PHYSICIAN OFFICE IT SECURITY GUIDE

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

BRITISH COLUMBIA

doctors of bc

Doctors Technology Office (DTO) offers a comprehensive suite of health technology practice supports and resources to guide family physicians and practice teams through the technology landscape. We provide guidance on up-to-date technology solutions that are aligned with security best practices and are a troubleshooting resource when technology fails.

To access additional information and resources on how to incorporate security safeguards into your practice, please visit the DTO website. Doctors Technology Office is an initiative of the Family Practice Services Committee (FPSC), one of four joint collaborative committees that represent a partnership of the Government of BC and Doctors of BC.

For more information, support or questions:

Doctors Technology Office

604 638-5841

DTOInfo@doctorsofbc.ca

doctorsofbc.ca/doctors-technology-office

Table of Contents

CMPA.ACPM
Empowering better healthcare
Pour l'avancement des soins de santé

The CMPA supports the use of appropriate privacy and security practices and encourages BC's physicians to consider the recommendations contained in this guide.

DISCLAIMER: Best practices for IT security depend on the sensitivity of the data and the individual situation and change regularly as new technology and methods become available. The individual physician must determine the degree to which each best practice applies to their situation.

This guide provides general information only. Doctors of BC accepts no liability whatsoever for any IT or security problems you may experience or for any claims, demands, losses, damages, costs, and expenses made against or incurred, suffered, or sustained by you due to those problems, nor any costs you may incur in resolving any gaps or issues in your IT infrastructure.

ABOUT THIS GUIDE

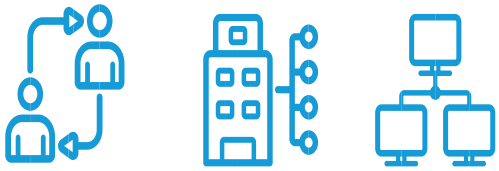
Physician clinics contain sensitive personal health information (PHI) patients entrust to others for their personal health and well-being. Protecting this personal health information through appropriate office systems is critical to support business continuity. Safeguards must be in place to ensure that physician clinics comply with the following:

- Section 34 of the Personal Information Protection Act (PIPA)
- Professional requirements of the College of Physicians and Surgeons of BC
- Guidance Documents from the Office of the Information and Privacy Commissioner for British Columbia (OIPC) for protecting information.

This publication draws from the above resources, focusing on key elements and best practices to enhance privacy and security at the clinic level. This shorter, more user-friendly guide aims to help physicians, clinic managers, staff, and IT support start on the path to achieving best practices for protecting clinics from information security risks.

Security Obligations Under PIPA

Physicians' offices and clinics are organizations subject to provincial private sector privacy law, the Personal Information Protection Act (PIPA). It should be noted that hospital and community clinics within health authorities Physicians' offices and clinics are organizations subject to provincial private sector privacy law, the Personal Information Protection Act (PIPA). It should be noted that hospital and community clinics within health authorities are governed by provincial public sector privacy law, the Freedom of Information and Protection of Privacy Act (FIPPA). This Guide only discusses the requirements of PIPA.



ADMINISTRATIVE SAFEGUARDS **PHYSICAL SAFEGUARDS** **TECHNOLOGY SAFEGUARDS**

Section 34 of PIPA requires organizations to protect personal information by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

This guide complements the BC Physician Privacy Toolkit by providing details, where applicable, practical steps and tools needed to protect personal health information in compliance with PIPA through applying appropriate safeguards.

You can find the information you need in the three sections of this guide, each of which highlights practical methods of safeguard clinic and patient information.

PLEASE NOTE: While this document provides physicians and clinic staff with a general guide to various privacy and security requirements, you will likely need more than this guide. We strongly recommend that you retain a knowledgeable and qualified IT professional to regularly assess and maintain your clinic network. If you wish to perform a self-assessment of privacy and security safeguards for your clinic, you may want to refer to Securing Personal Information: A Self-Assessment Tool for Organizations, published by the OIPC. Other templates and forms are available on the Doctors Technology Office webpage, and in Appendix A of this document.

ADMINISTRATIVE SAFEGUARDS

Creating a culture of security and safeguarding patient information is the responsibility of all clinic staff, including clinicians, managers, medical office assistants, IT personnel and service providers. This section provides guidelines for the fundamentals of administrative safeguards, which include:

- Designated roles and responsibilities
- Documented policies
- Human resources practices
- Incident management processes
- Risk management processes
- Business continuity and disaster recovery plans
- Internal assessments

Designated Roles and Responsibilities

Privacy Officer

In a medical practice, one physician is responsible for structuring and managing the privacy management program. This individual is the Privacy Officer.

The privacy officer leads and centralizes privacy and security-related decisions regarding safeguards. This person has the overall responsibility of ensuring these safeguards comply with the Personal Information Protection Act (PIPA) and meet professional practice standards required through the College of Physicians and Surgeons of BC. They must also support best practice recommendations through the Canadian Medical Protective Association (CMPA).

In a solo practice, the solo physician is the de facto privacy officer. The designated physician may choose to delegate responsibilities for the privacy management program to an employee, but that physician remains ultimately responsible and answerable to the College of Physicians and Surgeons of BC and the Office of the Information and Privacy Commissioner.

PIPA, Section 5 outlines that a clinic must:

- Develop and follow policies and practices necessary to meet the obligations of the organization under the Act.
- Develop a process to respond to complaints that may arise from not complying with the Act.
- Provide those privacy policies and practices, information on the complaint processes available to anyone who requests it.

Specific additional responsibilities include:

- Implementing and managing program controls over:
  - Compliance
  - Privacy breaches
  - Complaints, questions, and access to personal health information requests
  - Conducting or overseeing Privacy Impact Assessments (PIAs), where applicable
- Designing and implementing employee training
- Conducting ongoing assessments and revisions

The clinic privacy officer should be thoroughly familiar with all sections of this Security Guide, as well as the Doctors of BC Privacy Toolkit (see Appendix A).

Security Lead

The security lead is responsible for developing and maintaining standards (for hardware and software) and procedures to ensure that all requirements to safeguard personal health information, as required through PIPA, are implemented and complied with.

The security lead also assists the privacy officer in developing clinic security policies according to industry best practices. These are constantly evolving in response to emerging data security threats. The security lead assists the clinic in taking appropriate steps towards safeguarding personal health information. They should be aware of standards that may need to be met to permit trusted access to appropriate information from health provider registries across British Columbia.

This position typically requires professional experience in IT and network management. This means that clinics often outsource this security lead role to a contracted local IT support organization. Use this guide to help start a conversation with your local IT support organization. The Doctors Technology Office provides resources and technical information that can assist the security lead in this process. Targeted resources are available to help the privacy officer and security lead on the path to creating a culture of security.

NOTE: Physicians practicing under the LFP Payment Model may be eligible to receive payment for time spent on Privacy Officer responsibilities. Please refer to the LFP Payment Schedule.

Documented Policies

In addition to ensuring that policies and procedures are in place that meet professional standards established by the College of Physicians and Surgeons of BC and best practices by the CMPA, private medical clinics in British Columbia must comply with PIPA.

A clinic must:

- Develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under the Act
- Develop a process to respond to complaints that may arise from non-compliance with this Act
- Make information available on request. This includes:
  - Clinic privacy policies and practices
  - The process that clinics use to handle privacy complaints

Some basic policies that should be in place and documented include:

- Onboarding and offboarding processes for staff
- Secure transmission (email and fax) of personal health information
- End-of-day clinic closing procedures
- Confidentiality and information sharing agreements Guidelines on contracts and confidentiality agreements for staff are available on pages 21/22 of the BC Physician Privacy Toolkit.

Other policies besides these examples are required to protect personal health information. All staff should be familiar with and guided by the privacy and security policies that the clinic has in place. Links to various forms that clinics can adapt for their own use are provided in Appendix A.

Human Resources Practices

Hiring Clinic Staff

Anyone you are considering hiring in your clinic who will have access to personal health information— whether as an employee or a contractor—should be screened through background and reference checks.

Training Clinical Staff

Physician leads and clinic managers should actively support information security within the clinic through clear direction and commitment to staff training. All training programs should be developed to ensure staff are aware of and understand:

- Their personal health information security roles and responsibilities
- Permitted access, use, and disclosure of personal health information
- Permitted retention and disposal policies.
- Requirements for maintaining and securing passwords

> The Doctors of BC Privacy Toolkit contains a comprehensive set of self- guided webinars designed for clinic staff (See Appendix A).

