E-health Privacy and Security Guide

Designed to help physicians comply with personal health information laws

Doctors Nova Scotia | January 2021

Contents

Expanded Contents

Introduction

THIS GUIDE WAS PREPARED BY DOCTORS NOVA SCOTIA as a resource for community-based physicians and their staff on the topics of e-health privacy and security. It was designed to help physicians and staff members comply with personal health information laws, including the Personal Health Information Act (PHIA) and the Personal Information Protection and Electronic Documents Act (PIPEDA). It offers guidance to ensure privacy and security safeguards are up to date and followed, and includes the latest recommendations for electronic medical records (EMRs) and integrated solution options.

The guide is divided into seven modules:

Module 1: Legislation outlines obligations under PHIA and PIPEDA regarding an individual's private information under the custody and control of community medical practices.

Module 2: Breach Response explains what a privacy breach is and how to respond to one by following four steps to contain, evaluate, notify and prevent a future breach.

Module 3: Security Basics explains what a cyberattack is, provides examples of cyberattacks and outlines the security concepts of confidentiality, integrity and availability.

Module 4: Safeguards outlines recommendations to protect physicians, staff members, devices and data from cyberattacks.

Module 5: Electronic Medical Records explains what an EMR is, the effect of privacy legislation on EMRs and the features of the Telus Med Access EMR and the QHR Technologies Accuro EMR.

Module 6: EMR-integrated Solutions defines virtual care and integrated solutions, and explores the features of the Telus MedDialog, Telus EMR Virtual Visit, Health Myself patient portal and Medeo Virtual Care solutions.

Module 7: Checklists and Templates provides descriptions and links to checklists and templates that correspond to the previous modules.

The resource materials provided in this guide are for general information purposes only. Physicians and staff members should adapt the materials to fit and reflect their community practice.

This guide is not intended as legal or professional advice or opinion. It is recommended that physicians and staff members seek legal or professional advice should concerns arise.

Doctors Nova Scotia thanks Emily Gaunce, juris doctor and master of health administration candidate 2021, for her work creating this guide and Doctors of BC for granting permission to use content from its *BC Physician Privacy Toolkit*.

Module 1:
Legislation

Personal Health Information Act

The Personal Health Information Act (PHIA) is the health-care privacy law in Nova Scotia. The act governs the collection, use, disclosure, retention, disposal and destruction of personal health information (PHI). The act recognizes that individuals have the right to the protection of their PHI. It also recognizes that custodians are needed to collect, use and disclose PHI to support individuals in the management of their health care.

Personal health information refers to any identifying information about an individual that relates to their physical and mental health, provisions of care they have received, their bodily donations, their health card number and their substitute decision-maker.

Custodians

The Personal Health Information Act defines "custodian" as an individual or organization who has custody or control of PHI as a result of their powers, duties or responsibilities. Examples of custodians include regulated health professionals (e.g., physicians, nurses), group practices of regulated professionals, a health authority and continuing-care facilities.

Duties

Section 67 of PHIA requires you, as a custodian, to appoint a contact person within your practice to be responsible for:

- Ensuring you comply with PHIA
- Ensuring agents are aware of their duties under PHIA
- Responding to questions regarding your practice's information practices
- Responding to requests for access to and correction of health records
- Receiving and processing complaints under PHIA
- Communicating to and training staff about information policies and procedures and PHIA
- Developing materials for patients about your practice's policies and procedures

You must put in place information practices and policies that meet the requirements of PHIA, are reasonable and ensure patients' PHI is protected. The information practices and policies describe the purpose for and method by which you collect, use, disclose and destroy PHI, and the administrative, technical and physical information safeguards employed within your practice.

You are also responsible for implementing and complying with a complaints policy that allows patients to make complaints under PHIA.

In your role as a custodian, you must make available to patients a privacy statement detailing the following information:

- The contact information for you or your designated PHIA contact person
- A description of your practice's information practices and policies
- A description of how a patient can access or make corrections to their PHI
- A description of how a patient can make a complaint under PHIA

Agents

Under PHIA, an "agent" is a person who, with the authorization of the custodian, may act on behalf of you in matters regarding PHI. Agents may include employees or volunteers of custodians.

Duties

Agents may collect, use and disclose patients' PHI if you, as the custodian, are allowed to perform these activities; agents may do so only for your established purpose.

Agents also have the responsibility of:

- Signing confidentiality agreements and contracts that you require under PHIA
- Informing you of any privacy and security breaches
- Ensuring PHI is retained and destroyed in compliance with PHIA

Consent

To collect, use or disclose an individual's PHI, as a custodian you must obtain the individual's knowledgeable implied consent or express consent, unless consent is not required by PHIA. Consent, whether implied or expressed, must be: given by the individual; knowledgeable; voluntary; and related to the specific information at issue.

You may accept an individual's knowledgeable implied consent, rather than express consent, if you can reasonably infer that the individual understands your purpose for collecting, using or disclosing their PHI. To do so, you must make available to your patients a notice explaining your purpose in a manner that is easily accessible, readable and understandable to them. For example, place the Notice of Purpose in visible locations throughout your community practice. See Module 7: Checklists and Templates for a Notice of Purpose template.

An individual may limit or revoke their consent for you to collect, use or disclose their PHI at any time by providing notice to the custodian. Once notified of an individual's request to limit or revoke their consent, you must take the necessary and reasonable steps to comply with the individual's request. It is also your responsibility to inform the individual of any consequences that may arise from limiting or revoking consent (e.g., you are no longer confident in providing adequate care without the limited or revoked information).

Disclosure

As a custodian, you may disclose an individual's PHI to another custodian within the individual's circle of care. You may only do so if the disclosure is deemed reasonable and necessary to the provision of health care to the individual.

You may disclose PHI to an individual's family members or persons with whom the individual has a close personal relationship. You may only do so if the information is about the individual's present condition, the information is in general terms and the disclosure is not against the wishes of the individual.

There are situations when you, the custodian, may disclose PHI without the consent of the individual. The following are examples of when disclosure without consent may occur:

- To prevent the commission of an offence, fraud or abuse
- To persons who are legally entitled to make health-care decisions for an individual (e.g., substitute decision-maker)
- To the regulatory body of a health profession in order to perform their duties
- To any person if disclosure will prevent or diminish imminent and significant danger to another person
- To an office of a correctional facility in which the individual is lawfully detained
- To another custodian for the purpose of maintaining quality and standards of care
- To another custodian for the purpose of determining an individual's eligibility for insurance
- To assess risk management and maintain patient safety within the custodian's practice

You may disclose the PHI of an individual who is deceased, or believed to be deceased, to the individual's family member(s) or another person who has a close personal relationship with the individual, for the purposes of:

- Identifying the individual
- Informing the necessary people of the individual's death
- Informing the health care of the individual's spouse, parent, sibling or child
- Executing the wishes of the individual regarding organ or tissue donation

Retention and Destruction

The Canadian Medical Protection Association recommends that you, as a custodian, retain health records for at least 10 years from the last date of entry or, for minors, 10 years from when they reached the age of majority. You are required to create a written retention schedule for the PHI at your practice.

Once the retention period expires, PHI must be securely destroyed, erased or de-identified. "Securely destroyed" means to destroy the PHI so that reconstruction of the information is not reasonably possible (e.g., shredding paper records, wiping hard drives). "De-identification" refers to removing all identifiers from the PHI that could identify an individual.

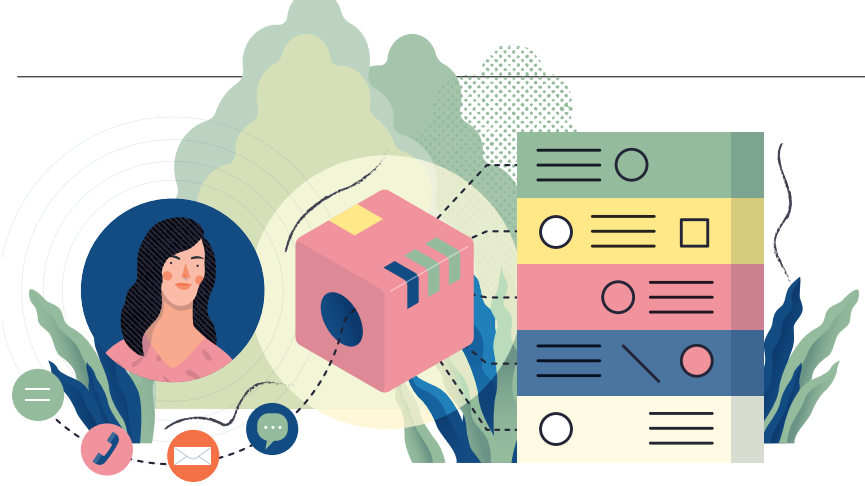
Access and Correction

Every individual has the right to access their health record that is in your custody or under your control as the custodian. Individuals must submit their requests to you in writing and pay a fee for access. Except in very limited circumstances (see below), you will grant the individual access to their health record as soon as possible.

