Vancouver Division of Family Practice
Security & Technology Assessment

Report: Top Recommendations

Based on the 65 Security & Technology Assessments performed at Vancouver family practice clinics between June 2024 - February 2025.

From June 2024 to February 2025, Vancouver primary care clinics were invited to participate in a Security & Technology Assessment as part of the PMH Connectivity & Digitization Program. Each assessment included a 1-2 hour on-site consultation with a security expert, a customized report outlining findings and recommendations for improving clinic security, as well as follow up support with the security consultant to address clinic specific questions.

Many participants expressed interest in understanding broader trends observed across clinics in the Vancouver area – particularly common cyber security challenges and areas for improvement.

Below, we share the most frequent recommendations from each of the six assessment categories. While the examples here reflect common findings, each clinic received a tailored report with recommendations specific to their context and capacity for implementation.

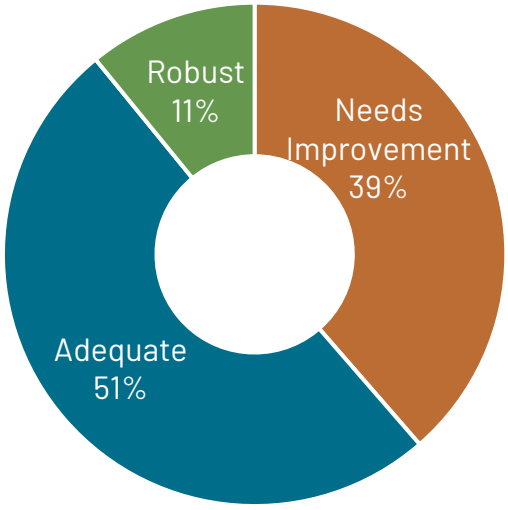
Advisory Note: The recommendations in this report are based on the most commonly made recommendations made during the Security and Technology Assessments performed from June 2024 to February 2025. They are not a comprehensive or complete list of all security measures a clinic should take to protect patient data and security. We advise that clinics seek the expertise of their IT provider/lead or an external security expert for decision making regarding the adoption of any recommendations.

EMR Security

Summary

The EMR Security assessment evaluated best practices around EMR security settings and workflows that ensure patient data is protected from unauthorized access.

Overall, a slight majority of clinics received an assessment rating of 'Adequate' or 'Robust', indicating a fair level of existing awareness around best practices for ensuring security in EMR application management.



Rating distribution across all clinics

Here are the top 3 detailed EMR Security recommendations provided to clinics.

Recommendation	Priority Level	Frequency
Enable IP restrictions	Medium	93% of clinics
Enable MFA (Multi-Factor Authentication)	Medium	68% of clinics
Disable concurrent sessions	Medium	58% of clinics

Detailed Recommendations

Enable IP restrictions – Medium priority

You do not have IP restrictions enabled, which means that anyone who gains access to your login credentials will be able to log in from anywhere to view patient data. **Consider enabling IP restrictions so only devices on the clinic network, or at practitioners' homes, can log in to your EMR**. Another related feature to consider is geo-restricting

access, so your EMR cannot be accessed by IP addresses outside of a list of permitted countries. Note that if you enable IP restrictions and thereby disable remote access to your EMR, practitioners will need to either use a VPN, or your EMR administrator will have to add all of your practitioner's home IPs to the list of allowed IPs. The VPN approach is preferable, as it will work consistently regardless of the location the practitioner is in and will ensure that they only access your EMR through the secure clinic network. The DTO's Health Technology team has both expertise in your EMR, and can make recommendations to help you decide on which VPN will suit your practice's needs best. They can be reached by emailing the main PSP contact email at psp@doctorsofbc.ca, where your inquiry will be redirected to the Health Technology team who can help guide you through these choices and how to integrate them with your EMR and practice workflow.