All clinical and office staff should attend regular (e.g., annual) privacy and security training, and the clinic should keep records of their successful completion. Training should focus on PIPA, and how to apply its requirements in an electronic medical record (EMR) environment. Doctors of BC has published a series of short, practical videos on this topic (in collaboration with authorities on privacy and security including the College of Physicians and Surgeons, CMPA, Office of Information and Privacy Commissioner for British Columbia [OIPC], and the Ministry of Health). Further clinic security training options are available through the Doctors Technology Office.

Confidentiality Agreements

The designated security lead should require clinic staff, and third-party vendors/service providers who may have access to personal health information, to sign a confidentiality agreement.

Physicians working in clinics are not typically expected to sign confidentiality agreements because they are bound by the existing professional standards set by the College of Physicians and Surgeons of BC. Group clinics may still choose to establish an additional commitment to privacy and security by having physicians sign a

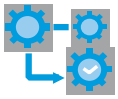
confidentiality agreement. Please refer to pages 21 and 22 of the BC Physician Privacy Toolkit for sample confidentiality agreements.

For various confidentiality agreement forms designed for clinic staff and third-party contractors, See Appendix A.

Offboarding Clinic Staff

When any staff member leaves a clinic through termination, resignation, or on extended leave, the clinic should ensure that: (Note: immediacy of the below will depend on each situation)

- The person's keys and pass cards are immediately recovered
- Access privileges are immediately revoked (or in the case of a planned departure, appropriately transferred to other staff), and this process is done with minimal impact on clinic operations.
- Access to non-clinic systems and information is revoked, and appropriate governing bodies are notified.
- IT staff should verify that any devices to be taken away by the person (e.g., smartphones, tablets) have been purged of clinic data before their departure using security best practices (see the section on Records Management).
- Appropriate security personnel are notified when someone leaves the clinic or is terminated.



Incident Management Processes

An "incident" is any occurrence of unauthorized access to personal health information. To be considered "unauthorized," the access must be in contravention of PIPA.

Some of the most common privacy breaches occur when personal health information is stolen, lost, accessed, or mistakenly disclosed when a computer or smartphone is stolen, or personal health information has been mistakenly emailed or faxed to the wrong person. Other breaches occur when there has been inappropriate access to information (intentional or unintentional).

The OIPC recommends four steps to manage privacy breaches:

1. Contain the breach
2. Evaluate the risks
3. Notification
4. Prevention

Additional guidance on responding to privacy breaches can be found in the OIPC Privacy Breaches: Tools and Forms, OIPC Breach Management Framework, and Doctors of BC Privacy Toolkit. See Appendix A.

The privacy officer for your clinic should be familiar with the basic steps needed to mitigate the damage of privacy breaches and prevent them from recurring.

Risk Management

Processes

Privacy and security risk management is a key responsibility of the clinic privacy officer. In assuming this responsibility, the privacy officer should consider what risks exist to clinic security, including emerging external risks such as ransomware.
The important first steps of this assessment are:

- Identify where personal health information is being held and how sensitive it is, including the location of temporary files used while downloading or printing.
- Assess potential security risks in the clinic. Since significant privacy and security risks can be subtle, and not necessarily technology-specific, all staff have an important role in identifying them. For one example, refer to the OIPC Self-Assessment Tool (see Appendix A).
- Create a list of the potential issues or risks, and then:
    - Evaluate the impact of each risk. Consider the consequences of losing the availability, integrity, or confidentiality of personal health information through a security failure.
    - Evaluate the impact on physicians, clinic staff, and patients if an identified security risk were to become an incident (e.g., a security breach).
    - Assess the likelihood of such failures occurring, including possible threats and vulnerabilities
    - Evaluate what risks are acceptable to the clinic.

By identifying the risks and systematically determining the impact and likelihood of them occurring, your clinic can prioritize appropriate responses. Together, you can create a risk management plan that your clinic, physician leads, and clinic managers, can follow to protect personal health information.

A sample clinic security self- assessment is available through the Doctors Technology Office.

Business Continuity

In the face of a catastrophic event, continuing to care for patients while protecting personal health information is critical for clinics. Your business continuity plan should include disaster recovery.

"Business continuity" is the capability of an organization to continue the delivery of products or services at acceptable, predefined levels following a disruptive incident. A disruptive incident can be any unplanned event that causes a general system or major application to become inoperable for an unacceptable length of time. Examples are a network being unavailable for an extended period, a lengthy power outage, and damage to or destruction of equipment or the facility.

Clinics should plan for unexpected, disruptive incidents.

At an absolute minimum, tested processes for backup must be in place to protect essential business systems, including clinic EMRs, critical network components, and configuration information.

A business continuity plan will help your clinic:

- Minimize the risk of failure to comply with PIPA's requirements for safeguarding information.
- Reduce the likelihood of decisions being made on an ad hoc basis after a major disaster.
- Prevent a minor disaster from becoming a major disaster.
- Provide a proper work environment for clinic staff, if there is damage to a facility.
- Provide an audit trail of what steps taken during the incident.
- Ensure that a review of "lessons learned" is conducted following the incident, to help define corrective and preventive actions.
- Ensure maintenance plans are developed to refresh the plan whenever new procedures or technologies
  are available to improve support and planned responses to future incidents.

For useful guides to help develop a plan for disruptive incidents, including major disasters, see Appendix A, Business Continuity and Disaster Planning Publications.

Consult your IT support and EMR provider on how to access and review audit logs.

Internal Assessments

The privacy officer and/or delegate should conduct random internal reviews of the entire system (hardware and networking) and EMR application audit logs. This ensures that users are not accessing or updating personal health information or printing or deleting files not directly related to their professional role. (See the section Turn On Audit Trail for more information).

For support in conducting an internal clinic security assessment, you may contact the Doctors Technology Office.

PHYSICAL SAFEGUARDS

Section 34 of the Personal Information Privacy Act (PIPA) requires technology safeguards to be in place to protect personal health information from unauthorized use, disclosure, copying, modification, or disposal. This section notes that security requirements are reasonable and meet reasonable standards. Basic physical safeguards to protect personal health information include:

- Computer displays and printer placement best practices
- Networking and server equipment security protocols
- Strong records management
- Fire suppression measures

Best Practices for Computer Displays and Printer Placement

Computers, displays, and printers should be physically located in settings that minimize unauthorized viewing and access.

- Position computer screens in patient areas (such as the reception desk) so that unauthorized users cannot easily view them.
- If it is not physically possible to prevent unauthorized users from viewing computer screens that could display patient information, consider purchasing privacy screens for the monitors.
- Install printers in locations where unauthorized users cannot potentially access them (e.g., away from public areas).

Securing Network and Server Equipment

Clinic network and server equipment should be kept in a secure area.

- Ensure all network equipment (e.g., physician private network equipment, clinic switches) is in a secure and locked area—preferably in a dedicated wiring closet—to prevent unauthorized users from plugging their own devices into the clinic network.
- If server equipment has additional ventilation requirements to minimize the potential hardware failure from overheating, seek advice from your IT support for specific recommendations.
- To avoid the fire risk, do not store combustible materials that are used for other purposes where servers and network equipment are located (e.g., paper records, cleaning supplies).

While keeping systems secure and protected from unauthorized use, clinic policies and procedures should also allow for emergency access by staff in case of fire.

Records Management

Records management includes not only the keeping of records, but also their safe disposal when they are no longer required.

To comply with this requirement means that:

- All computer equipment must be securely disposed of when no longer required.
- Personal health information may not be kept on obsolete electronic equipment.

The National Institute of Standards and Technology (NIST) in the US publishes various standards on computers and information security. Standard 800-88 is most used to securely sanitize media when it is no longer required. Of the three types of sanitation cited in the standard, you should use “purge” and “destroy” for media that will physically leave the clinic’s control. You can do this by using software or physical techniques.

Using software is an advantage as it allows for the reuse of sanitized media, such as portable hard disks and USB keys. However, keep in mind that not all software designed to securely delete files meets the NIST 800-88 standard. Before using software for this purpose, be sure that it is compliant with NIST 80088 revision1 , and that it produces a certificate of destruction that can be presented for audit purposes.

Physical destruction is another effective—although permanent—media sanitization option. Driving a nail through hard disk platters and smashing solid-state drives may be effective, and solid-state memory chips should be thoroughly destroyed as well. To be compliant with NIST, your clinic should keep a record of the media (the type of media, serial number, etc.) that has been disposed of in this way.

Please refer to Appendix A for a sample agreement for local IT.