However, you may refuse an individual access to their health record if you reasonably believe any of the following:

- The record is subject to legal privilege (i.e., contains legal advice)
- Another law prohibits or protects the record from disclosure
- The record was created for the purpose of ensuring quality and standards of care at your practice
- The record is part of an ongoing inspection, investigation or proceeding authorized by law
- Accessing the record could result in a risk of serious harm to the treatment, recovery, mental or physical health of the individual
- Accessing the record could result in a risk of serious harm to the mental or physical health of another individual
- The record contains information provided by a third-party in confidence to you as the custodian
- Accessing the record could result in the release of another individual's PHI
- The request is deemed to be frivolous, vexatious or amounting to an abuse of the right of access

If you refuse access, you must provide the individual with a written explanation of your refusal and inform the individual they are entitled to make a complaint to the Office of the Information and Privacy Commissioner for Nova Scotia about the refusal.



Personal Information Protection and Electronic Documents Act

The Personal Information Protection and Electronic Documents Act (PIPEDA) is federal privacy law, applicable in Nova Scotia, that governs the collection, use and disclosure of personal information by private sector organizations. Like PHIA, PIPEDA recognizes that individuals have the right to the protection of their personal information and that there is a need for organizations to responsibly collect, use and disclose personal information in reasonable and appropriate circumstances.

Personal information refers to any information that identifies an individual, but does not include the name, title or business address or telephone number of an employee of an organization.

The main difference between PHIA and PIPEDA is that while both create obligations concerning personal information, PHIA is specific to personal information in the context of health care.

Your Practice as Custodian

Under PIPEDA, an organization such as a community medical practice acts as the custodian of an individual's personal information.

It is your and your practice's responsibility to protect personal information by following these 10 principles:

1. **Accountability**: Your practice is responsible for all personal information under its control; therefore, you must designate an individual as being accountable for your practice's compliance with PIPEDA principles (e.g., implementing policies and practices giving effect to the principles).
2. **Identifying Purpose**: At or before the time of collection, you must identify the purpose for which your organization is collecting individuals' personal information.
3. **Consent**: You must have the knowledge and consent of individuals for you to collect, use or disclose their personal information.
4. **Limiting Collection**: You must limit the personal information you collect from individuals to only the information necessary to fulfill your organization's purpose.
5. **Limiting Use, Disclosure and Retention**: You may not use and disclose personal information for reasons other than your identified purpose and you may not retain personal information for longer than is necessary to achieve your purpose.
6. **Accuracy**: The personal information you collect must be accurate, complete and up to date, but not beyond the purpose for which you collect the information.
7. **Safeguards**: You must have in place security safeguards that will protect the personal information.
8. **Openness**: As an organization, you will make available upon request your personal information protection policies and practices.
9. **Individual Access**: Upon request, you must inform individuals of the use and disclosure of their personal information by your organization; you must give them access to their information; and, you must allow individuals to challenge or amend the accuracy and completeness of their personal information.
10. **Challenging Compliance**: You must allow individuals to challenge your organization's compliance with and accountability to PIPEDA principles.

Consent

To collect, use or disclose an individual's personal information, as an organization your practice must obtain the individual's consent.

Your practice must make known to the individual the nature, consequence and purpose for which you are collecting, using or disclosing their personal information. In other words, you require the individual's full knowledge and consent.

Obtaining express consent is ideal when dealing with sensitive information (e.g., banking information), while implied consent may be appropriate for less sensitive information (e.g., name, address).

An individual may withdraw their consent at any time. Your practice is responsible for informing the individual of the consequences that may arise from withdrawing.

Disclosure

Your practice may not disclose personal information for anything other than your original purpose for collection, use and disclosure.

There are exceptions that allow your practice to disclose personal information without the individual's consent, such as:

- To identify an individual who is injured, ill or deceased
- To inform of an emergency that threatens the life, health or security of the individual or another person
- To assess, process or settle an insurance claim
- To comply with a subpoena, warrant or order made by a court, person or body with jurisdiction to demand the information
- To a government institution with lawful authority to obtain the information due to national security, defence of Canada, enforcing and administering Canadian laws, contacting and communicating with the next of kin or representative of the individual

Retention and Destruction

You practice is required to create and implement guidelines and procedures for the retention of personal information, including minimum and maximum retention periods, and for the destruction of person information.

When your organization no longer requires an individual's personal information for the purpose(s) for which the information was originally sought, your practice is responsible for destroying, erasing or de-identifying the personal information.

Access and Correction

When an individual requests access to their personal information held by your organization, your practice is obliged to provide the individual with access. Your practice is responsible for responding to the individual's request within a reasonable timeframe with minimal cost to the individual. Your organization will ensure the personal information requested is readable and understandable (e.g., explanations are provided for abbreviations or code).

Should an individual identify that a correction of their personal information is required, your practice must amend the information through the revision, deletion or addition of information.

Your practice may refuse to provide an individual their personal information if to do so would be to reveal personal information about a third party. Your organization may also refuse if providing the information could threaten the life or security of another person.

Module 2:
Breach Response

OBLIGATIONS
in legislation

Physicians and staff members within your practice must comply with legislation that imposes an obligation to protect the privacy of:

- Personal health information – the Nova Scotia Personal Health Information Act (PHIA)
- Personal information – the federal Personal Information Protection and Electronic Documents Act (PIPEDA)

For the purposes of this module, personal health information and personal information will be referred to collectively as "private information."

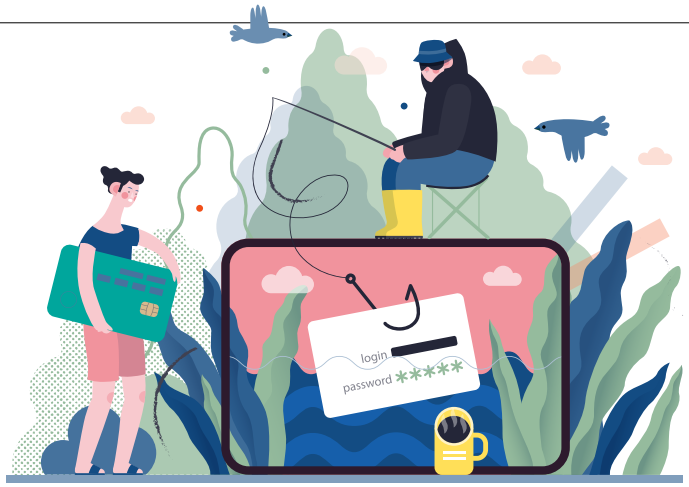
What is a Privacy Breach?

A privacy breach or a breach of security safeguards occurs when there is intentional or unintentional access, collection, storage, use, copy, disclosure, modification, loss or disposal of private information without authorization. Such an act is unauthorized if it contravenes PHIA and/or PIPEDA and requires a prompt and well-organized response.

Privacy breaches take many different forms, from misdirected faxes containing personal health information, to the loss of hard drives containing personal information, to medical files blowing out the back of a garbage truck.

The following are further examples of common types of breaches:

- Sending private information to the wrong person
- Sharing your password(s)
- Looking through files or database systems at private information that you do not need to know
- Not verifying a person's identify before disclosing private information
- Leaving office doors or cabinets unlocked, or not logging off computers
- Theft or loss of equipment or a device containing private information



How to Respond to a Privacy Breach

There are four key steps to respond to a privacy breach: contain, evaluate, notify and prevent. The first three steps should be undertaken immediately upon discovery of the breach or in very quick succession. The fourth step should be undertaken once the causes of the breach are known, in an effort to find longer-term solutions to the identified problem.