Reference: DTO Recommendations for VPN Setup and Usage
Reference: CHR guide on restricting IP addresses

Enable MFA (Multi-Factor Authentication) – Medium priority

The DTO recommends MFA be enabled for all EMRs. This is especially important when IP restrictions are not enabled, because MFA provides an additional level of security and identity verification to ensure that only authorized users are accessing patient records. **Consider contacting your EMR provider to see if you can enable MFA on your EMR, especially for any users accessing the EMR remotely**.

Reference: DTO Clinic Security Guide: MFA for EMRs
Reference: CHR guide on enabling and configuring MFA
Reference: Myle guide on enabling MFA
Reference: Oscar Pro guide on enabling and configuring MFA

Limit concurrent sessions – Medium priority

Concurrent sessions are currently enabled, which means that your login credentials for your EMR can be used on more than one device at the same time. **Consider contacting your EMR provider to request that concurrent sessions be limited to only 2 or 3 sessions within the same IP address, or disabled entirely**. This will help increase the chance you are alerted if someone else logs in using your credentials and can help you more quickly detect instances of unauthorized access.

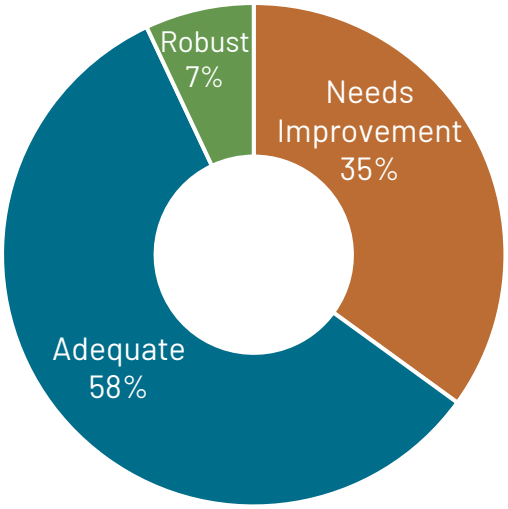
Reference: Telivy guide to understanding and mitigating the risks of concurrent logins
Reference: Open Worldwide Application Security Project on concurrent sessions
Reference: CHR guide to account-wide security setting configuration

Note: Not every EMR publishes their user guides to the public, so please check your own EMR's user documentation to see if this feature is available if you do not see a guide listed for your EMR on the above reference lists for these recommendations.

PC Security

Summary

This PC Security assessment examined the security of a clinic's personal computers (PCs) - both those used by staff and/or practitioners. We found that many clinics had some room for improvement relating to their computer security. Of note was that many clinics were not aware that Microsoft is ceasing support of Windows 10 in October 2025, after which time Microsoft will no longer provide operating system security updates.
Recommendations were provided to **75% of participating clinics to update or upgrade one or more computers (either Windows or MacOS).**



Rating distribution across all clinics

Here are the top 3 detailed PC Security recommendations provided to clinics.

Recommendation	Priority Level	Frequency
Enable screen lock after 5-10 min of inactivity	High	73% of clinics
Improve password complexity	Medium	65% of clinics
Plan for replacing Windows PCs by Oct 2025	Medium	62% of clinics

Enable screen lock after 5-10 min of inactivity – High priority

While locking the screen when walking away from the computer is a common operational policy, it is vulnerable to any sort of natural human error. **Consider ensuring that every device is set to automatically lock the screen after a maximum of 10 minutes of inactivity.** It would also be prudent to remind all practitioners and staff to use a keyboard

shortcut[1] to lock their computer as they leave their workstation to ensure that the computer is locked the moment it is left unattended.