Fire Suppression Measures

Appropriate fire suppression measures should be in place in all clinics. When you conduct a fire suppression and general business continuity risk assessment, consider that water sprinklers may permanently damage electrical equipment, including computers, servers, and network equipment.

Follow these guidelines to establish fire suppression safeguards:

- In general, Class C or multipurpose dry chemical Class ABC type fire extinguishers are recommended by the Canadian Centre for Occupational Health and Safety. Ask for advice from your clinic IT support provider, office building manager, and local fire protection authorities before implementing specific systems to protect network equipment and servers.
- Fire alarm and suppression systems should be tested and refreshed according to manufacturer guidelines and building management requirements.
- Ensure fire extinguishers are not expired.
- Train staff, and offer periodic refreshers, to ensure they are thoroughly familiar with how to use fire extinguishers.

Other Physical Safeguards

Other physical safeguards that you can implement to limit access to information include, but are not limited to:

- Imposing a role-based system of access to offices and records on a 'need to know' basis
- Clearing desks at night
- Locking filing cabinets and cupboards
- Logging out of the network before leaving for the day
- Keeping "in transit" records with staff carrying them or locked away out of sight
- Using a cross-cut shredder to dispose of sensitive documents
- Installing a monitored alarm system

For more advice on maintaining physical safeguards see the link to the BC Physicians Privacy Toolkit in Appendix A.

TECHNOLOGY SAFEGUARDS

Security for clinic computing systems includes safeguarding in-office hardware, local servers, and remotely connected devices, such as laptops, tablets, and smartphones. It also involves safeguarding operating systems and all networks—wired and wireless—from potential threats and having strong access controls in place. Implementing security best practices with the support of IT is the responsibility of all clinic staff.

In the office, all clinic staff should understand the importance of and implement these routine safeguards:

- Using strong passwords or passphrases
- Applying a setting for auto logoff after a period of inactivity
- Using a password-protected screensaver
- Locking mobile phones when inactive
- Protecting mobile device data with a username and password
- Transmitting personal information safely (e.g., protocols for fax, email)
- Maintaining backups

Other best practices safeguards will require IT support, including:

- Keeping firmware, operating systems, and all software security patches up to date
- Hardening servers
- Applying strong encryption to protect data at rest and in transit, on both clinic computing systems and mobile devices
- Installing firewalls and anti- malware, such as anti-spam or antivirus software
- Restricting cookies
- Installing a hardware or software intrusion detection system for your wired and wireless network
- Installing a data leakage/data loss prevention system
- Configuring the operating system
- Implementing access control

The rest of this section discusses these best practices.

Hardened Servers

"Hardening" is a process that restricts functions to reduce the vulnerability of servers. This is particularly important when they are open to the Internet. The goal of hardening is to eliminate as many security risks as possible on a given system, recognizing that greater vulnerabilities exist when a system is required to perform more than one function (e.g., delivering electronic medical record application services; storing identifiable personal health information in documents, databases, or spreadsheets).

You will likely rely on your IT support to harden your clinic server. The IT industry publishes helpful recommendations on how to harden specific servers. Also, when installing or configuring servers, clinic IT support should follow guidelines established by their server software vendor.

In addition to adhering to IT industry guidelines, clinics should implement application whitelisting on computing systems to help prevent unauthorized applications from being used.

Automatic Lockouts

Clinics should configure computers to lock out users after a predefined period of inactivity, or an unsuccessful number of login attempts. The timing of this will depend on the operational environment:

- In general, automatic lockout should occur in 30 minutes or less, depending on the sensitivity of the information.
- If the user is frequently away from the desk, they should regularly manually log out.
- To reduce the potential for "brute force" attempts with password combinations by unauthorized users, computers should be configured to automatically lock out after a maximum of 10 unsuccessful login attempts, with account lockout duration of 30 minutes.

Lockouts can be enabled through the electronic medical record (EMR) application, the operating system, or both. Note that locking out only at the EMR level may still leave the workstation open to unauthorized access to potentially sensitive email, documents, and data. To keep the highly confidential personal health information contained in the EMR safe, the best choice is to enable lockouts for both the EMR and the operating system.

You may need to consult your EMR vendor to enable the application lockout feature. Once your clinic policy is established for lockouts, end-users should not be permitted to alter the settings.

> Clinic computers should be automatically locked out after being unattended for 30 minutes at the longest, or significantly less time where there is a risk of unauthorized users gaining access.

Encrypted Data

Encryption standards evolve over time. For the moment, choose an encryption solution that uses Advanced Encryption Standard (AES) with 256-bit key length, simplified key management and escrow (consult your IT support provider if necessary). Support for Intel® AES-NI technology, UEFI, and GPT platforms will help to future-proof hardware purchases. Do not underestimate the importance of keys, and where this information is kept. Your encryption algorithm is only as good as the key needed to unlock it.

> "Encryption" is the process of encoding a message or information in a way that limits access to authorized parties only.

All data, including server backups, should be encrypted whether the data is in transit, or at rest.

If your clinic stores personal health information on a local server (e.g., a server located inside the clinic), ensure that:

- All server backups are stored off-site in a secure location, preferably managed by a qualified business that specializes in this type of service.
- The server is backed up daily to provide the most up-to-date data possible in the event of server hardware failure.
- Recovering from the backup is tested regularly.
- All backup media, such as a USB or tape drives, is encrypted and protected using strong passwords or passphrases known only to authorized individuals.
- Backup tapes and removable storage media are stored away from magnetic sources to avoid erasure.

If your clinic stores personal health information on computers (desktops and laptops), mobile devices (e.g., laptops, smartphones and tablet devices), and removable media (e.g., USB drives), ensure that:

- All devices are password protected and encrypted to reduce the risk of disclosure in the event of loss or theft.
- Devices such as desktops or laptops have built-in hard drive (firmware) encryption.
- Removable devices, such as USB drives, have built- in encryption software.
- The operating systems on devices have built-in encryption software (e.g., Microsoft's BitLocker), which can also be used to encrypt a USB drive. Alternatively, a third-party commercial product may be used (e.g., Folder Locker).

Firewalls

Another important safeguard is using firewalls on personal desktop computers. Firewalls employ high- security settings and should be installed and enabled on all clinic computers.

Firewall tips:

- Personal firewall software is typically part of the operating system, but default settings are often configured with a low-security threshold or may be turned off completely. Ask your IT support to identify the settings on your computers.
- Configure the software to a higher security setting to provide another layer of protection against unauthorized access.
- Some operating systems (e.g., Windows 10 and Mac) provide built-in firewall protection that allows the end user to customize to its highest security settings, which should be used.
- Clinics should also purchase commercially available personal antivirus or firewall software (e.g., Bitdefender, Webroot, ZoneAlarm, Norton/ Symantec) and configure it to the highest security setting possible for your clinic. Special considerations are required if a firewall is being

set up for a clinic that has been connected to the Physicians Private Network (PPN). For further information see the section on Network Security.

Antivirus and Anti-malware Software

Antivirus software detects computer viruses and disarms or removes them, preventing this form of malicious software from interfering with a computer system, or spreading to other devices. Many antivirus software vendors offer expanded protection to include a wider variety of malicious software, known as "malware."

Antivirus and anti-malware applications should be configured to automatically update virus signatures.

Besides computer viruses, malware includes keyloggers, Trojans, worms, and ransomware. These forms of malware can present more serious risks to clinics, as they are frequently designed to steal confidential data, passwords, and other account information, or in extortion scams by holding critically important data hostage until a ransom is paid.

Anti-malware software should be automatically updated to keep its database of virus signatures current.

Some pointers to keep your systems safe:

- Run or schedule automatic software updates daily (after normal business hours) to ensure they do not interfere with the performance of other applications.
- Consider upgrading or changing to software that provides layered security to achieve overall protection against cyber threats. This type of software includes anti- malware (including antivirus) and desktop firewall capabilities.
- Do not use outdated software, even if virus signatures are still available.
- Avoid free software. It may not be immediately obvious how the cost of free software is recouped by the vendor. This poses risks to the clinic that are not covered by contracted software license agreements, data-sharing agreements, or vendor privacy statements.

Restricted Cookies

"Cookies" are small text files that are downloaded onto a computer while the user is visiting a website. They are stored—either temporarily or permanently—as a means for the site to recognize the user and keep track of their preferences. Cookies are used to help website visitors support legitimate business practices. However, they can introduce vulnerabilities to systems, and you should include their restriction in your clinic's IT security plan. Cookies can be altered by malicious users or software. They are designed to be stored on the local computer drive as part of normal browser operation, and this means they can damage stored information.