At each step of the breach response, you should document all relevant information.

See page 29 for breach response tools.

1

Step 1: Contain

If you suspect a privacy breach has occurred, as the responding custodian or agent you should conduct an initial assessment of the situation which may include considering the following questions:

- Did the unauthorized use, collection or disclosure of private information occur?
- Does private information continue to be at risk?
- Is there a possible violation of policy or law?

If the answer to any of the above questions is yes, then a privacy breach has occurred.

Once you have determined that a privacy breach has occurred, you should contain the breach to prevent further unauthorized access, collection, use or disclosure of the private information. The following actions should be undertaken to contain a privacy breach:

- Isolate or suspend the unauthorized activity that led to the privacy breach. This may involve shutting down the system that was breached
- Recover the private information, records or equipment that were breached
- If copies of the private information have been made, recover and/or destroy the copies
- If private information was sent to the wrong person, call the recipient and ask them to securely destroy any electronic copies or printouts of the private information
- If an unauthorized person has access to private information, disable or suspend their account, revoke computer access codes and/or change passwords
- Notify law enforcement if the privacy breach involves theft or criminal activity
- Do not compromise evidence to be used in breach investigation and correction

2

Step 2: Evaluate

Once the privacy breach has been contained, the responding custodian, agent or privacy officer within your practice should conduct an investigation of the breach. The investigation can also take place as a team effort. During the investigation, document all evidence and information pertaining to the breach.

The purpose of the investigation is to: determine the cause and extent of the breach; determine potential harms; identify who should be notified of the breach; and ensure the breach has been contained properly.

To inform your investigation, consider the following questions:

Personal Health Information Involved

- What private information was breached? How sensitive is the information?
- In what format was the private information (e.g., electronic, paper)?
- How was the private information protected (e.g., password, encrypted)?

Cause and Extent

- What was the cause of the breach? Was private information lost or stolen?
- What is the extent/scope of the breach?
- Is there a risk of further exposure, is the breach a systemic problem or was the breach an isolated incident?
- Have you recovered the breached private information?

Individuals Affected

- Who is affected by the breach (e.g., patients, employees, practitioners, other organizations, the public)?
- How many individuals are affected by the breach?

Potential and Foreseeable Harm

- What are the consequences of the breach toward those affected (e.g., security risk, identify theft, humiliation, relational harm, loss of trust)?
- What steps have you taken to minimize the harm to individuals?

If you are not sure how to evaluate the risk of a breach, check out the Risk Rating Overview Chart on page 6 in Key Steps to Responding to Privacy Breaches. Find this and other breach response tools listed on page 29.

3

Step 3: Notify

Who, When and How to Notify

As the responding custodian or agent, it is your responsibility to determine who must be notified of the breach, whether it be some or all of the following people:

- Individual(s) whose private information was breached
- Primary physician of affected patients
- Office of the Information and Privacy Commissioner for Nova Scotia (OIPC)
- Professional regulatory bodies, insurers or law enforcement

When making this decision, you must consider the private information involved, the cause and extent, the individuals affected, and the potential and foreseeable harms. You should also take into consideration contractual obligations, risks (e.g., fraud, theft, hurt, humiliation), the effect on your practice (e.g., loss of confidence) and legislative requirements.

The Personal Health Information Act (PHIA) and the Personal Information

3 continued

Protection and Electronic Documents Act (PIPEDA) provide guidance on whom you should notify:

- Sections 69 of PHIA and 10.1 of PIPEDA require that you notify the affected individual(s) immediately if it is determined that the breach:
  - o Has the potential to cause the individual harm or embarrassment (PHIA)
  - o Creates a real risk of significant harm to an individual (PIPEDA)
- Section 70 of PHIA states that custodians may use their discretion to notify the affected individual(s) if they determine:
  - o It is unlikely a breached has occurred; or
  - o There was a breach, but under the circumstances there is no potential for harm or embarrassment to those affected. In this instance, you are required to notify the OIPC of the breach
- Section 10.1 of PIPEDA requires you to notify the OIPC of any breach

Prompt notification allows individuals to enact measures to protect themselves against the harms of the privacy breach. Provide direct notification to those affected by phone, in person, by email or by mail. Provide indirect notification, such as posting on your website or by press release, only when those affected by the breach are unknown, the breach has affected a large number of individuals or when direct notification could cause further harm.

What Should be Included in the Notification?

When informing affected individuals and/or the OIPC of a privacy and security breach, your notification must include the following information:

- Date of the breach
- Description of the cause and extent of the breach
- Description of the private information breached
- Protentional and/or foreseeable harm to the individual
- Measures taken to contain the breach and reduce its harm
- Steps the individual can take to protect themselves from harm
- Measures taken to prevent future breaches
- Contact information of a person within your practice who can answer questions and provide further information
- Contact information for the OIPC, noting that individuals have the right to submit complaints to the OIPC

4

Step 4: Prevent

Once you have completed the contain, evaluate and notify steps, a more thorough investigation of the cause of the breach should be conducted by the responding custodian or agent, or the most appropriate individual within the practice, such as the privacy officer.

A thorough investigation of the breach's cause involves performing an audit of all physical, technical, administrative and personal privacy controls and security safeguards within your practice.

It is important to implement recommendations and changes stemming from the investigation, of which the following may be examples:

- Updating controls and safeguards where necessary
- Reviewing your practice's privacy and security obligations under PHIA and PIPEDA
- Reviewing and updating your practice's privacy and security policies
- Developing a privacy breach protocol for your practice (if not already in place)
- Retraining all staff members on their privacy and security obligations

Finally, in accordance with section 10 of the Personal Health Information Regulations (PHIA Regulations), as a custodian you are required to maintain a record of every privacy and security breach that posed a risk to a patient's private information. This record must also detail corrective measures you have taken to prevent future breaches.

Module 3:
Security Basics

What is Cybersecurity?

Cybersecurity is the processes and techniques involved in protecting sensitive data, computer systems, networks and software applications from cyberattacks.

"Cyberattack" is a general term that covers a broad range of topics, including:

- Accessing sensitive information via unauthorized access to networks and systems
- Tampering with systems and data stored within them
- Disrupting the normal functioning of businesses and practices
- Locking users out of their systems with the intent of extortion
- Exploiting resources

With cyberattacks becoming more sophisticated and inventive, it's important to understand and mitigate the risks.

Types of Attacks

The first step is understanding the types of threats and attacks.

Phishing

Phishing is the most common form of cyberattack. It occurs when a cybercriminal sends spam emails that imitate a legitimate source. The emails have strong subject lines with attachments such as invoices or job offers, or may appear to be important emails from officials in an organization. They trick victims into compromising the security of their organization by revealing login credentials, credit card numbers, bank account information and other sensitive information.

Social Engineering

Social engineering is an attack where hackers use fake advertisements, prize offers or similar lures to trick victims into providing personal information and bank account information. The information is then cloned and used for crimes like financial fraud and identity theft.

Ransomware

Ransomware is a software program that uses a unique, robust encryption algorithm to block access or lock files on the targeted system. Hackers generate a unique decryption key that is saved on a remote server that prevents victims from accessing their files. They then demand a ransom to provide the key or to decrypt (or unlock) the data. Paying the ransom may not result in recovering the data.

Botnet Attacks

Botnets are a network or group of devices connected on the same network to execute a task. Hackers attempt to access the network and plant malicious code or malware to stop the network from working. Botnet attacks include being locked out from computers or systems (temporarily or indefinitely), spreading spam emails or stealing confidential data.