Reference: DTO Clinic Security Guide: Technology Safeguards
Reference: Setting a screen lock on MacOS / Setting a screen lock on Windows

Improve password complexity – Medium priority

Low password complexity makes it easier for anyone with access (remote or in person) to the computer to easily guess the password and install malicious software without authorization. **Consider implementing a policy for minimum password complexity, with higher standards for administrator accounts, which should also include instructions for rotating them on a semi-annual basis.**

Reference: Doctors of BC Technical Bulletin on Easy-To-Remember Complex Passwords
Reference: Guide to changing passwords on Windows
Reference: Guide to changing passwords on MacOS

Plan for replacing Windows PCs by Oct 2025 – Medium priority

Some of the computers we looked at together are currently using Windows 10, but do not meet the hardware requirements to upgrade to Windows 11. Windows 10 will reach 'end of life' on October 14, 2025, and at that time all Windows 10 computers will not receive any further performance or security updates, as Microsoft is ceasing support of Windows 10 at that time. While this is a medium priority item at this point, it will be a high priority security risk next year. **Consider developing a plan for purchasing and replacing all PCs which are unable to be upgraded to Windows 11** so that you can ensure that your devices remain up to date with all security and vulnerability patches.

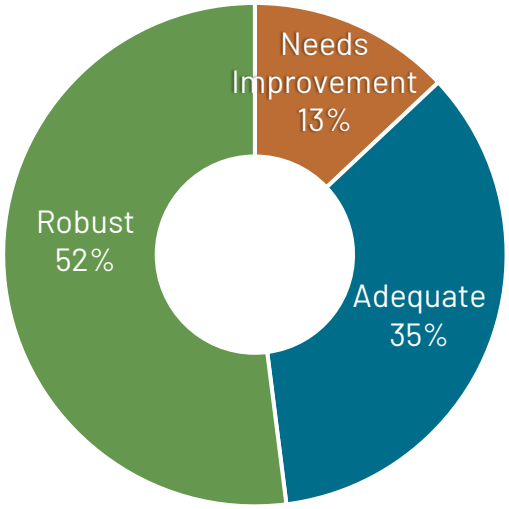
[1] Windows + L for Windows, or Control + Cmd + Q for MacOS

Network Security

Summary

The Network Security assessment examined the security of the clinic's wireless (Wi-Fi) network, including any guest networks if available. Many clinics had robust network security thanks to factors including clear guidance from the DTO as well as a clearly established industry standards for wireless network security in use across existing network devices and internet providers.

Most clinic networks required only one or two small—but important—security enhancements, rather than a complete overhaul of their existing infrastructure.



Rating distribution across all clinics

Here are the top 3 detailed Network Security recommendations provided to clinics.

Recommendation	Priority Level	Frequency
Wi-Fi password changed on a semi-annual basis	Medium	75% of clinics
Change Wi-Fi password from default	Medium	40% of clinics
Physically secure router	Medium	32% of clinics

Change Wi-Fi password on a semi-annual basis – Medium priority

Changing your Wi-Fi password on a semi-annual basis will help ensure that any person who gains unauthorized access to your Wi-Fi network will not have access that continues to persist, also known as persistence. Preventing persistence is an extremely important part of cybersecurity as it limits the amount of compromise possible. **Consider implementing a policy to change the clinic Wi-Fi network on a semi-annual basis, as well as changing your Wi-Fi password immediately.** This way, either malicious actors or

former staff or friends of staff members who might have had the password at some point will not continue to have access to your clinic's network indefinitely.

Reference: DTO Technical Bulletin - Wireless: Reduce Risks and Improve Performance

Change Wi-Fi password from default – Medium priority

Some routers have a default password that is the same for all devices of the same make and model. Other routers have a kind of formula from which quasi-unique passwords are generated, but which are easily guessed. Furthermore, any person who has enough time to snap a quick photo of the sticker on your router now has the credentials to your Wi-Fi network, and depending on the router, may also have administrative access to the router itself. **Consider ensuring that the Wi-Fi password is different from the default, and ensuring that it is rotated and changed on an annual or semi-annual basis.**

Reference: DTO Technical Bulletin - Wireless: Reduce Risks and Improve Performance