Malicious cookies can be used to:

- Steal sensitive personal health information of another user, which can lead to fraudulent acts such as identity theft.
- Track web browsing history of a user, which may be unknowingly sold to online advertising agencies, resulting in end users receiving junk emails and unwanted advertisements.

To protect against malicious cookies, you should have all of your computers configured to allow cookies only from trusted sites. You can find configuration options to adjust cookie settings in your Internet browser's options menu.

TIPS to Defend Against Cyber Attacks

The rise of malicious software is an emerging threat to healthcare information systems. A wide variety of measures are needed to protect clinics from the many types of threats, but the first and most important line of defense is making sure clinic staff are aware of the risks of installing malicious content on their computers.

> "…by 2025, lack of talent or human failure will be responsible for over half of significant cyber incidents."
> – 2023 Gartner Report

All staff should have a basic understanding of malware, which is software that has been specifically designed with malicious intent and takes many forms, including:

- **Social engineering** is the art of manipulating people's willingness to be helpful and give up confidential information.
- **Phishing** is the fraudulent use of email to make a user believe that its contents are from a legitimate source, to gather personal information.
- **Malware** is malicious software that infects a computer or network.
- **Ransomware** is a form of malware that encrypts files and then sends a message to the infected computers demanding payment to unlock the files.

> To learn about email and text message scams, see the Canadian Anti-Fraud Centre.

Other forms of malware are adware, spyware, worms, Trojans, and notably, email scams (see Appendix B, Glossary).

Ransomware has caused some of the most widespread and particularly devastating attacks on health care organizations and clinics in recent years.

Here are some tips to help prevent ransomware attacks, and to mitigate the effects of an attack, should one occur:

- Keep all hardware (computers, servers, routers, switches, etc.) and software (firmware, anti- malware, etc.) updated with the latest security patches.
- Never log in as the administrator for day-to-day access. Use a user account instead. (See the section Create Effective User Accounts on Clinic Systems below).
- Regularly back up data and test recovering from backups.
- Do not open any email attachments from within your email program and treat all with suspicion. Save the attachment somewhere else and scan for malware before opening. If you do not trust that your desktop anti-malware software will keep you safe from malicious attachments, contact the sender by a different method (e.g., phone, text message) and ask them to confirm that they sent it.
- Implement application whitelisting, an IT technique that is increasingly being used to ensure that only authorized programs can run on a computer.
- Disable any macros that may be present in Word, Excel, or other applications unless absolutely required.
- When web browsing, access only trusted, well- known websites, and use caution when clicking on links or downloading files.
- When setting up network security, use "small office business class" grade wireless routers, and similar grade network firewalls with active web filtering. Provide a separate wireless network for non-staff access.
- Focus on awareness and training: Since staff are an important line of defense against security threats, make sure they know the risks involved, and what to do to prevent ransomware or other malware from creating a major business continuity incident, or privacy breach.

Mobile Device Security

Using mobile devices to access patient health records and other clinical data in a clinic setting can pose a significant risk if they are unsecured. The Office of the Information and Privacy Commissioner & Auditor General of British Columbia recommend taking the following 15 steps to effectively secure mobile devices, in order of priority.

Begin with Step 1 and work your way to Step 15:

1. Password-protect all mobile devices.
2. Lock your screen.
3. Encrypt your device.
4. Limit password attempts.
5. Use anti-malware software.
6. Don't jailbreak or root mobile devices (see Appendix B—Glossary)
7. Be selective with apps. (Apps are designed to collect a wide range of information from mobile devices, which can be convenient, but in some cases can steal information. Install only apps that come from an official "app store," such as iTunes or Google Play. Consult your privacy officer for help if needed).
8. Limit app permissions. (Consider the implications of an application's request for permission to access information before installing it).
9. Keep software up to date.
10. Limit location information. (Weigh the convenience of apps that use GPS against the privacy issues associated with the information gathered on user habits).
11. Review voice commands. (Voice command processing typically takes place on computer servers that may be located outside of Canada. If you don't find this feature useful, consider disabling it).
12. Promptly report lost or stolen devices.
13. Bluetooth, Wi-Fi, and NFC (near-field communication) should be configured with appropriate security or turned off in public places.
14. Safely dispose of your device.
15. Consider using Find My Phone (an app available to locate your phone, under this name or a similar name).

For more information on securing mobile devices, see Appendix A, OIPC Mobile Devices: Tips for Security and Privacy.

Clipboard Security

The clipboard (copy/paste function) temporarily stores copied text, images, or files in memory. While most clinical applications themselves do not automatically place patient data on the clipboard, users often copy/past clinical notes or sensitive patient information from non-integrated applications into their electronic medical records (EMRs, i.e. Accuro, Profile, Dragon Dictate, AI Scribe).

This creates privacy and security risks if:

1. The clipboard contents are accessed by malicious software (i.e., clipboard hacking).
2. Sensitive data remains in memory longer than necessary, increasing the risk of unintentional disclosure.

Why Copy and Paste is a Security Concern

Section 34 of BC's Personal Information Protection Act (PIPA) requires that "*An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks*."

1. Clipboard Hijacking and Data Leakage:

   When you copy sensitive data, it is stored temporarily in the clipboard. Malicious software or authorized applications running on the system can often access clipboard contents, leading to data breaches, credential theft, or unauthorized data transmission – even across organizational boundaries.
2. Pastejacking Attacks:

   "Pastejacking" is when malicious code or links are substituted into a user's clipboard without the user's knowledge. When pasted, they may execute harmful commands or expose confidential information unknowingly. This is particularly concerning if users are instructed to paste into terminals or administrative fields.
3. Exfiltration via Shadow IT and AI Tools:

   Employees may unintentionally copy patient data or confidential documents into third-party AI tools, personal email, or unsanctioned messaging apps. Modern data loss prevention (DLP) tools rarely track clipboard movements into unsanctioned apps, making such leakage difficult to detect and control.
4. Unmonitored Fileless Data Movement:

   Unlike traditional files transfers, clipboard actions (copy/paste or typing) do not generate file-based security events, so DLP

solutions may not log or block them. This allows data to move undetected between applications or users.

5. Browser and Application Vulnerabilities:

   Browser and application flaws may allow cross-site scripting (XSS) or manipulation of pasted data introducing further vectors for attack or data corruption.

6. Hidden Clipboard Cache in Microsoft Windows 10-11:
   Windows 10 and 11 maintain a **hidden cache folder** not visible in File Explore that stores copies of clipboard content – including screenshots and sensitive data – even after the clipboard history has been cleared.
   This hidden cache is created by the **Windows Shell Experience Host** and stores clipboard data as PNG image files and other formats. These files persist on disk even after restarting the PC or clearing the visible clipboard history (accessed via Win + V). They are hidden by default in File Explorer but can be viewed using PowerShell or command-line tools.
   Microsoft states this cache is temporary; however, in practice, it remains until manually deleted. Users concerned about privacy may need to run cleanup scripts or disable clipboard history features to prevent long-term retention.

   Key Differences from the Visible Clipboard History:

   - The visible clipboard history (Win+V) stores up to 25 items and can be cleared normally.
   - The hidden cache stores items invisibly on disk and may persist indefinitely.

Lack of encryption

Clipboard data cached by Windows 10–11—including hidden cache files—is **not encrypted on disk**.

- Clipboard data is typically stored in plain text or image format for performance reasons.
- While Windows includes **BitLocker** and **Personal Data Encryption**, these do not apply to clipboard cache files directly.
- The hidden clipboard cache remains unencrypted during active use, making it potentially accessible if someone gains filesystem access.

If **full-disk encryption** (e.g., BitLocker) is enabled, clipboard cache data benefits indirectly from that protection. Without it, cached clipboard data is readable by anyone with OS-level or physical access to the device.

Security Implications

Hidden cached clipboard files present another attack surface. Malware or attackers with administrative access can extract sensitive clipboard data from the filesystem, even after the clipboard appears "cleared."

In short:

- Real-time clipboard hacking captures live data.
- Hidden cached files allow recovery of previously copied data.
- Enabling disk encryption, limiting admin access, and regularly clearing clipboard cache help reduce this risk.

Built-in Protections

On macOS

- **App Sandboxing:** Restricts apps (especially from the App Store) from accessing clipboard data unless explicitly allowed.
- **Universal Clipboard Controls:** Can be disabled in *System Settings -> General -> AirDrop & Handoff.*
- **Clipboard Access Prompts:** Some apps request explicit permission to access the clipboard (macOS Ventura+).