Cybersecurity and COVID-19

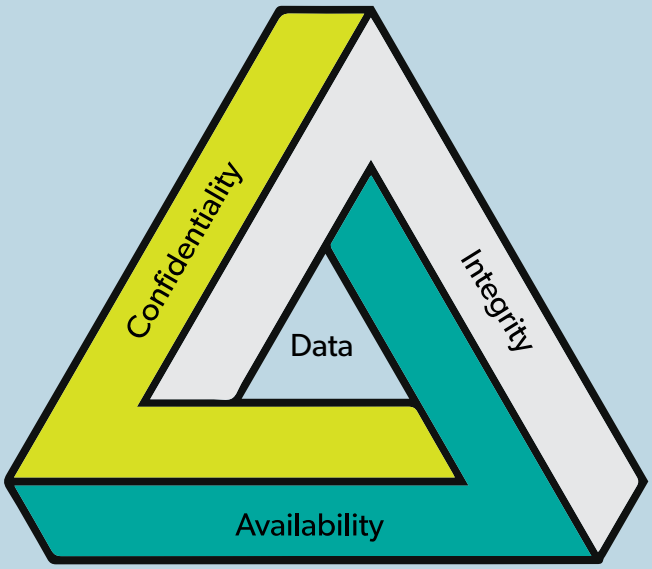
Cybercriminals are taking advantage of the COVID-19 pandemic to engage in an increasing volume of malicious cyber activities. Since January 2020, they have been using COVID-19 related content to trick victims into opening links and attachments. Examples of the false content include local and regional public health updates, access to cures and treatments, and access to needed medical supplies. Cybercriminals have also been using brands, logos and styles of legitimate health organizations and agencies to gain trust from victims.

The following are examples of known COVID-19 cyberattacks:

- In March 2020, phishing emails impersonated the Public Health Agency of Canada's medical officer of health. The emails delivered malware through an attachment
- In April 2020, phishing text messages impersonated the Canadian Emergency Response Benefit. The messages told victims they could access the benefit by divulging their personal financial details

It is expected that the number of COVID-19 related cyberattacks will continue to rise with the health sector as a target. These attacks will have negative effects on patient care, privacy, health-care providers, research facilities and medical manufacturers.

Physicians and staff members must take all precautions to prevent future cyberattacks.



Key Considerations

Cybersecurity is based on three fundamental concepts: confidentiality, integrity and availability. This is known as the "CIA triad"

Confidentiality

Confidentiality refers to methods used to protect private information. This concept requires defining and enforcing access levels for information. This can be done in a variety of ways, including:

- Developing an access control list
- Using file encryptions and file permissions
- Separating information into various segments organized by who needs access and the sensitivity of the information

Integrity

Integrity is an essential component of the CIA triad. Integrity means protecting data from deletion or modification by unauthorized parties and ensuring the ability to reverse any unauthorized changes.

Availability

This concept refers to the availability of your data. Access channels, authentication mechanisms and systems all must work properly to ensure the data they protect is available when needed. This means all necessary components like hardware, software, networks, devices and security equipment should be maintained regularly.

Risks

The following are examples of the possible consequences cyberattacks may have on you and your practice:

- A phishing attack resulting in identity fraud and theft
- A ransomware attack resulting in data and/or financial loss and reputational damage
- A breach of PHIA and PIPEDA legislation resulting in legal consequences

Module 4:
Safeguards

Protect Yourself

There are several steps you can take to safeguard your systems and data. The following is not an exhaustive list but provides key steps to use as a starting point. For a more comprehensive look at infrastructure changes you can make in your practice, refer to the Doctors of BC Physician Office IT Security Guide.

Password Protection

Passwords are one of the most important safeguards for confidential personal health information (PHI) and other personal information and sensitive data. Password best practices dictate that all practice physicians and staff members who have access to clinical and operational systems should be provided with a unique user ID and temporary password. Upon receipt, temporary passwords should be changed to ensure they are easy to remember but also secure, robust and difficult to guess.

One or more individuals (e.g., physician lead, clinic manager, privacy officer, security lead) should be assigned to manage practice user accounts and govern user access. The designated individuals should periodically audit user accounts and profiles to ensure access is appropriate and up to date. They should also ensure profiles are properly configured and that all inactive accounts are disabled within a reasonable amount of time.

Secure and Robust Passwords

Unauthorized access is a serious risk to the security of PHI and other sensitive information on devices in your practice. Passwords must be strong and complex. The following is a guideline for creating a good password:

- Has a minimum of eight characters
- Contains uppercase characters (A to Z)
- Contains lowercase characters (a to z)
- Contains numerals (0 to 9)
- Contains non-alphanumeric keyboard symbols (!, $, #, %)

When creating a strong password, remember the following:

- Longer passwords are better
- Avoid using words found in the dictionary
- Avoid replacing letters with special characters and numbers (e.g., replacing s with $ or e with 3)
- Avoid reusing the same or similar passwords on other sites
- Avoid writing down passwords. If you must write down a password, keep it in a safe and secure location

If you have access to multiple web-based accounts, it is recommended that you use a commercial password manager. The password manager generates secure and unique passwords for each account which reduces the chance of your accounts and systems being compromised. If you chose to use a password manager to access web-based accounts, consider these recommendations:

- Use a commercial product. Doctors Nova Scotia members

can use a one-time only promo code, "TTWWRR30," for 30% off personal and family plans with Keeper Security
- Ensure the password manager allows you to configure the master password with multi-factor authentication and use the guidelines above to create the password
- Use the password manager on computers that only you and your staff members have access to within your practice

Secure Usernames

Usernames should be uniquely identified and attributed to one individual within your practice. The level of system access for each physician and staff member should match the information access requirement of their role (e.g., the least access privilege necessary for their duties).

Sharing usernames and passwords between practice users is a security and privacy risk for the following reasons:

- The individual using a shared username and password has access to another individual's profile with the specific privileges granted to that individual
- The individual who was originally assigned a unique username and password is at risk of being held responsible for the actions of anyone else who uses their credentials

Multi-factor Authentication

Multi-factor authentication (MFA) adds another layer of account security. It supplements your username and password with another factor that only you can access. Whenever possible, protect yourself with the extra layer of security that MFA provides.

What is MFA?

Multi-factor authentication uses two or more independent factors to identify a user requesting access to an application or service. Two-factor authentication is the most common form of MFA. It pairs your first authentication factor, which is something you know (like your password), with a second different type of factor, such as something you have or something you are.

Types of authentication factors are as follows:

Something you know	Something you have	Something you are
Password	Smartphone	Fingerprint
Personal identification number (PIN)	Token	Retinal scan
Security question	Smart card/ID badge	Voice pattern

If one of your MFA factors is compromised, this will not allow hackers to access your account. In other words, if your password is stolen or your phone is lost, the chances of someone else having your second-factor information is highly unlikely. Note that using a password in combination with a PIN is not considered two-factor authentication because both pieces of information come from the same factor category: something you know.

How Does MFA Work?

When MFA is activated on your account, each time you log in from a different device, you will be sent an authorization check. Depending on the application or how you configured the MFA, the authorization check can be sent in a variety of ways: as a passcode sent to your associated email account or a text message sent to your smartphone. You must enter the code prior to receiving access to your account. Without the code or approval, a hacker cannot gain access to your account.

Why Use MFA?

Data breaches are alarmingly frequent and affect millions of people. The stolen information typically includes usernames and passwords that can give cybercriminals access to user accounts. Weak passwords alone can easily be guessed and even strong ones can be compromised through phishing or hacking. As more personal information is stored in online applications, an increase in privacy breaches and identity thefts is a concern.

It is recommended to use MFA whenever possible to neutralize the risks associated with compromised passwords by adding an additional layer of security to protect sensitive information. If a password is hacked, guessed or phished, a hacker would still need the required second factor to access the account, making the stolen password alone useless.

Risks of MFA

While MFA does provide added security, it is not a perfect solution. It is most often exploited through social engineering. For example, a hacker does not need to compromise your MFA security if they can call a support line, pose as you, and reset your password. Or if malware on your phone intercepts your text messages, such as a one-time passcode, and sends the message directly to the hacker.

To mitigate the risks of social engineering, establish a security PIN or password for your account. The PIN or password will be requested by the telecom provider when any type of change or service is requested over the phone or in person.

Protect Your Devices

Keep Software and Hardware Up to Date

One of the easiest ways to protect yourself and your data is to keep your software and hardware up to date. Cyberattacks take advantage of software vulnerabilities in common applications (e.g., operating systems, browsers) that need regular updates to be safe and stable. Applying software updates in a timely manner is an essential step you can take to protect your information.