Physically secure router – Medium priority

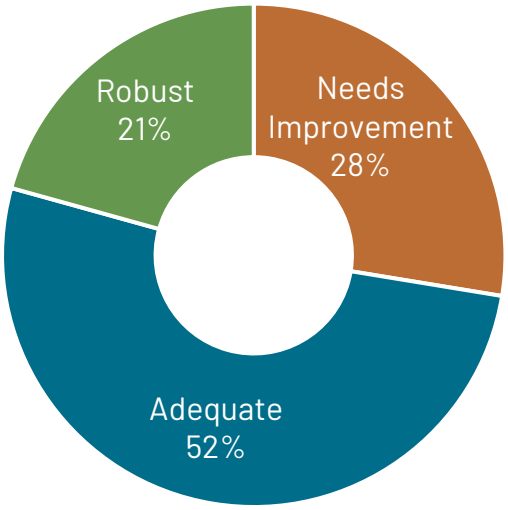
Physically securing networking equipment is essential to protect your clinic's network infrastructure from tampering, unauthorized access, and attacks that could compromise any devices on the network. If a networking device is accessible, a malicious actor could reconfigure it or install malicious software, compromising the entire network**. Consider ensuring your networking equipment is stored in a locked cabinet or room, with sufficient ventilation to prevent overheating.**

Reference: DTO Technical Bulletin - Wireless: Reduce Risks and Improve Performance

Physical Security

Summary

The Physical Security assessment reviewed how clinics managed devices and documents containing patient information to prevent unauthorized access, damage, or theft. This area showed an even distribution of assessment ratings, with the most common recommendations involving securing computers, printers, and network routers from theft and/or unauthorized access or viewing.



Rating distribution across all clinics

Below are the top 3 detailed Physical Security recommendations provided to clinics.

Recommendation	Priority Level	Frequency
Physically secure computers	Medium	87% of clinics
Secure peripherals from unauthorized access / viewing	Low	75% of clinics
Protect computers from unauthorized viewing	Medium	64% of clinics

Physically secure computers – Medium priority

During the on-site assessment's walkthrough, it was noted that the main reception desk's computer(s) were not physically secured and easy to access by clinic visitors. **Consider moving them out of sight into well-ventilated locking cabinets, or disabling all unused ports and securing the machines with a cable lock.** Ensuring that all clinic computers and peripheral devices are not easily stolen will reduce the risk of data breaches, safeguard active EMR sessions, and prevent accidental exposure of patient data.

Reference: DTO Physician Office IT Security Guide: Guidelines for Computer Placement

Secure peripherals from unauthorized access / viewing – Medium priority

Some of your devices such as printers, scanners, and fax machines are in easily accessible locations, allowing for the possibility that patient records might be viewed or malicious devices installed on them to log and store the data that is sent and received by them. **Consider securing these devices in such a way that prevents unauthorized access and/or theft.** If there is no location you can place these devices to better prevent access, even installing a cable lock on these devices can offer some basic security against theft.

Reference: DTO Physician Office IT Security Guide: Guidelines for Computer Placement

Protect computers from unauthorized viewing – Medium priority

Often, the screens of computers in use at a clinic are used to view and enter sensitive patient information. While this is not typically an issue for computers used in exam rooms during a patient visit, some of the computers at your clinic are not located in exam rooms and, if used to view or edit patient data, could result in unauthorized viewing of patient records by someone other than the patient or practitioner. **Consider installing privacy screens, changing the orientation of the monitors, or relocating these workstations to another, more secure location.**

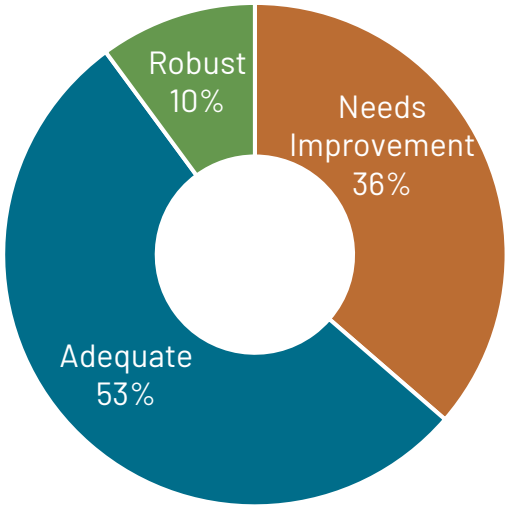
Reference: DTO Physician Office IT Security Guide: Guidelines for Computer Placement

Note: The Physical Security recommendations provided to participants varied most in wording and priority, depending on device placement and exposure to unauthorized access. At a minimum, all devices should be kept out of easy reach of visitors. Where possible, they should also be secured to prevent theft or tampering, such as the installation of malicious hardware.