On Windows

- **Windows Security (Defender):** Provides real-time protection and can detect and block malicious clipboard-monitoring processes.
- **Controlled Folder Access:** Limits access to sensitive folders, reducing clipboard-related attacks.
- **Cloud Clipboard Management:** Disable cloud sync for the clipboard in *Settings -> System -> Clipboard.*
- **Hidden Clipboard Cache Awareness:** Be aware of the hidden cache files on Windows 10-11 and use cleanup scripts or disable clipboard history to ensure data is not persistently stored.

Best Practices for Safe Clipboard Use

1. **Copy only What's Necessary**
   a. Avoid copying entire documents or full patient records. Copy only minimum data needed.
   b. Always carefully review copied clinical documentation for accuracy before adding it to the patient's health record or sharing it.
2. **Clear Clipboard After Use**
   a. **macOS:** User third-party utilities like *Pastebot* or *Clean Clip* to auto clear.
   b. **Windows:** Press Windows + V -> Clear All.

3. **Disable Clipboard Syncing**
    a. Turn off cloud syncing unless absolutely required, especially on shared or clinical devices.
4. **Use Trusted Apps Only**
    a. Avoid unknown browser extensions or software not vetted by your IT or privacy teams.
5. **Keep Systems Updated**
    a. Regular updates help patch vulnerabilities that could expose clipboard data.
6. **Run Regular Security Scans**
    a. Use antivirus or endpoint detection tools to identify clipboard-monitoring threats.
7. **Enable Full Disk Encryption**
    a. Use BitLocker or equivalent tools to protect cached clipboard data from unauthorized access.

Email Security

Email is generally transmitted across the Internet as an unencrypted, easily read text message. Before it arrives in the recipient's inbox, it may pass through many hardware devices that are maintained by multiple service providers located around the world.

This means that email is not a secure method of transferring personal health information unless special precautions are taken. Email may not be the appropriate mode of communication in all circumstances, clinics should develop clear, written policies on the use of email to communicate patient information, and ensure those policies are followed consistently. Additional guidelines and recommendations on developing office policies related to email and fax are outlined on pages 52-55 of the BC Physician Privacy Tool Kit.

If email is the only method available to send personal health information, consider using applications that can encrypt the message. Here are two examples:

Use public/private passwords pair

Public and private passwords—created as a pair for encryptions—are better known as "public/private certificates" or "keys." To encrypt an email before sending, a user can look up a public key that is posted on the Internet and freely available, created by the recipient. The sender can use this public key to encrypt the email or file before sending.
Once the message is in the recipient's inbox, that person can use their own private key to decrypt the email. Since no passwords need to be shared between users when using public/private certificates, it is not necessary to find a secure method of transmitting the password itself, such as phoning the recipient or sending a fax: only a public key is required to encrypt the message. This option offers a significant advantage over using an ordinary password-encrypted file such as a zip file.

> Email is not a secure method of transferring personal health information unless special precautions are taken.

Two email encryption solutions for clinics that use public and private keys are:

- GPG4win
- Mailvelope

Non managed keys alternatives

Other email encryption solutions take a somewhat different approach. Encryption is still done, but by the service provider and the setup/administration is simplified because users do not have to manage any public/private keys pair. Instead, a secure portal to the email server that encrypts the communication is used to secure and protect both sender and receiver, using the same service provider. When the recipient is not using the same service provider, or simply does not have a secure solution, a temporary tunnel is provided to the recipient. Instead of an email, the recipient receives a "you have received email" email. When the recipient responds, the temporary secure tunnel is automatically established to protect the receiver.

Here are some examples:

- Hushmail
- Brightsquid

In BC, the privacy legislation (PIPA) permits physicians to communicate with a patient via email without the protection of encryption, if the patient has provided appropriate informed

consent and acknowledged the risks. Before initiating email communication with a patient, physicians and clinics should communicate the following to patients:

- How emailing or faxing personal health information can result in accidental disclosure or interception by other people.
- What precautions the clinic has taken to reduce the risk of an intercepted transmission.
- What other delivery options are available for very sensitive information (e.g., sending photocopies by mail or courier).

Finally, all emails should include a confidentiality notice when broadcasting email messages. Use the bcc field to protect the privacy of every recipient when inserting email addresses.

The Doctors of BC Privacy Toolkit has guidelines on obtaining appropriate consent. See Appendix A.

Fax Security

Misdirected faxes are a common type of privacy breach throughout the BC health authorities. Errors can occur when someone misdials a number, or when a physician's office moves and does not update their fax number.

For sample email and fax confidentiality notices, see Appendix A.

To protect against privacy breaches with faxes, clinics should ensure that:

- The fax number being used is active and correct.
- The sender takes utmost care that the fax number has been accurately dialed.
- A fax cover sheet is always used, and always includes the name, address, and phone number of both the sender and receiver.
- A confidentiality notice is attached.
- Fax numbers with preprogrammed numbers are regularly checked for accuracy.
- Fax confirmation reports are checked to ensure correct transmission.
- Fax machines are used only by authorized staff.
- The receiver confirms that their fax machine is in a secure location or is notified in advance of the fax and requested to stand by the receiving machine.

Data Integrity and Protection when Moving Patient Information

At times, clinical records and patient personal health information needs to be moved out of the clinic (e.g., when a clinic moves to a new address), or transferred to another location (e.g., when records are needed by a specialist or hospital).

In these cases, all staff are responsible for ensuring that the information is protected and for following appropriate policies and procedures:

- Clinic policies, procedures, and confidentiality agreements should reflect personal responsibilities that all clinic staff must protect clinic personal information.
- Paper and electronic records containing personal health information should be physically protected (see Section 2 of this guide, Physical Safeguards).
- Any removal of patient records or other personal health information from the clinic, for any reason, should be properly authorized and documented.
- All computing devices or electronic media (e.g., laptops, smartphones, and USB drives) containing personal health information must be encrypted.

For best practices on retention and secure transfer of clinical records published by the CMPA, see Appendix A.

Network Security

Most clinics are large enough to have a full network system, making safeguarding of information more critical. Ensure the following measures are in place.

Disable network plugs/ports in public areas

Unauthorized individuals plugging their laptop or other devices into accessible clinic network plugs (wall sockets) installed in public areas is a security risk. To minimize this risk:

- Test unused network plugs to be sure they are not active, especially in public areas.
- Verify that the other end of the cable at the wiring closet is not connected to the local network switch or router.

Install a firewall with stateful monitoring

"Stateful monitoring" or inspection, also known as dynamic packet filtering, is a firewall technology that monitors the state of active connections. This information can be used to determine which network packets are allowed through the firewall. Firewalls with stateful monitoring limit authorized traffic to clinic requirements and should be used in clinics in place of passive firewall filters commonly found in consumer grade routers. Some firewalls have built-in IDS features (see next item).

Install a network intrusion system (IDS)

An (IDS) includes measures to detect wireless network intrusion, is recommended as a part of minimum requirements to secure personal health information by to the OIPC and is cited in the Doctors of BC
Privacy Toolkit training webinar "Keeping Personal Information Safe."

Install a data loss prevention (DLP) system.

An (IDS) includes measures to detect wireless network intrusion, is recommended as a part of the minimum requirements to secure personal health information by the OIPC and is cited in the Doctors of BC Privacy Toolkit training webinar: *Keeping Personal Information Safe.*

Private Physician Network

If your clinic is on the Private Physician Network (PPN), you will need to take additional measures:

The PPN service must be cancelled before moving

If your clinic on the PPN is moving or closing, it is important to contact Provincial Health Services Authority (PHSA) and your EMR vendor at least one month ahead of time. Otherwise, the PPN equipment will remain at the old location, and the next tenant could potentially use this service and gain unauthorized access to the network.

The PPN must not be interconnected to any commercial Internet services without appropriate security measures

In some cases, clinics that are using the PPN may require a second Internet connection (e.g., wireless service for patients, digital music). In this case:

- Be sure these services are not connected to each other without appropriate security measures, including specialized firewall configurations and hardened servers so that only appropriate information can be accessed.
- In all cases, ensure that EMR information destined to the EMR vendor does not cross the Internet portion of the network, and vice versa. EMR traffic and Internet traffic flows must be kept separate.

- Configuring secure interconnected services on different networks is a complex task. Advance approval must be obtained from PHSA.
- Designing and properly configuring patient data to ensure it is securely isolated on the PPN requires a highly skilled professional and must receive advance approval from PHSA.