Software updates make your experience better and ensure you get the most out of your technology. In addition to security fixes, software updates can include the upgrade or removal of features, improved compatibility with different devices or applications, and improved stability. It is important to prevent cyberattacks by upgrading and/or replacing software that no longer receives updates from the manufacturer.

There are financial considerations to upgrading the hardware you use in your practice (e.g., computers, printers, networks). However, there are also costs with keeping old and outdated hardware. As devices age, they become prone to problems, their speed and resources cannot keep up with application updates, and they become less likely to work with newer applications.

The following upgrades are recommended for the hardware in your practice:

- Laptops, Desktops, Tablets and Other Devices: Purchase a comprehensive three-to five-year warranty for your devices and replace them when the warranty expires. Having up-to-date devices allows you to leverage the most current technology, making you less at risk for attacks
- Local Area Network (LAN) Infrastructure: Update firmware periodically, but otherwise replace every 10 to 15 years
- Wireless Area Network (WLAN) Infrastructures: These should be replaced as often as every two to three years

Use Anti-virus and Anti-malware Software

Using robust anti-virus and anti-malware software is critical in today's environment. Anti-virus software detects and disarms viruses, and then removes them from your computer before they interfere with your systems. Anti-malware software works in the same way as anti-virus software, but also targets other malicious software, including ransomware, worms and Trojan horses. Update your anti-virus and anti-malware software regularly to ensure they continue to recognize the evolving viruses and malware created by cybercriminals.

Use a Firewall

Firewalls are another recommended safeguard to enable or install on your practice's desktop computers and laptops. Your computer's operating system typically comes with its own firewall software. Ensure this program is turned on and set to a high-security threshold to protect against unauthorized access. You should also consider purchasing a commercial firewall software (e.g., Bitdefender, Webroot, ZoneAlarm, Baracuda). Once purchased, the program should be configured to the highest security setting that is best for your practice.

Protect and Segregate Devices and Equipment

To protect the personal health information (PHI) stored on the devices and equipment in your clinic, follow these recommendations:

- Segregate and secure your mobiles devices, digital audio recorders, cameras and any other portable equipment (do not store them all in the same place)
- Enable PIN passwords and encryption on all devices
- Back up your devices regularly and keep the back-ups in a safe location
- Know how to remotely wipe PHI from your equipment
- Only use apps from trusted sources
- Be careful when using public wireless networks (Wi-Fi)

Protect Your Data

What is Data Transmission?

Data transmission is sending, receiving and transferring data between two or more devices. For example, your tablet sending a patient's test result file to the desktop computer at your practice.

When is Data Vulnerable?

Your role as a custodian is to protect the PHI within your care. However, that data can be made vulnerable, or more likely to be breached, when it is shared or transferred. For example, you could send a patient's PHI to the wrong health-care provider if the email address is misspelled or the fax number is inputted incorrectly. It is therefore important to have measures in place to help send, receive and transfer data safely and securely.

Share Data Securely

The following are various methods you can use to share data securely.

Email Encryption

Email encryption involves disguising the content of your email to prevent unintended recipients from accessing sensitive information. Even if someone intentionally intercepted your email, its contents would be unreadable without a passcode. It is recommended that you consistently encrypt emails containing PHI and other sensitive data to reduce the chances of a privacy breach.

Secure File Sharing

Secure file sharing allows you to share your files confidentially with other health-care providers or health organizations. You encrypt the file before sharing and the file can only be decrypted with a passcode. Encrypted files can be shared through an internet connection, local network or private network. When you share a secure file, you can also restrict access to the file, meaning recipients can be limited to view only or unwritable versions of the file.

Sneakernet

Sneakernet refers to the transfer of data between computers by removable, physical devices (e.g., USBs, hard drives). Using this method avoids transferring secure data over a network that can be hacked or breached. As an added security measure, you are typically able to password-protect and/or encrypt these devices.

File Permissions

When sharing a file with sensitive data, you are able to set and manage the file's permissions for individuals accessing the information. You may grant full control permissions which allows others to read, write, delete, edit file permissions and take ownership of the file. You can also limit a file's permissions to change (read, write, delete) or read only.

Disaster Recovery

Disaster recovery refers to the policies and procedures created and implemented to protect your practice from cyberattacks or device failures. You should develop policies and procedures that address preventive, corrective and detective strategies for if or when data is breached or lost (e.g., hardware, application and data restoration).

Monitor Access

Monitoring how and when your practice's system is accessed is important to protecting the data within your custody. Monitoring involves observing, identifying and reporting on the access activities within your practice. The goal is to detect unusual or unauthorized internal or external activity in order to protect PHI and prevent future breaches.

When protecting yourself, your devices and your data there are many considerations of which you must be aware. If you have questions, reach out to vendors from whom you have purchased tools or services, or to the e-health advisor at Doctors Nova Scotia:

- Brent Andrews, E-health advisor: brent.andrews@doctorsns.com

Module 5:
Electronic Medical Records

What is an EMR?

An electronic medical record (EMR) is a practice-based computer application that facilitates the long-term collection of personal health information (PHI) from patients in digital format. The majority of EMR users in Nova Scotia are community-based physicians, with more than 1,200 physicians using an EMR in their practice.

EMRs and PHIA

Personal health information contained within EMRs is subject to the Personal Health Information Act (PHIA). As outlined in Module 1: Legislation, physicians who have custody and control over PHI are deemed to be custodians of the information. As a custodian who maintains an EMR, you are obliged to implement electronic information system safeguards within your practice:

- Protect your network's infrastructure, including physical and wireless networks (Wi-Fi), to ensure secure system access
- Protect your hardware and its supporting operating systems to ensure the system functions consistently and only authorized persons have access to the system
- Protect your system's software (e.g., mandating user identity authentication before allowing access)

You must create and maintain policies that support the enforcement and implementation of the above listed safeguards. You must also maintain a record of every security breach of your EMR system and the corrective measures you have taken to prevent future privacy and security breaches.

The following two EMRs are approved by the Nova Scotia Department of Health and Wellness:

Med Access EMR

Med Access is a web-based EMR that is customizable and adaptable to your practice's clinic, user and workflow preferences and needs. It is owned, marketed and supported by Telus Health Solutions Inc.

The following are features of Med Access:

- Informed Patient Care: View patient history and data on a single screen; use interactive graphs and flow sheets to track testing; review lab results; monitor patient trends
- Better Patient Outcomes: Set individual and population patient health goals; engage patients in self-care
- Workflow Efficiency: Dashboards and encounter templates increase your practice's workflow speed and minimize data entry
- Remote EMR Access and Connection: Web-based platform allows you to access and connect to your EMR (e.g., patient records, clinic information) from anywhere you have an internet connection, whether at the clinic or on the go
- Clinic Operations Management: Flexible appointment scheduling, streamlined billing, electronic prescriptions, referral management
- Continuous Support: Customizable training, ongoing support from Telus and EMR user learning sessions

Considerations for Custodians

When implementing Med Access into your practice as a custodian, consider the following best practices:

Limiting Collection

- Define and document the purpose(s) for which you are collecting personal health information (PHI)
- Ensure staff members at your practice are knowledgeable of the purpose for collecting PHI and can clearly explain the purpose to patients
- Determine which available EMR information fields are necessary for the provision of health care
- Ensure staff members at your practice are trained on what gathered information is necessary for the provision of health care
- Gather only the information deemed necessary for the provision of health care

Limiting Use

- Capture the minimum amount of PHI in notes and alerts
- When creating, editing and running reports, only use identifying PHI when necessary (e.g., create aggregate reports when possible)
- Limit who can create, edit and run reports to those staff members who require access to complete their duties
- Develop a policy for your practice on accessing and using EMR reports (e.g., safeguards that must be in place, using an encrypted USB)

Limiting Disclosure

- Disclose only the minimum amount of PHI for health-care purposes
- Ensure the amount of PHI disclosed is appropriately limited (e.g., for MSI, disclose only the PHI required for claims administration purposes)

Sources and Accuracy of PHI

- Use EMR templates to reduce manual data entry errors
- Regularly verify and updated patients' PHI in your EMR to ensure accuracy and completeness
- Document what PHI was removed or added to a patient's chart when merging or unmerging patient charts
- Document the identity of a substitute decision-maker under the appropriate patient's chart
- Ensure your health-care provider address book is up to date to prevent unauthorized PHI disclosure
- Confirm changes to existing claims to ensure PHI are accurate and complete before submitting to MSI

