you have a question or a comment.

When your hand is raised the button looks like this:



Click on the button to lower your hand if your question or comment has been addressed.

CLINIC IT SUPPORT COMMUNITY UPDATE

DTO Website Update – Technical Centre

- **Clinic IT Support Past Learning Sessions Info**

The Clinic IT Support Community Learning Session webinars provide direct knowledge-sharing venue for IT professionals and self-supporting physicians to connect with DTO. The online learning sessions provide topical and trending information beneficial to the IT support of clinics.

New/Updated Technical Resources

- IT Support Selection Checklist for Clinics
- Microsoft Windows 10 Upgrade Checklist
- PPN Technical Support Guide for Clinics
- Tech Bulletin - Microsoft to End Windows 7 Support
- Wireless Network Best Practices Guide for Clinics

OIPC PRIVACY AUDIT REPORT

- 22 medical clinics were recently audited by the *Office of the Information and Privacy Commissioner for BC (OIPC)* to assess how effectively they protect personal information and comply with the *Freedom of Information and Privacy Act (FIPA)* and the *Personal Information Protection Act (PIPA)*.

- The primary takeaway from the audit is that clinics need to attend to developing, implementing, and maturing their privacy management program.

- This includes ensuring appropriate resources, policies and procedures, training and compliance monitoring are in place to safeguard personal information.

- 16 key recommendations were highlighted by the report to help address the gaps found, most of which are addressed in our DTO Security Course.

- Link to OIPC Audit & Compliance Report P19-01: https://www.oipc.bc.ca/audit-and-compliance-reports/2340

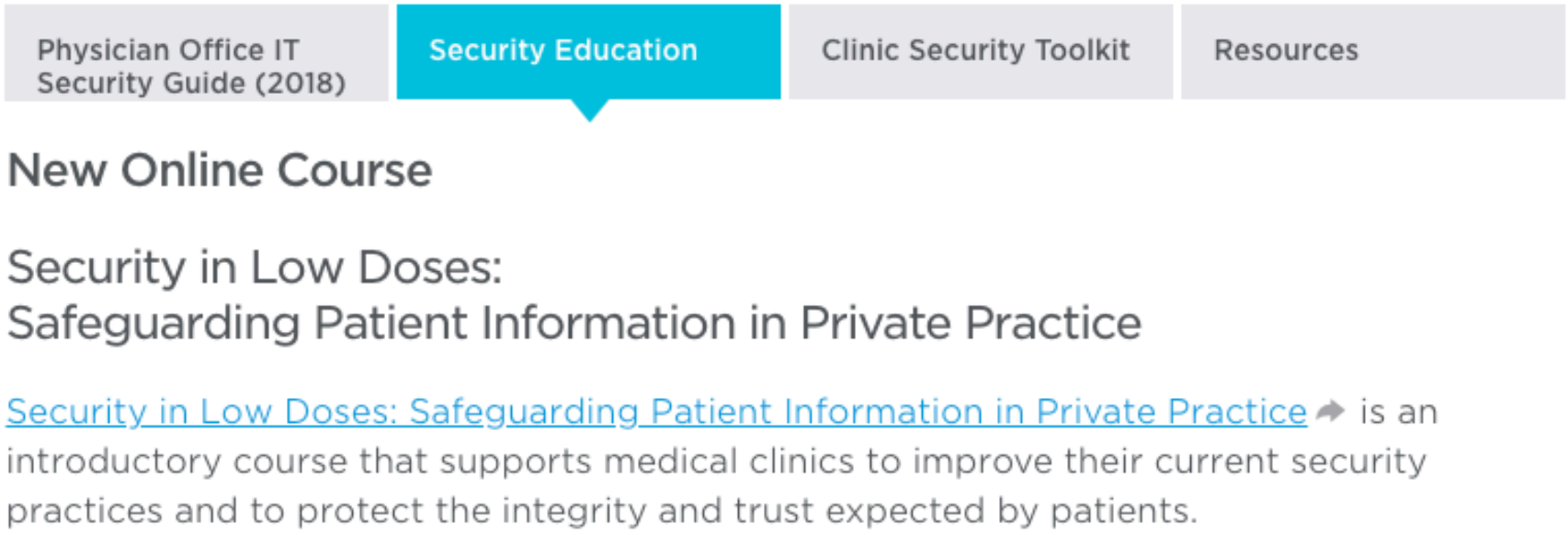
PROVINCIAL EHEALTH VIEWERS

- The provincial eHealth viewers are secure, read-only Electronic Health Records (EHRs) managed by provincial health authorities that deliver patient-centric information to support healthcare providers in their delivery of patient care.
  - **CareConnect** - PHSA
  - **Unified Clinical Information (UCI)** – Fraser Health
- A clinic must be on the **Private Physician Network (PPN)** to access CareConnect and UCI.
- DTO offers an introductory security course to support the requirements of provincial eHealth viewer access.