Wireless Networks

Properly securing a wireless network in a clinical setting is complex, and the convenience of wireless introduces inherent risks when it is used to access personal health information. The default security settings of wireless systems may not be configured to industry best practices. If a clinic installs the wireless network solution with default settings still in place, there is potential for unauthorized users to access the clinic's local network and possibly obtain personal health information.

When installing a wireless network, clinics should:

- Use "small office business class" wireless equipment that offers professional features, security standards, and support that are generally higher quality than consumer-grade home devices.
- Configure wireless solutions using industry best practices for networks in a highly secure environment. Wherever possible, this should include using radius authentication when permitting access to internal clinic networks.
- Be especially alert to vulnerabilities that may compromise wireless security. Have a plan to mitigate risks to personal health information and/ or provide contingencies (e.g., wired access), should they occur.

For current best practices to configure wireless security, reach out to the Doctors Technology Office at dtoinfo@doctorsofbc.ca

Keep in mind that wireless routers typically broadcast access well beyond the physical walls of the clinic, and present opportunities for unauthorized access that may not be easily detectable. Your clinic should hire qualified IT support vendors with extensive knowledge and experience in installing and supporting secure wireless solutions. Remember:

- Do not provide patients and visitors with Wi-Fi access to your clinic's network.
- Set up a separate wireless network that is isolated

from the clinic's primary local network.

- Avoid the use of public Wi-Fi connections to send information. If you must, use virtual private network (VPN) technology.

Wi-Fi access to the internal clinical local network should not be granted to patients or visitors.

Operating Systems

Security measures necessary for operating systems used in a clinic are simple—and important.

Ensure that all operating systems and all plugin software are up to date. Computer software manufacturers routinely provide security updates for their operating systems and Internet browser plug- ins, to ensure that security risks to their software are minimized.

Computers should be configured to:

- Automatically install these updates so that important security updates are not missed.
- Schedule the updates outside of normal business hours, as they can take time to install and would likely impact system performance until the installation is complete.
- Leave computer devices powered on and logged off at night, so the updates can be automatically installed (scheduled updates will not happen if the computer is in hibernation mode).
- Allow downloading and installation of software only by system administrators, in compliance with clinic security policies.

Access Control

All the safeguards described in this guide will be of little use if access to the system is not protected. Strong access control means implementing and enforcing policies and procedures for user access, password use and storage, login and logoff, considerations for remote access, and more.

Manage the Password System

Passwords are one of the most important tools for safeguarding personal health information. But passwords—like the information they are protecting— must themselves be secure. Please visit the Canadian Centre for Cyber Security's Best Practices for passphrases and passwords website for more information.

All staff members who have access to clinical systems should be provided with a unique user ID and temporary password, to be changed immediately upon receipt. Passwords should be easy to remember, but difficult for others to guess.

One or more individuals should be assigned to manage user accounts (e.g., the physician lead, clinic manager, privacy officer, or security lead) to govern user access. This requires that:

- All passwords are secure and robust.
- All users are assigned a unique username.
- Role-based access profiles are properly configured.
- All inactive accounts are disabled in a timely manner.

Keep passwords secure and robust

- Unauthorized access—due to passwords being easily guessed or poorly protected—presents a serious risk to the security of personal health information. Therefore:
    - Passwords must be strong ("complex").
    - If you need to write your password down for future reference, it should be done in a manner that protects its intended use and be kept in a safe location.

Do not use the "remember my password" and "auto fill" features in browsers that automatically insert your user ID/password and other personal identifiable information. Doing so may allow anyone at the workstation to access the application without being challenged to confirm their identity. In addition, the storage location of this information is known, so the complete file containing them can be easily stolen.

Passwords are commonly short strings (8-16 characters) mixing letters, numbers and symbols. However, short passwords – even with complexity – are vulnerable to being cracked by brute force or guessed via common patterns. Examples like "Winter2025!" or "Hospital123" are too predictable and easily compromised.

Passphrases are longer sequences of words or characters, such as "PurpleGardenFishDance2025". They have several advantages:

- Easier to remember than complicated, random passwords.
- Much hard to crack due to length and unpredictability.
- More resistant to brute force and dictionary attacks.
- Recommended length is at least 13-10 characters; longer is better.
- Example passphrases: "MyCoffeeMugIsBlueInJune!" or "SunsetRunnersElkMapleTree"

Strong passwords can be difficult to create and even more difficult to remember.

Adopt FIDO Passkeys – The Future of Authentication

- Passkeys replace passwords with cryptographic keys stored securely on your device.
- Authentication is done via biometrics or device PINs – no password typing needed.
- Passkeys are immune to phishing and cannot be stolen from servers.
- Supported by major platforms and increasingly adopted in healthcare systems.
- Enables seamless, secure cross-device login experiences.

Avoid reusing the same password or a similar one

When a site is compromised, other sites of higher value (more important) may become compromised as well. Using similar passwords to remember multiple accounts is one of the most common reasons higher valued accounts are hacked.

If you must access dozens of web-enabled lower value and higher value accounts, a commercial password manager that automatically generates a very secure, unique password for each account is recommended. It will isolate every system in case one website has been compromised. This can reduce the chances of inadvertently using 'similar' passwords that could put valuable systems at risk.

If you choose to use a password manager to access web services hosting non-clinical data, the following is recommended:

- Use a commercial product.
- The security of a password manager is only as good as the strength of the master password/access control method used to access it. Select a product that allows you to configure the master password with two-factor authentication (see section below).
- Like any critically important application, use the commercial password manager only on computers that you have unique access to, which are not left logged in and unattended.

Keep usernames and passwords secure

Usernames that are uniquely identified with an individual should provide access through role-based profiles. The level of access for each user should match the user's information access requirements and provide the least privilege necessary based on the user's job function.

Sharing usernames and passwords between users is a security and privacy risk because:

- The person using the shared username immediately has access to the other person's role profile, with specific rights and privileges that may be unique to that person.
- Sharing passwords will circumvent the auditing process built into clinic computers, file servers, and EMR applications. This puts a person who was originally assigned a username and password at risk of being held responsible for the actions of another person who uses the first person's credentials.

Wherever possible use two-factor authentication

Protecting systems containing confidential information can no longer rely on strong passwords alone. For this reason, many commercial web-enabled services—as well as clinic information systems and remote access to the Physician Private Network—provide two-factor authentication/multi-factor authentication(2FA/MFA) as an optional, more secure method to access an account.

When set up correctly, two-factor authentication has the potential to strengthen security, while reducing the requirements to maintain complex passwords that may still be compromised through malware, social engineering, etc.

Two-factor authentication, also known as two-step or multiple step verification, describes access that requires two distinct—or two levels of—authentications. (A login that requires a user ID and a password is considered single-factor authentication).

Remote access to clinical systems should always use Two-factor Authentication. See the section on Remote Access Control for more details.

To qualify as 2FA, two out of the three following factors are required before someone can gain access:

1. Something you know:

- Personal identification number (PIN)
- Password
- Physical movement pattern

2. Something you have:

- Phone/mobile phone
- ATM card
- Key fobs such as an RSA token or Yubico USB stick

3. Something you are:

- Voiceprint
- Fingerprint
- Retina scan

Any combination of two of these three is considered 2FA (e.g., a credit card with a pin/password plus fingerprint; login plus password plus RSA token).

Create Effective User Accounts on Clinic Systems

Besides maintaining a strong password system, access security must also consider user logins and implement other access policies. Follow these steps to secure access to user accounts on your clinic system:

- **Avoid using generic logins (e.g., MOA1, MOA2, PHYSICIAN1, PHYSICIAN2)**

  This action will negate information access monitoring measures and audits required to assess compliance with PIPA. To protect staff, each login ID on clinic computers and EMRs should uniquely identify users and should never be shared when new staff join the clinic. Use unique user IDs that clearly and exclusively identify individuals. This protects the person entering data from others using the same account. It may also help to determine the cause of the breach and what preventative actions to take for future reference.

- **Avoid using the administrator account on a routine, day-to-day basis**

Accounts with full administrator rights to desktops, servers, or EMRs should be limited. Instead, set up a basic user account for day-to-day requirements. This will limit the potential for damage, should a malicious application attempt to install itself onto the computer in the background, or make other inappropriate changes. It will also provide a necessary audit trail.

- **Assign rights through group-based roles**

  To provide consistent management, use consistent controls that are applied across the clinic domain.

- **Implement EMR role-based authentication**

  Assign access to clinic systems and EMR applications for each user using role-based profiles. Role-based profiles allow the administrator to consistently control what the end user can create, view, update, and delete.