Consent

- Ensure a common method of documenting consent within your EMR is practised by all staff members
- Ensure your practice's Notice of Purposes and Privacy Statement documents (relied upon for obtaining patient consent) are up to date with any changes that may affect how PHI is collected, used, disclosed or stored within your EMR

Consent Management

- Review your Notice of Purposes document to ensure it includes information on how patients may submit a request to limit or revoke consent to their PHI
- Develop and/or update a consent management procedure on how to manage patient consent directives. The procedure should cover topics such as implications of limiting consent, applying consent directives to your EMR and circumstances when consent directives are overridden

Access and Correction Rights

- Document any requests made by patients to correct their PHI in your EMR, regardless of whether the correction was made or not
- Document any actions taken to correct a patient's PHI in your EMR
- Utilize secure measures to provide patients with their requested PHI records

EMR User Access

- Manage EMR access privileges carefully to ensure users are only accessing the PHI necessary to fulfill their role and duties
- Designate one staff member to manage user accounts and EMR access
- Verify user access permissions before making changes to access privileges
- Have custodians and agents sign a confidentiality agreement

Administrative Safeguards

- Develop a management policy for privacy and security breaches that complies with PHI and PHIA requirements
- Develop practice procedures for handling breaches of your EMR
- Develop a safeguards policy for using the Med Access mobile app (e.g., use complex passwords, enable screen lock)

Technical Safeguards

- Ensure laptops and computers have appropriate firewall, anti-virus and anti-spyware protections
- Do not use public computers, public wireless networks (Wi-Fi) or laptops and home computers with shared users
- Do not use unsecure email addresses (e.g., Gmail) when sending documents containing PHI

Physical Safeguards

- Ensure computers, screens and printers are physically positioned within your practice to reduce unauthorized viewing and access
- Require users to log out of the EMR or lock their computers when they leave their desks unattended
- Ensure desks are cleared of PHI and cabinets containing PHI are locked at the end of each day
- Use a shredder when disposing of PHI documents
- Dispose of equipment in a secure manner that prohibits the recovery of any PHI

System Audit Functions

- Augment audit reports with functionality information that is not audited (e.g., taking screen shots, editing attachments) when responding to a user activity request
- Summarize within a user activity report the PHI that could have been accessed and by whom
- Develop an audit policy to ensure ongoing monitoring of audit reports and to identify and address unauthorized EMR activity
- Limit who has access to audit reports as the reports likely contain PHI

Data Portability

- Ensure retention schedules take into account all forms of PHI contained within your EMR (e.g., patient charts, billing information, audit reports)
- Develop a policy outlining PHI retention periods and disposal plans (e.g., de-identification of information, secure destruction)

Accuro EMR

Accuro is a cloud-based EMR that is customizable to your practice's clinical and workflows needs. It is owned, marketed and supported by QHR Technologies.

The following are features of Accuro:

- Patient Charts: View and analyze patient history and data on a single screen; order tests, requisitions and referrals; complete encounter notes and attach documents; view preventative care and incomplete tasks
- Labs and Imaging: Interface with health authorities, hospitals and private testing centres to download lab results, diagnostic imaging and other hospital reports; review documents, scans and faxes in one location; file documents into patient charts
- E-prescriptions: Write and renew prescriptions quickly and accurately; communicate directly with pharmacists through messaging; track medication history; duplicate high and low dose warnings
- Waitlist: Manage patient waitlists by urgency, date and procedure; view average wait times; track requisitions and referrals; print booking forms populated with personal health information (PHI)
- Appointment Scheduling: Book appointments; access patient contact information; generate labels; access schedule from remote locations
- Traffic Manager: View visual map of clinic room vacancies; identify clinic rooms with symbols; manage clinic walk-ins; create reports on wait times, appointment lengths and visit completion times
- Medical Billing Software: Streamline submissions to government billing; manage claims, errors, reconciliation and resubmission; reduce printing needs
- Medical Forms: Utilize pre-made medical forms and templates; customize forms and templates; digitize paper forms and import into EMR
- Letter Generation: Utilize pre-made consult, requisition and referral letters; customize letters; auto-populate from address book
- Clinic Data Reports: Generate reports from EMR data to optimize provision of care, workflows, preventative care; review patient visits by appointment type and reason; access billing code and revenue information
- Data Sharing: Share patient records between colleagues and clinics; allow temporary providers to view read-only records; control what is shared with other providers
- Mobile EMR: Access patient records on your phone away from the clinic; send secure messages, clinic notes and test results to staff members; patient PHI is not stored on phone

Considerations for Custodians

When implementing Accuro into your practice as a custodian, consider the following best practices:

Limiting Collection

- Identify the purpose(s) for which you are collecting PHI
- Ensure staff at your practice are knowledgeable of the purpose for collecting PHI and can explain it to patients
- Determine which available EMR information fields are necessary for the provision of health care
- Ensure staff at your practice are trained on what gathered information is necessary for the provision of health care
- Gather only the information deemed necessary for the provision of health care

Limiting Use

- Capture the minimum amount of PHI when completing patient profile pop-ups
- When creating, editing and running reports, only use identifying PHI when necessary (e.g., create aggregate reports when possible)
- Limit who can create, edit and run reports to those staff members who require access to complete their duties
- Develop a policy for your practice on accessing and using EMR reports (e.g., safeguards that must be in place, using an encrypted USB)

Limiting Disclosure

- Disclose only the minimum amount of PHI for health-care purposes
- Ensure the amount of PHI disclosed is appropriately limited (e.g., for MSI, disclose only the PHI required for claims administration purposes)

Sources and Accuracy of PHI

- Use EMR templates (e.g., requisitions, prescriptions) to reduce data entry errors
- Regularly verify and update patients' PHI in your EMR
- Document what PHI was removed or added to a patient's chart when merging or unmerging patient charts
- Ensure your health-care provider address book is up to date to prevent unauthorized PHI disclosure
- Confirm significant changes to existing claims to ensure PHI is accurate and complete before submitting to MSI

Consent

- Ensure a common method of documenting consent within your EMR is practised by all staff members
- Ensure your practice's Notice of Purposes and Privacy Statement documents (relied upon for obtaining patient consent) are up to date with any changes that may affect how PHI is collected, used, disclosed or stored within your EMR

Consent Management

- Review your Notice of Purposes document to ensure it aligns with the consent management functions in your EMR
- Develop and/or update a Consent Management Procedure on how to manage patient consent directives. The procedure should cover topics such as implications of limiting consent, applying consent directives to your EMR, sharing incomplete PHI because of a consent directive and circumstances when consent directives are overridden

Access and Correction Rights

- Document any requests made by patients to correct their PHI in your EMR, regardless of whether the correction was made or not
- Document any actions taken to correct a patient's PHI in your EMR
- Utilize secure measures to provide patients with their requested PHI records

EMR User Access

- Manage EMR access privileges carefully to ensure users are only accessing the PHI necessary to fulfill their duties
- Verify user access permissions before making changes to access privileges
- Designate one staff member to manage user accounts and EMR access
- Develop a User Access Policy to outline your expectations, as the custodian, regarding user access management within your practice (e.g., limit search results to 100 results, require passwords to have 12 characters)
- Have all custodians and agents sign a confidentiality agreement

Administrative Safeguards

- Develop a management policy for privacy and security breaches that complies with PHI and PHIA requirements
- Develop practice procedures for handling breaches of your EMR (e.g., contain, evaluate, investigate, notify)

Technical Safeguards

- Ensure laptops and computers have appropriate firewall, anti-virus and anti-spyware protections
- Ensure your EMR requires users to create strong passwords that must be used to unlock the EMR
- Do not use public computers, public wireless networks (Wi-Fi) or laptops and home computers with shared users
- Do not use unsecure email addresses (e.g., Gmail) when sending documents containing PHI

Physical Safeguards

- Ensure computers, screens and printers are physically positioned to reduce unauthorized viewing and access
- Require users to log out of the EMR or lock their computers when they leave their desks unattended
- Ensure desks are cleared of PHI and cabinets containing PHI are locked at the end of each day
- Use a shredder when disposing of PHI documents
- Dispose of equipment in a secure manner that prohibits the recovery of any PHI

System Audit Functions

- Augment audit reports with functionality information that is not audited (e.g., taking screen shots, editing attachments) when responding to a user activity request
- Summarize within a user activity report the PHI that could have been accessed and who could have accessed the PHI
- Enhance all reports with information from the audit log, patient log and document log within your EMR
- Develop an audit policy to ensure ongoing monitoring of audit reports and to identify and address unauthorized EMR activity
- Limit who has access to audit reports as the reports likely contain PHI

Data Portability

- Ensure retention schedules take into account all forms of PHI contained within your EMR (e.g., patient charts, billing information, audit reports)
- Develop a policy outlining PHI retention periods and disposal plans (e.g., de-identification of information, secure destruction)

Module 6:
EMR-integrated Solutions

What is Virtual Care?