Data Security & Integrity

Summary

The Data Security and Integrity assessment examined how clinics protect and manage patient records. While many clinics now use cloud-based EMRs, some still maintain physical records that require secure storage. Even in fully digital environments, patient data is often shared via USB drives, fax, or email—highlighting the need for secure handling and disposal of both digital and paper records. Most recommendations in this area focused on strengthening storage practices and disposal procedures to safeguard patient information.



Rating distribution across all clinics

Below are the top 3 detailed Data Security & Integrity recommendations provided to clinics.

Recommendation	Priority Level	Frequency
Develop process for disposing of devices securely	Medium	40% of clinics
Develop policy for disposing of documents securely	Medium	33% of clinics
Secure paper medical records	High	23% of clinics

Physically secure computers – Medium priority

In accordance with PIPA and PIPEDA regulations, devices containing medical records or information such as USB keys or CD's, or old devices such as computers, servers, or back-up hard drives must be destroyed such that no information is recoverable. **Consider hiring a secure device disposal service or developing a policy for securely disposing of devices that may contain personal health information.**

Reference: Doctors of BC Guidelines for Secure Destruction of Personal Information

Develop policy for disposing of documents securely – Medium priority

In accordance with PIPA and PIPEDA regulations, documents containing medical records or personal health information that are no longer required must be destroyed by crosscut shredding. **Consider developing a policy for establishing when records are no longer required, which should include the process for securely disposing of these documents, as well as ensuring they are kept in a secure locked room, cabinet, or bin until ready to be shredded.**

Reference: Doctors of BC Guidelines for Secure Destruction of Personal Information

Secure paper medical records – High priority

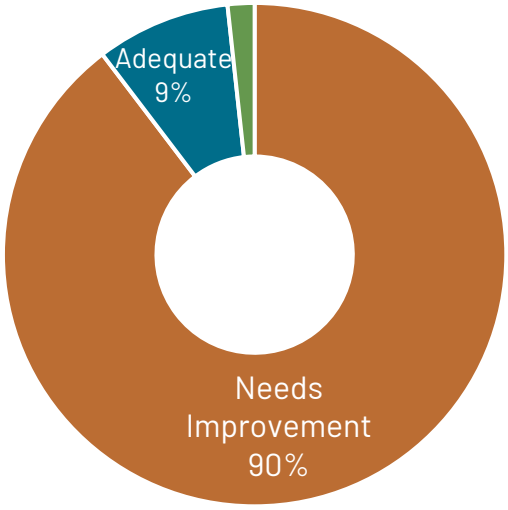
During the on-site assessment, it was noted some patient records were either left out in the open until they could be scanned and uploaded to the EMR, or stored in an area that was not secured from unauthorized access. Doctors of BC has a number of specific recommendations that are based on the federal and provincial privacy laws, called PIPA and PIPEDA, which specify that records should not be placed in a location that allows viewing or access by anyone not directly involved in the patient's care, and should be stored securely, in a locked cabinet or room. **Consider storing patient records in a location that meets the recommendations set out by Doctors of BC and the College, which are intended to ensure your compliance with the legal requirements set out by PIPA and PIPEDA.** While there may not be room in your practice to store all records in a locked room that not accessible to the public, any records that are stored in publicly accessible areas should be stored in cabinets that are kept locked at all times.