DTO SECURITY COURSE & TOOLKIT

- **Security in Low Doses: Safeguarding Patient Information in Private Practice**
  - Free online course hosted on the UBC CPD Website
  - Includes Clinic Security Toolkit & Resources

- **Physician Office Security: Safeguards 101 Workshop**
  - In-person workshop providing a basic introduction to safeguards



ROLES AND RESPONSIBILITIES OF PRIVACY OFFICER AND SECURITY LEAD

HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

GUIDE FOR A PRIVACY OFFICER AND SECURITY LEAD

Summary

This Guide assists clinics in documenting basic responsibilities of a Privacy Officer and Security Lead. Both roles play a vital role in:

- protecting patient information
- creating a culture of security
- establishing required measures to mitigate risk (safeguards)

Appointing the Privacy Officer and Security Lead and documenting their responsibilities is the first step in creating a culture of security at the clinic. Recognizing the process is complex, the Doctors Technology Office (DTO) created tools and resources. This Guide and the attached checklists can be adopted by clinics as guidance in creating their own framework, documentation, and training.

IT SUPPORT SELECTION CHECKLIST

- **Assess Your Clinic Technology Support Needs**
- **Interview Local IT Support Companies**
- **IT Support Service Questions**

HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

IT SUPPORT SELECTION CHECKLIST FOR CLINICS

Summary

This document offers a checklist of guiding questions to help select local information technology (IT) support for a private practice clinic. Prepare for interviews with IT support companies by assessing the specific needs of the practice. With this information, proceed to interview multiple companies for a potential service contract using the checklist below as a guide. Use a blank document or piece of paper to make notes of the answers provided and check off the questions once answered.

CLINIC SECURITY SELF-ASSESSMENT CHECKLIST

- **Administrative Supports**
- **Physical Safeguards**
- **Technology Safeguards**

DTO Doctors Technology Office
A GPSC initiative

TECHNOLGY SAFEGUARD	Yes	No	Unsure	Comments
1. Staff is aware that the "Save Password" feature in browsers should not be used when accessing applications and systems via internet.	☐	☐	☐	

ELECTRONIC ASSETS MANAGEMENT GUIDE

Asset Management Tools

- Device Inventory List
- Software Inventory list
- IT Activity Log

HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

ELECTRONIC ASSETS MANAGEMENT GUIDE

Summary

This guide helps private practice clinics in managing their IT infrastructure in order to support their privacy and security policies. By understanding and maintaining the technology tools at your practice, you can reduce the risk of a privacy breach and the burden of managing that risk.

ROLE-BASED ACCESS GUIDE

Access Management Tools

- Access Rights Management Checklist
- Access Rights Per Role Matrix Form
- User Access Maintenance Form

HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

ROLE-BASED ACCESS TO ELECTRONIC SYSTEMS GUIDE

Summary

This guide helps private practice clinics to implement an access management framework that will protect confidentiality and personal information using a role-based access concept. Staff access to clinical systems and devices are provisioned by defined roles which can be mapped similarly within workstation user accounts and most EMRs.

PASSWORD MANAGEMENT GUIDE

- **Why Clinics Need a Password Management System**
- **Guiding Principles of Password Management**

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.

DTO Doctors Technology Office
A GPSC initiative

RECOMMENDED DOCUMENTATION FOR CLINIC PRIVACY AND SECURITY

DTO Doctors Technology Office
A GPSC initiative

RECOMMENDED DOCUMENTATION FOR CLINIC PRIVACY AND SECURITY

Summary

This guide describes essential privacy and security documentation for a primary care clinic. Along with maintaining a library of digital records, create hard-copy binders easily accessible in case of major computer network failure.

Privacy and Security Binder Content

The Privacy and Security Binder should contain key information that is a foundation of personnel training and trusted information source for daily operations. It is an important part of your clinic security culture and can play an important role during a privacy breach investigation or when resolving complaints.