Virtual care is a method by which health professionals can deliver health-care services without in-person interactions with patients. Synchronous virtual care is delivered by telephone or video (e.g., videoconferencing, telehealth, telemedicine), while asynchronous virtual care is delivered through secure messaging between the health-care providers and patients.

Doctors Nova Scotia's virtual care tool kit, Getting Started with Virtual Care, can help guide physicians on synchronous virtual care options.

What is an EMR-integrated Solution?

An EMR-integrated solution is a product that enables virtual care, integrates with your practice's EMR and provides tools and capabilities not necessarily found in the original EMR. You may choose to use one or more of the following EMR-integrated solutions:

Telus MedDialog

integrated with Telus Med Access

Telus MedDialog is a communication solution that integrates with the Telus Med Access EMR. It facilitates communication through the EMR with health-care professionals outside your practice.

The following are features of Telus MedDialog:

Clinic Operational Efficiency

- Communicate, collaborate and share patient information with other health-care providers through your EMR
- Reduce manual transcribing, scanning and phoning by posting communications to patient charts
- Send and receive multiple digital communications, e-faxes, e-consults and reimbursements simultaneously
- Incoming messages and faxes are sent directly to patient charts based on your EMR contact database
- Forward incoming messages to your practice's physicians and staff members

Continuity of Care and Patient Safety

- Facilitate and improve patient continuity of care
- Populate patient charts with most recent demographic information
- Receive confirmations of communication deliveries
- Shared patient information is stored in EMR
- Digital communications and e-faxes follow security best practices and regulatory requirements

Telus EMR Virtual Visit

integrated with Telus Med Access

Telus EMR Virtual Visit is an encrypted virtual care solution that integrates with the Telus Med Access EMR. It facilitates continuous workflow, reduces task redundancy and enhances continuity of care within the EMR.

The following are features of Telus EMR Virtual Visit:

Conducting Virtual Visits from Your EMR

- Schedule appointments with patients into your workflow
- Conduct video conferences with full audio and visual capabilities, and live-chat messages
- Review a patient's health records and take notes while conducting a video visit with the patient
- Access the solution from your smartphone, tablet, laptop or desktop computer from anywhere with an internet connection
- Use the visit timer to track and manage virtual visit times and durations

Provide Remote Primary Patient Care

- Reduce the risk of exposure (to COVID-19, for example) for you and your patients
- Click on a link to access the virtual call with your patient
- Observe and/or triage your patients' physical symptoms (e.g., appearance, body language, breathing pattern) through the video feed
- Provide more interactive care by video than by phone

Ensure Patient Confidentiality and Data Integrity

- Encrypted video and audio protect patient privacy
- Discuss patient personal health information (PHI), test results, treatments and preventative care in a secure manner
- Follow best practices by storing data and documentation within your EMR for record retention and audits

Features Coming Soon

- Launch appointments within a virtual waiting room where staff can confirm patient arrivals and patient health card information, and conduct initial triage
- Send brochures, requisitions and other forms to patients
- Save the visit start and end times, along with the live chat log, in the patient's EMR chart
- Send patients appointment invitations for visits within 48 hours
- Patients can share photos with you that can be stored in their EMR charts

Medeo Virtual Care

integrated with QHR Accuro

Medeo Virtual Care is a web-based virtual care solution that integrates with QHR Technologies' Accuro EMR. It facilitates secure virtual patient visits, messaging and online booking.

The following are features of Medeo Virtual Care:

Secure Patient Messaging

- Converse with patients through secure messaging from anywhere with an internet connection
- Close or reopen a conversation thread with a patient
- Share files and information from a patient's EMR chart
- Access and filter your own inbox based on patient, date, unread messages, drafts or closed message threats

Video Visits

- Schedule appointments through the Medeo web application
- Initiate virtual visits from Medeo using a web browser anywhere with an internet connection
- Turn on or off video sharing or audio settings anytime during appointments
- Converse with patients via a live chat during visits
- Upload and share files to Medeo during virtual appointments
- Capture a screenshot from your or the patient's video feed
- Leave and then return to virtual visit without having to schedule a new appointment

Other Features

- Secure your account by using phone verification (i.e., login with code sent to phone)
- Secure virtual conferences and calls through encryption
- Save time and money by allowing patients to book appointments online
- Review and audit messages and attachments with documented time stamps

Health Myself Patient Portal

integrated with Telus Med Access

The Health Myself patient portal is a web-based virtual care solution that integrates with the Telus Med Access EMR. It facilitates secure virtual engagement between health-care providers and patients.

The following are features of Health Myself:

E-booking

- Customize appointment types and characteristics (e.g., length, check-in time, cancellation policy, reminders)
- Decide when patients can schedule appointments and what type of appointments they can book
- Configure portal schedule for invite only, guest and/or new patient access
- Save administrative time by allowing staff members to focus on other clinic duties
- Improve service quality by allowing patients to book appointments through the portal rather than over the phone

Appointment Reminders

- Choose or combine multiple methods to notify patients of their appointments (e.g., email, short messaging service, voicemail)
- Customize the appointment reminder message by provider or appointment type
- Have the EMR remind patients to confirm their appointments. Once confirmed, patient appointment status will be updated in the EMR
- Save administrative time by using the portal's appointment reminder rather than having staff members call patients
- Reduce no-shows by sending reminders to patients of their appointment times, dates and locations

Self Check-in

- Save administrative time by allowing patients to check themselves into their appointments using their smartphones:
    - o Upon arriving at the clinic, patients click the check-in link or scan the check-in QR code
    - o Patients update their demographic information and complete any necessary e-forms that are then populated into their EMR chart
    - o Once patients have completed their check-in, they are marked as "arrived" in your EMR
- Improve patient flow and wait times by eliminating check-in lineups

Messaging

- Transmit encrypted communications over a secure network
- Decide which patients have access to the messaging system
- Start and download conversations from a patient's chart
- Create individual or shared inboxes that can be assigned to specific users or workgroups
- Share and receive documents with patients over a secure network
- Receive notifications if a patient has not read a time-sensitive message
- Improve service quality and save time by sending secure emails and messages rather than phoning

Broadcasting

- Send out notifications when you have announcements (e.g., flu clinics, vacation)
- Reach out to patients due for checkups prompting them to schedule appointments
- Inform patients about health and wellness programs
- Be proactive and encourage preventative care by promoting health education and healthy lifestyles to patients

E-forms

- Customize e-forms and e-questionnaires
- Allow patients to share their personal health information (PHI) through secure e-forms and e-questionnaires from their homes on their own devices or at your clinic on your device
- Send out e-forms to patient before or after their appointments

Module 7:
Checklists and Templates

Legislation Tools (Module 1)

Complaint Form
- Created by: Department of Health and Wellness (DHW)
- Description: The Complaint Form is completed by the patient when making a complaint under the Personal Health Information Act (PHIA) to the custodian
- Link (see "d" under "Forms to be completed by patients;" Microsoft Word document)

Complaints Policy Template
- Created by: DHW
- Description: The Complaints Policy Template provides patients with information on how to make a complaint to a custodian regarding the custodian's compliance with PHIA
- Link (see "g" under "Templates;" Microsoft Word document)

Confidentiality Agreement Template
- Created by: DHW
- Description: The Confidentiality Agreement Template provides custodians with a sample confidentiality agreement to be used between them and their medical and non-medical agents
- Link (see "h" under "Templates;" Microsoft Word document)