In general, access to personal health information should be provided only on a "need to know" basis, as authorized by the piracy officer or other authority. For example, a scheduling clerk does not typically need access to full patient medical charts.

Disable Auto-Complete User ID/ Password Storage for Access

When accessing a website that requires a username and password for authentication, some Internet browsers (e.g., Internet Explorer, Firefox, Chrome) offer the option to automatically store the username and password for future use.

This auto-complete feature should be disabled, as it can compromise safeguards designed to protect personal health information:

- It provides what would otherwise have been secure authentication credentials to anyone using that computer to gain full access to confidential sites.

- If the end user has the same username and password to login to the EMR application and to a workstation, these credentials can be compromised by an unauthorized user using the same workstation.

- As some websites provide single sign-on to a suite of interconnected web applications, enabling the autocomplete feature may capture credentials that access a much wider range—and potentially more sensitive applications—than just the website that the browser feature originally used to capture the initial login.

In most web browsers, disabling the auto-complete password function can usually be found under an options menu. Users should be prevented from altering these settings.

Turn On Audit Trail

EMR applications have a user-level access auditing feature built in; however, this feature may not always be turned on, or if it is turned on, the clinic may not be actively reviewing the audit log.

Be sure this feature is turned on and actively reviewed by the clinic's privacy lead or delegate to monitor privacy and security of personal health information. At a minimum, the audit log captures which users have logged onto to the EMR, which patient records they have reviewed and/or printed, and which files have been modified or deleted.

Workstations may also have auditing features to monitor printing and file access on the user's device. If available, they should be turned on and periodically reviewed.

Monitor VIP Records

If your clinic has some VIP patients (e.g., political leaders, celebrities), the audit access to these records should be monitored and reviewed to ensure they are not being viewed by unauthorized users. The clinic security lead or their delegate should have a regularly scheduled process to review public figures' records with the privacy officer. They must provide alerts if any suspected anomalies are found.

Disable Inactive User Accounts

When an account becomes inactive, for example, in cases when an employee leaves the clinic, the account should be disabled immediately (see the section on terminations in the first section of this guide, Administrative Safeguards).

Workstation login accounts should be disabled using the operating system's administrator tools, and EMR login accounts should be disabled through the EMR application's built-in administrator tools. If necessary, contact the EMR vendor helpdesk for assistance.

Remote Access Control

Physicians frequently need to view personal health information from outside the clinic, such as from home or to support on-call coverage. This remote access carries its own security considerations.

If your clinic is on the PPN (Private Physician Network), online remote access to the EMR data centre using computers is most frequently provided through "tokens" issued by TELUS on behalf of BCCSS (BC Clinical and Support Services). These tokens use an encrypted SSL (secure sockets layer) virtual private network (VPN) tunnel with two-factor authentication (see below).

An exception to the use of TELUS is Med Access EMR, which uses web-based software with built-in remote access certificates. The PPN's security design requires the clinic to be accessed remotely through cloud- based remote-control applications, such as TeamViewer or LogMeIn, rather than other desktop applications.

Whether or not your clinic is on the PPN, you should use two-factor authentication as an additional security measure to access a remote system. For more information, see Manage the Password System.

APPENDIX A: RESOURCES

Doctors of BC

Doctors Technology Office

Doctors Technology Office (DTO) offers a comprehensive suite of health technology practice supports and resources to guide family physicians and practice teams through the technology landscape. We provide guidance on up-to-date technology solutions that are aligned with security best practices and are a troubleshooting resource when technology fails.

- General Information About Support Services

Privacy Office

To assist physicians in meeting their obligations under the Personal Information Protection Act (PIPA), Doctors of BC, the Office of the Information and Privacy Commissioner for BC, and the College of Physicians and Surgeons of BC partnered to update the BC Physician Privacy Toolkit: A guide for physicians in private practice, originally published in 2004, and subsequently updated in 2009 and 2017.

All forms referenced in this section are from the Doctors of BC Privacy Toolkit. Additional resources are available through the Doctors Technology Office.

Access and Correction of Personal Information

- Patient Request for Access to Personal Information
- Patient Request for Correction to Personal Information

Sample Confidentiality and Data-Sharing Agreements

- For Physician Office Employees
- For Third Parties
- For Health Authority Employees Working within a Physician Practice
- Data-Sharing Agreement

Consent

- Consent to Communicate Electronically
- Consent for Research

Certificate of Destruction

- To document the destruction of media containing personal information

Fax and Email Confidentiality Forms

- Email Disclaimer
- Fax Disclaimer

Other

- Responding to a Privacy Breach—Key Steps for Physicians
- Guidelines for Electronic Medical Records and Role-Based Access

Office of the Information Privacy and Commissioner for BC

Resources to help ensure clinics are prepared to respond, document, and where appropriate, report a breach. Additional guidance on responding to privacy breaches can be found in the Doctors of BC Privacy Toolkit (see section 12).

- A Guide to BC's Personal Information Protection Act
- Getting Accountability Right with a Privacy Management Program
- Privacy Breaches: Tools and Resources
- Mobile Devices: Tips for Security and Privacy
- Self-Assessment Tool for Organizations Designed for all businesses, this self-administered tool provided helps to identify current strengths and weaknesses in safeguards designed to protect personal health information.

College of Physicians and Surgeons of British Columbia (CPSBC)

- Standards and Guidelines
- Virtual Care
- Medical Records

Canadian Medical Protective Association (CMPA)

- Electronic Records—Tips to Improve Safety
- Electronic Records Handbook
- A matter of records: Retention and transfer of clinical records
- Encryption just makes sense

Other Resources

- Anti-malware/ Antivirus comparison sites

  AV-TEST | Antivirus & Security Software & AntiMalware Reviews

- Business Continuity and Disaster Planning Resources

  Doctors of BC - Business Pathways - Contingency Planning

  Emergency Preparedness for the General Practitioner in a Clinical Office

Practice Continuity Guide for Family Physicians

- General Clipboard Behavior and Security Risks

  Microsoft Support – Using the Clipboard (Windows 10/11)

  https://support.microsoft.com/en-ca/windows/using-the-clipboard-30375039-ce71-9fe4-5b30-21b7aab6b13f

  Microsoft Learn – Clipboard Overview for Win32 Applications

  https://learn.microsoft.com/en-ca/windows/win32/dataxchg/clipboard

- Windows-Specific Protections & Controls

  Disable Cloud Clipboard Sync (Settings Overview)

  https://support.microsoft.com/en-ca/windows/using-the-clipboard-30375039-ce71-9fe4-5b30-21b7aab6b13f

  Microsoft Learn – Per-User Services in Windows (Clipboard User Service)

  https://learn.microsoft.com/en-ca/windows/application-management/per-user-services-in-windows

  Configure Clipboard Redirection (Azure Virtual Desktop)

  https://learn.microsoft.com/en-ca/azure/virtual-desktop/redirection-configure-clipboard

- macOS Clipboard & Privacy

  Apple Platform Security Guide (search: clipboard or pasteboard)

  https://support.apple.com/en-ca/guide/security/welcome/web

  Apple Developer – NSPasteboard Documentation

  https://developer.apple.com/documentation/appkit/nspasteboard

APPENDIX B: GLOSSARY

Adware	Software, which can take the form of malware when designed with malicious intent, that displays or downloads unwanted advertising material while a user is online.
Authentication	A method designed to allow a computer application to verify credentials, usually in the form of a username and password for single-factor authentication, or a username and password plus a token for multi-factor authentication.
Breach, Privacy or Security	An action by an authorized or unauthorized user that results in a negative impact, or causes interruption, disclosure, unauthorized access, modification, destruction, or denial of service
Brute Force	A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). The software used is math-based and generates many consecutive guesses.
Business Continuity	The capability of the organization to continue the delivery of products or services at acceptable predefined levels following a disruptive incident.
Business Continuity Plan	The documentation of a predetermined set of instructions or procedures that describes how an organization's business functions will be sustained during and after a significant disruption.
BCCSS	BC Clinical and Support Services, the organization that manages the Physician Private Network: a private Wide Area Network (WAN) owned by the BC provincial government.
Compliance	The action of meeting requirements as set out in relevant laws, regulations, standards, ethical principles, codes of conduct, contractual agreements, or policies and procedures.
Confidentiality	The responsibility of an individual to safeguard the secrecy of data concerning another individual.
Cookies (website)	Small text files that are downloaded onto a user's computer while visiting a website and are stored either temporarily or permanently as a means for the site to recognize the user and keep track of their preferences.
Consent	Voluntary agreement by an individual or their legally authorized representative to allow collection, use, or disclosure of the individual's personal information.
Disclosure	Sharing, exposing, or providing access to information, including to another organization, to the third party or to the individual.
Disaster	A major incident that seriously interrupts, or is expected to interrupt, operations for 24 hours or more.
Disclosure of Information	The release of available personal information to a person other than the person the information concerns, or a person employed by or in the service of the party holding the information.
Disruption	An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).
Encryption	The process of encoding a message or information so that only authorized users can access it.
Email and Text Scams	A fraud in the form of an unsolicited email that claims the prospect of a bargain or something for nothing.