QUICK POLL QUESTIONS

Which of the DTO Clinic Security Toolkit resources we discussed today do you feel is the most valuable from your IT perspective?

a. Roles and Responsibilities of the Privacy Officer and Security Lead	**1**	**8%**
b. Clinic Security Self-Assessment Checklist	8	68%
c. Electronic Assets Management Guide	1	8%
d. Role-Based Access Guide	0	0%
e. Password Management Guide	2	16%

QUICK POLL QUESTIONS

Which of the DTO Clinic Security Toolkit resources we discussed today do you feel would be the most problematic to support?

a. Roles and Responsibilities of the Privacy Officer and Security Lead	**4**	**31%**
b. Clinic Security Self-Assessment Checklist	2	15%
c. Electronic Assets Management Guide	2	15%
d. Role-Based Access Guide	4	31%
e. Password Management Guide	1	8%

SECURITY QUESTIONS FROM PHYSICIANS

- How and when should we encrypt devices with personal info on them? (hard drives, USB sticks, etc.)
  - Any device that holds personal information needs to be encrypted. Many options are available for encryption, and a good starting place we suggest is the built-in encryption methods that the operating system or device may already offer (Bitlocker for Windows Pro and Enterprise versions, Filevault for Mac OS).
  - Pro or Enterprise versions of Windows are expected to be used as standard for access to important security features like this as well as other important features to control windows updates schedules etc.
- What type of password management software should we use?
  - DTO is vendor agnostic but can suggest features to look for and provide some example solutions to review and understand the types of features available. Common solutions include Dashlane, Lastpass, and Yubikey
  - Generally, using the local instead of cloud option with apassword manager is more secure when it comes to clinic use. Usage is primarily local to the clinic so cloud access from other locations would just add unnecessary security risks.

SECURITY QUESTIONS FROM PHYSICIANS

- What should we do for business continuity and disaster recovery systems (outside of EMR system)?
  - Most EMRs provide solutions or services for business continuity for the EMR but the other business-critical systems at the clinic must be considered as well.
  - There are many services to consider for this purpose also. The main points we stress are that there is a secure offsite backup for critical systems and info, as well as ensuring that data storage agreements cover a clinic's obligation under provincial privacy law (regional hosting, data usage agreements).
- Can we use public Wi-Fi to access personal health information?
  - Public Wi-Fi should never be used to access personal health information.
  - Any access to this information should be done through a secure VPN like that provided by the Private Physicians Network (PPN).
  - Any public Wi-Fi offered at a clinic should be separate from the clinic's Local Area Network (LAN) that is used for business.

RESOURCE LINKS

DTO Technical Centre

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

DTO Physician's Office IT Security Education

https://www.doctorsofbc.ca/resource-centre/physicians/doctors-technology-office-dto/physician-office-it-security/