Fee Estimate for Access Form
- Created by: DHW
- Description: The Fee Estimate for Access Form provides custodians with a form to give patients when they are requesting access to their own personal health information
- Link (see "c" under "Forms to be completed by custodian;" Microsoft Word Document)

Fee Schedule
- Created by: DHW
- Description: The Fee Schedule provides custodians and patients with information from PHIA on the fees custodians may charge when providing access to a patient's personal health information
- Link (see "i" under "Forms to be completed by custodian;" Microsoft Word document)

Notice of Purposes Template
- Created by: DHW
- Description: The Notice of Purposes Template provides patients with a description of the purpose for which the custodian collects, uses and discloses their personal health information
- Link (see "a" under "Templates;" Microsoft Word document)

PHIA – Rules Summary and Checklist for Custodians

- Created by: Office of the Information and Privacy Commissioner for Nova Scotia (OIPC)
- Description: PHIA – Rules Summary and Checklist for Custodians provides a summary to custodians about the collection, use, disclosure and protection of personal health information. The document also provides a checklist to help custodians consider their obligations under PHIA
- Link (PDF document)

Privacy Policy Templates

- Created by: DHW
- Description: The Privacy Policy Templates provides patients with additional information about the custodian's privacy responsibilities and practices
- Link (see "d" under "Templates;" Microsoft Word document)

Request for Access to Personal Health Information Form

- Created by: DHW
- Description: The Request for Access to Personal Health Information Form is completed by the patient when requesting access to their personal health information from the custodian
- Link (see "a" under "Forms to be completed by patients;" Microsoft Word document)

Request for Correction to Personal Health Information Form

- Created by: DHW
- Description: The Request for Correction to Personal Health Information Form is completed by the patient when requesting correction of their personal health information from the custodian
- Link (see "b" under "Forms to be completed by patients;" Microsoft Word document)

Request for a Fee Waiver Form

- Created by: DHW
- Description: The Request for a Fee Waive Form is completed by the patient when requesting the custodian waive fees associated with accessing their personal health information
- Link (see "c" under "Forms to be completed by patients;" Microsoft Word document)

Response to Request for Access – Granted in Full Form

- Created by: DHW
- Description: The Response to Request for Access – Granted in Full Form is completed when a custodian is granting full access to a patient's request for access to their personal health information
- Link (see "d" under "Forms to be completed by custodian;" Microsoft Word document)

Response to Request for Access – Granted in Part Form

- Created by: DHW
- Description: The Response to Request for Access – Granted in Part Form is completed when a custodian is granting partial access to a patient's request for access to their personal health information
- Link (see "e" under "Forms to be completed by custodian;" Microsoft Word document)

Response to Request for Correction – Granted in Full Form

- Created by: DHW
- Description: The Response to Request for Correction – Granted in Full Form is completed when a custodian is granting full correction to a patient's request for correction to their personal health information
- Link (see "f" under "Forms to be completed by custodian;" Microsoft Word document)

Response to Request for Correction – Granted in Part Form

- Created by: DHW
- Description: The Response to Request for Correction – Granted in Part Form is completed when a custodian is granting partial correction to a patient's request for correction to their personal health information
- Link (see "g" under "Forms to be completed by custodian;" Microsoft Word document)

Response to Request for Correction – Not Granted

- Created by: DHW
- Description: The Response to Request for Correction – Not Granted Form is completed when a custodian does not grant a patient's request for correction to their personal health information
- Link (see "h" under "Forms to be completed by custodian;" Microsoft Word document)

Retention Schedule Template

- Created by: DHW
- Description: The Retention Schedule Template provides a documentation method for guidelines, authority, retention period, retention mode and disposition date for medical records containing personal health information
- Link (see "b" under "Templates;" Microsoft Word Document)

Written Privacy Statement Template

- Created by: DHW
- Description: The Written Privacy Statement Template provides patients with a summary of the custodian's privacy policy, including how personal health information is collected, used and disclosed; patient rights to limit or revoke their consent; how patients can request correction of and/or access to their health record; notification of privacy breaches; how patients can make complaints and appeal to the OIPC
- Link (see "c" under "Templates;" Microsoft Word document)

Breach Response Tools (Module 2)

Breach Letter Template to Patients

- Created by: Department of Health and Wellness (DHW)
- Description: The Breach Letter Template to Patients informs patients when their personal health information has been breached. Each letter should be customized to the circumstances of the privacy breach. The template outlines what information should be included in the letter (e.g., description of breach, recovery process, security improvements, recommendations)
- Link (see "f" under "Templates;" Microsoft Word document)

Breach Reporting Form for Review Officer

- Created by: DHW
- Description: The Breach Reporting Form for Review Officer is used by the custodian to notify the OIPC review officer of a privacy breach of personal health information. The form is used when the custodians decides the patient will not be informed
- Link (see "a" under "Forms to be completed by custodian;" Microsoft Word document)

Privacy Breach Checklist

- Created by: Office of the Information and Privacy Commissioner for Nova Scotia (OIPC), in *Key Steps to Responding to Privacy Breaches*
- Description: The Privacy Breach Checklist ensures all relevant factors in the four-step privacy breach response procedure are considered. The checklist also determines if the breach should be reported to the OIPC
- Link (see pages 13-21; non-writeable PDF document)

Privacy Breach Reporting Form, Privacy Breach Considerations Table and Risk Recorder, and Risk Rating Chart

- Created by: Doctors Nova Scotia, in Electronic Personal Health Information Breach Reporting Protocol
- Description: The Privacy Breach Reporting Form, the Privacy Breach Considerations Table and Risk Recorder, and the Risk Rating Chart are used to: document the nature of the privacy breach; consider all relevant factors related to the breach; determine whether notification is required; outline a follow-up plan for after notification; and conduct a risk analysis
- Link (see Appendices A-C, pages 5-11; non-writeable PDF document)

Report to the Office of the Information and Privacy Commissioner

- Created by: Information Access and Privacy Services, Department of Internal Services, Government of Nova Scotia, in *Managing a Privacy Breach: Protocol and Forms*
- Description: The Report to the Office of the Information and Privacy Commissioner is a template used to submit a summary report of a privacy breach to the OIPC, should it be deemed necessary
- Link (see Appendix C, pages 25-26; non-writeable PDF document)

Risk Rating Overview Chart

- Created by: OIPC, in *Key Steps to Responding to Privacy Breaches*
- Description: The Risk Rating Overview Chart may be used as a guide to determine the level of risk posed by a particular breach. Each public body, health custodian or municipality must make their own assessment of the risk given the unique circumstances of the situation
- Link (see pages 6-7; non-writeable PDF document)

Security Basics Tools (Module 3)

Reasonable Security Checklist for Personal Information

- Created by: OIPC
- Description: The Reasonable Security Checklist for Personal Information helps custodians ensure they have in place appropriate security measures and standards against various risks (e.g., unauthorized access)
- Link (PDF document)

Safeguard Tools (Module 4)

Safeguards Policy Template

- Created by: DHW
- Description: The Safeguards Policy Template provides information on how personal health information is protected from theft, loss, unauthorized access, collection, use, disclosure and modification while in the control of the custodian
- Link (see "e" under "Templates;" Microsoft Word document)

References

Doctors Nova Scotia

- Getting Started with Virtual Care: Everything you need to know to provide synchronous virtual care
- Templates and forms
- Tool kits for physicians

Doctors of British Columbia

- BC Physician Privacy Toolkit: A guide for physicians in private practice
- Physician Office IT Security Guide

Health Myself

- Patient Portal

Legislation

- Breach of Security Safeguards Regulations (federal)
- Personal Health Information Act (provincial)
- Personal Health Information Regulations (provincial)
- Personal Information Protection and Electronic Documents Act (federal)

Nova Scotia Department of Health and Wellness

- Toolkit for Custodians: A Guide to the Personal Health Information Act

Office of the Information and Privacy Commissioner for Nova Scotia

- Tools for Health Custodians

QHR Technologies

- Accuro EMR
- Medeo Virtual Care

Telus Health

- EMR Virtual Visit
- Med Access EMR
- MedDialog