EMR	Electronic medical record: a system within a practice that enables a health care professional, such as a family physician, to record and store the information collected during a patient's visit instead of, or in addition to, a paper file. The EMR may also allow the physician to access personal health information from other electronic health record systems.
FIPPA	Freedom of Information and Protection of Privacy Act: Privacy legislation in British Columbia that governs how personal information is collected, used, disclosed, and protected by public bodies, including health authorities and the Ministry of Health.
Hardening	A process to reduce the surface of security vulnerabilities in the system, recognizing that its surface of vulnerability is larger when a system performs more functions. Designing and configuring hardened systems is based on the principle that single-function systems are more secure than a multi-purpose one.
Incident, Privacy or Security	An incident that includes a contravention of legislation, or the privacy and security policies or practices implemented by a clinic. This includes, but is not limited to, personal information agent agreements, data-sharing agreements, confidentiality and non-disclosure agreements, and agreements with third-party service providers. An incident may also be a suspected privacy or security breach.
Jailbreaking	A modification made by some iOS users to add a greater variety of features over what the manufacturer recommends. See also "rooting."
Macro	A set of programmed sequences that, in its simplest form, imitates keystrokes or mouse clicks to replace a repetitive series of actions. Macros, which can be executed within a word processing or spreadsheet application such as Word or Excel, may also perform a wider range of functions through Visual Basic and other programming applications. Although macros can be convenient, they have been used to perform malicious actions or install malware as soon as a document is loaded.
Mail and Wire Scams	Any scheme to intentionally deprive an individual of property or honest services using mail or wire communications.
Malware	Hostile or intrusive software, including computer viruses, worms, Trojans, ransomware, spyware, adware, scareware, and other malicious programs. Malware is defined by its malicious intent, acting against the requirements of the computer user.
Mobile Device	A portable device that provides computing, information storage, or retrieval capabilities for personal or business use (e.g., BlackBerry).
OIPC	Office of the Information and Privacy Commissioner for BC: an oversight body responsible for educating the public concerning their rights under privacy legislation and ensuring that organizations fulfill their obligations under privacy legislation. See the OIPC website for more information.
Personal Health Information	Information about an individual that is collected, used, or disclosed as part of a medical record for the purpose of delivering health services to that individual. In the E-Health Act, personal health information is defined as "recorded information about an identifiable individual that is related to the individual's health or the provision of health services to the individual."
Personal Information	Information, including personal health information, about an identifiable individual which includes factual or subjective information about that individual. This information includes, but is not limited to, name, personal address, birth date, physical description, medical history, gender, education, employment, and visual images such as photographs or videotapes.
PHSA	Provincial Health Services Authority (Contact ppnadminphsa.ca)
Phishing	Email fraud is intentionally designed to motivate an individual to volunteer personal information for criminal use or install malware on their computer.
PIPA	Personal Information Protection Act: BC's privacy legislation that governs how personal information is collected, used, disclosed, and protected by private sector organizations, including physicians' private practices and other private healthcare facilities.

Plug-ins	Software components that add a specific feature to an existing computer program, allowing it to be customized according to the user's needs. Examples are plug-ins used in web browsers to add new features such as virus scanners and preferred search engines.
Private Network	An end-to-end network that allows secure, high-speed access to an electronic medical record, secure Internet access, and secure email messaging.
PPN	The Physician Private Network: a private Wide Area Network (WAN) owned by the BC provincial government, and managed by BCCSS. The PPN is designed and monitored by TELUS and was built for the use of doctors who are using an application service provider application for electronic medical records.
Privacy Breach	An incident where there is unauthorized access to collection, use, disclosure, or disposal of personal information. Such activity is unauthorized if it occurs in contravention PIPA or Part 3 FIPPA.
Privacy Officer	The individual designated to be accountable for ensuring organizational compliance with privacy legislation, industry standards for privacy, and privacy-related professional and regulatory obligations. In a medical practice, one physician must be designated as the privacy officer. In a solo practice, the physician is the de facto privacy officer. The responsible physician may choose to delegate responsibilities for the privacy management program to an employee, but they remain ultimately responsible.
Radius Authentication	Remote Authentication Dial-In User Service is a networking protocol that provides centralized Triple A (Authentication, Authorization, and Accounting) management for users who connect and use a network service.
Ransomware	A type of malware that threatens to publish the victim's data or prevent access to it, by encryption, unless a ransom is paid.
Reasonable Security Measures	The measures taken to protect personal information from unauthorized collection, use, or disclosure by implementing physical, technical, and administrative controls. Factors to consider when implementing reasonable measures include the sensitivity of the personal information, the likelihood of a privacy breach, the harm caused if a breach occurred, the type of record involved, the cost of the security measures, and current industry standards.
Remote Access	The ability to access a computer or network from outside the practice.
Role-Based Access	Access privileges to a computer or network based on job functions rather than individual users. Users are granted privileges in accordance with the "need to know" and "least privilege" principles by virtue of being authorized to act in specific roles.
Rooting	A modification made by some Android users to add a greater variety of features over what the manufacturer recommends. See also "jailbreaking".
Security	Controls that protect personal information from unauthorized collection, use, or disclosure. Examples include locking cabinets, or in relation to electronic records, password protections, encryption, and firewalls. See also "Reasonable Security Measures".
Security of Information	The preservation of the confidentiality, integrity, and availability of personal information. Information security is achieved by implementing policies and procedures based on relevant legislation, standards and ethical principles, careful planning, design, implementation and maintenance of appropriate technology solutions, and managing ongoing operations related to the collection, classification, access, and disclosure of personal information.
Social Engineering	The art of manipulating people's willingness to be helpful and to give up confidential information. The social engineer/con artist appeals to vanity, authority, and greed or pretends to be some- one they are not to exploit a person's natural inclination to trust. Using social engineering techniques to obtain a user ID and password is a lot easier than the highly skilled and complicated hacking methods.

Spyware	A form of malware that is installed on a computer system without the knowledge of the owner and is designed to collect confidential information through logging keystrokes and other techniques, while hidden from the user.
Staff	May include employees, locum physicians, associates, visiting specialists, medical students, residents, physicians-in-training, contractors, and volunteers with whom you collect, use, or disclose personal information.
Strong Password	A password that is sufficiently long or random that it is producible only by the user who creates it. It is case sensitive and includes a random combination of alphanumeric characters and symbols.
Third Party	In the context of personal information that is controlled by a practice, anyone outside the practice or the individual the information is about.
Trojan	A form of malware that is designed to mislead users concerning its true intent. Unlike computer vi- ruses and worms, Trojans do not usually propagate themselves, but, analogous to the "Trojan horse" of ancient times, rely on users to allow them to enter a trusted environment by the practice or third party that collected the information for a specified purpose.
Two-Factor Authentication	The combination of username/password (something an authorized user knows), and some other physical identification tool like a secure ID token (something an authorized user has), which are both required to verify the identity of a person.
Use	Any operation (other than collection or disclosure) performed on or consisting of personal information by the practice or third party that collected the information for a specified purpose.
USB Memory Key	A compact data storage device that is typically removable and rewriteable. The most common use of USB memory keys is to transport and store files such as documents, pictures, and videos.
Whitelisting	A method of indexing approved software applications to permit them to be present and active on a computer system. Whitelisting is used to assist in protecting computers and networks from executing potentially harmful applications.
Virus	A form of malware that, in addition to having malicious effects, will replicate itself when executed by inserting its own code into other computer programs, and in some cases data files or the "boot" sector of the hard drive.
VPN	Virtual private network: an authentication and encryption method that allows connection from outside the practice to the EMR over the Internet with enhanced security.
Worm	A form of standalone malware that replicates itself to spread to other computers. Often it will use a computer network to spread by exploiting security failures on target computers. Unlike computer viruses, worms do not require other computer programs or humans to propagate.

115 - 1665 West Broadway
Vancouver BC V6J 5A4
doctorsofbc.ca
@doctorsofbc