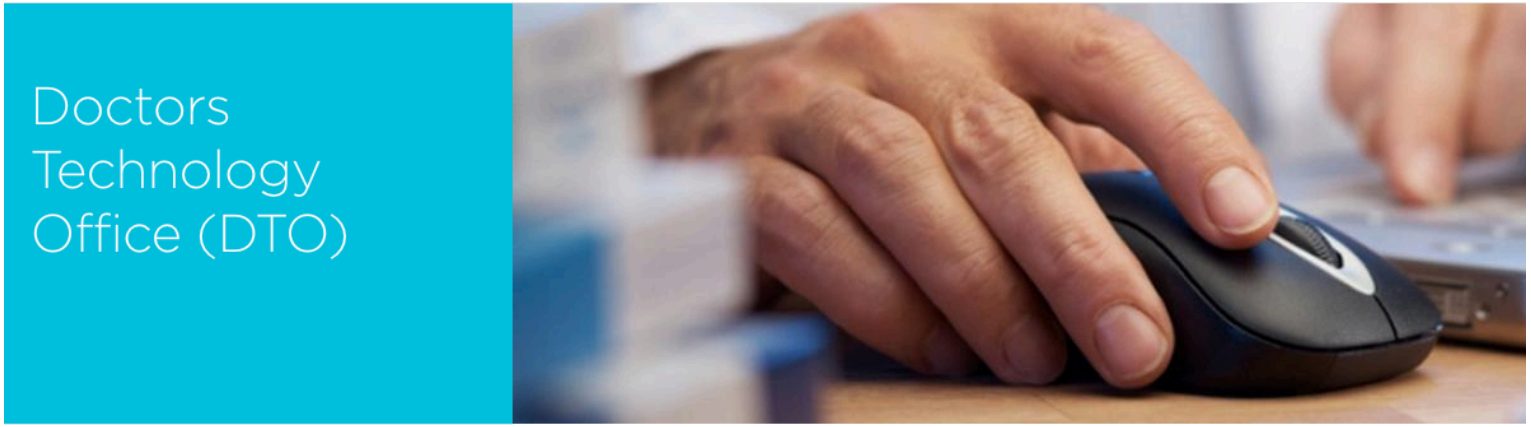
Doctors of BC Privacy Toolkit Website

https://www.doctorsofbc.ca/resource-centre/physicians/managing-practice/privacy-toolkit/

Office of the Information & Privacy Commissioner Website

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

DTO SUPPORT DESK



Thank you! For any questions or additional feedback, please contact us at: 604 638-5841 or DTOinfo@doctorsofbc.ca

SESSION Q&A

Question	Answer
Does DTO have any off-site backup requirements or recommendations for clinics?	They key challenge around this is that although most EMRs offered an offsite backup service (cloud-based), clinics need to also consider backing up other business-critical software and areas where personal information may be kept outside of the EMR. We do recommend an off-site backup system for the case of fire or flood and that it is a best practice to ensure that storage is within Canada when possible.
Are there requirements for managed services?	This will depend on the specific managed service being used. In general, all the security requirements we cover in our DTO resource materials should be considered when choosing services. We touch on things such as contracts, data storage location and usage considerations, and ensuring that agreements are in place with the service to ensure data is only used as expected.

SESSION Q&A

Question	Answer
Is there anything simpler than OS encryption like a shareware program a doctor can handle themselves?	We mention OS encryption because it is standard and generally easy to access within the operating system. There are many other encryption software available and are not able to recommend specific solutions, but we do stress that whatever solution is used that it must still be supported by the manufacturer.
Any status updates on the Private Physicians Network (PPN)?	Planned upgrade work on the PPN infrastructure has recently been completed to improve stability and speed offerings for all service types. PHSA decides upon the service offered on a clinic by clinic basis. NaaS (Network as a Service), was piloted on the PPN for the past 2 years and is now officially offered to physicians in the province as a service option.

SESSION Q&A

Question	Answer
Is there a hard date by which all these privacy and security requirements must be in place for a clinic?	We understand that not all of these requirements are in place yet for clinics in B.C. but they are expected to be in place already in order to meet the provincial privacy obligations of the clinic and as suggested general best practices. To be able to access provincial systems like the eHealth Viewers and the PPN, these types of requirements are now required to be signed off on by clinics. Security is a culture and ongoing discussion and the DTO security courses and tools aim to help clinics meet those requirements if they are not already.

SESSION Q&A

Question	Answer
What about MSP (billing) vendors that are US-based for remote support and monitoring?	The current privacy laws are stricter for public agencies like hospitals and health authorities in terms of where personal information can be stored (must remain in country for storage). While private companies like general practice clinics are not held to quite the same standard – it is still best practice to ensure that where possible, personal information used by vendors is stored in Canada. If it does need to leave the country for processing, an agreement with the vendor should be in place where they state how they will be using that information (processing only, not shared, store securely) so you can ensure they adhere to the privacy policy of the clinic.

SESSION Q&A

Question	Answer
Many patient data transfers I receive from other clinics that I do not manage are not sent to us without appropriate encryption or even with password protection in some cases. What is Doctors of BC doing to help education physicians province-wide about the importance of securing info like this?	This information is included in our physician security courses and resource materials that we provide and advertise to physicians across BC. We do stress the important of encrypting and password protecting all personal information being transported and welcome this feedback from you so we may stress this even more. It is also good to call out that it is indeed best practice to ensure that password for encrypted archived are sent separately from the data itself so they cannot be intercepted together. We will reinforce this in our DTO physician education.

SESSION Q&A

Question	Answer
Does Island Health have a system like Fraser Health (eHealth Viewer)?	The primary provincial eHealth Viewer outside of Fraser Health is CareConnect. This is administrated by PHSA and includes the Vancouver Island Health Authority access within that system.