Reference: Doctors of BC Privacy Toolkit: Employing Safeguards
Reference: Doctors of BC: Is it safe to leave paper files unattended in the office?
Reference: BC College of Physicians Practice Standard: Medical Record Management

Vulnerability Awareness & Planning

Summary

The Vulnerability Awareness and Planning assessment examined clinic policies and staff training related to cybersecurity. It also aimed to raise awareness amongst clinic teams about the importance of their roles in maintaining a strong security posture to protect patient data. This was the most common area for improvement across nearly all clinics, highlighting a critical need for better staff training and clear privacy and security policies. These measures help ensure that staff understand their responsibilities and know how to respond appropriately to potential privacy or security breaches.



Rating distribution across all clinics

Here are the top 3 detailed Vulnerability Awareness & Planning recommendations provided to clinics.

Recommendation	Priority Level	Frequency
Regular staff cybersecurity and phishing training	High	98% of clinics
Develop a clinic Incident Response Plan (IRP)	Medium/High	85% of clinics
Keep a record of all technical activities	Medium	82% of clinics

Regular staff cybersecurity and phishing training – High priority

A critical part of any business' success in security is staff training and awareness, as humans are the largest security vulnerability in any system. The CareConnect Privacy and Security Declaration requires security awareness training to be provided when onboarding new staff, as well as reviewed yearly. **Consider developing a policy to ensure this**

training is included in the onboarding process and reviewed on a yearly basis as part of your usual staff professional development.

Reference: Vancouver Division Cybersecurity Training Resources

Develop a clinic Incident Response Plan (IRP) – Medium priority

These are plans or checklists that should be readily available to staff in the case of a security or privacy breach and should describe all necessary steps when responding to such an incident. It should include questions about how the incident occurred, when it was discovered, how it was responded to, and the process for notifying affected individuals. It should also include a post-breach analysis section that should examine the immediate response to the breach, as well as the long-term strategies taken to mitigate the risk of this happening again. **Consider developing an incident response plan checklist and communicating it to all staff. This plan should also be reviewed and updated on an annual basis.** There is a list of resources and templates to assist with developing this in the Appendix of this document.

Keep a record of all technical activities – Medium priority

In order to satisfy the requirements set out in the CareConnect Privacy and Security Declaration, you must keep a record (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 your clinic/worksites' network, either directly or remotely. **Consider keeping a file of all such receipts or invoices and ensuring that staff are aware of this requirement.**

Appendix: Resources for developing policies and checklists

Broad Guidelines

The Digital Governance Standards Institute (DGSI), in accordance with the Standards Council of Canada and in collaboration with Public Safety Canada, has developed a standard of cybersecurity in healthcare. While not legislation, this standard is intended to be used for conformity assessment, which can be used to form a basis for setting legal precedent regarding the evaluation of whether a clinic's cybersecurity had met the legislative requirements set out in PIPA and PIPEDA during the period when a privacy or security breach occurred. This document provides clear and understandable suggestions for best practices in healthcare cybersecurity that are in line with what are considered the best practices required by the various legislations relating to privacy and data protection.

Cybersecurity: Cyber resiliency in healthcare (PDF) – *DGSI, Public Safety Canada*

Recommended Documentation for Clinic Privacy & Security (PDF) - *DTO*

Tips for Developing Privacy and Security Policies (PDF) - *DTO*

Physician's Privacy Toolkit (web page) – *DTO*

Privacy and Security Resources for Physicians (PDF) – *DTO*

Canadian Center for Cybersecurity: Developing an IRP (PDF) – *Gov't of Canada*

Templates and Worksheets

Privacy Policy Worksheet (Word Document) - *DTO*

Clinic Privacy Policy Template (Word Document) - *DTO*

Privacy Breach Policy Guide & Template (PDF) - *OIPC*

Privacy Breach / Incident Response Plan Checklist (PDF) – *OIPC*

Staff Confidentiality Agreement Template (Word Document) – *DTO*

Third Party Confidentiality Agreement Template (Word Document) – *DTO*