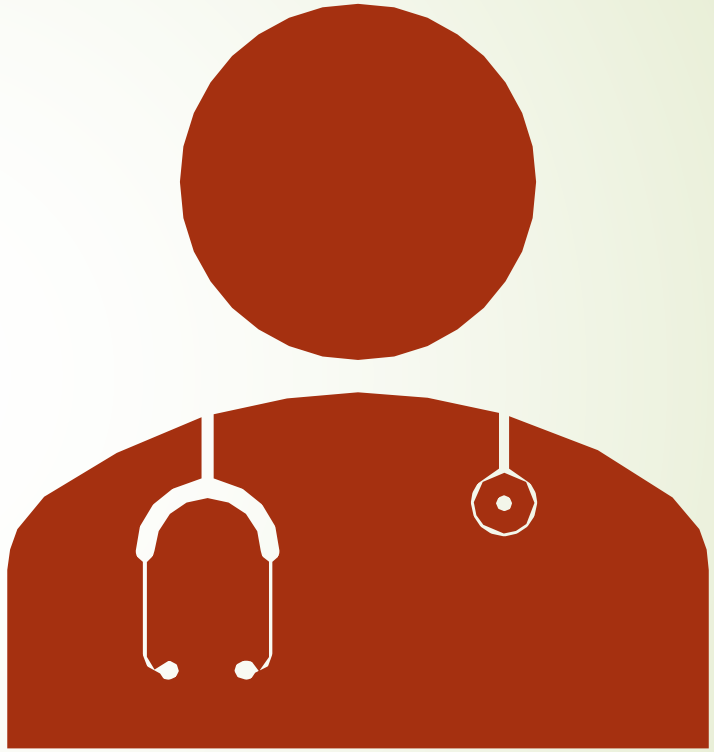
EMR Privacy and Security:

Collaborative Health Record

Compliance and Privacy/Security of Electronic Medical Records



- Everyone has a role to play in the privacy and security of electronic health information — it is a shared responsibility.
- The purpose of this presentation is to provide health care providers a resource to better understand how to integrate the Health Information Act (HIA) and security requirements into their practices.
- This presentation also includes educational information on privacy and security laws, rules, principles, and best practices to system users of the TELUS Collaborative Health Record (CHR), an Electronic Medical Record (EMR) chosen by the Province of PEI to be the provincial single instance EMR for use by health care professionals across the Island.

Information Privacy, Security, and Confidentiality

Privacy vs. Confidentiality

Confidentiality is the moral, ethical, legal, professional and employment obligation to protect the information entrusted to us

Includes anything you learn about the patient, including information on patient's hospital chart, any information shared verbally, and any electronic information

Privacy is the right of an individual to determine when, how and to what extent they share information about themselves with others

It is the right of the patient to control the collection, use and disclosure of information

Health Information Act (HIA)

- HIA provides direction to all organizations and individuals who collect, use, disclose and retain personal health information (PHI)

- Under HIA, the patient has the right to access PHI, request a correction to PHI, know who has accessed their information and challenge privacy practices

Personal Health Information (PHI)

PHI is any information and/or data that a healthcare professional collects to identify an individual and determine appropriate care. This includes information collected orally and/or in written form

- Every organization has an obligation to protect the privacy, confidentiality and security of personal information to which it is entrusted
- Examples include date of birth, address, medical record number (MRN), Health Card number, records from previous visits, name of healthcare provider, family history, and all information related to physical or mental health
- The HIA states that custodians must take reasonable steps to inform patients of the purpose for which the personal health information is being collected. Physicians will need to exercise their clinical judgment and common sense as it is not practical or necessary to have a conversation about collection with every patient. Brochures, notices or signs help to comply with this portion of the act

Health Information Act (HIA)

The purposes of this Act are

- (a) to establish a set of rules for custodians regarding the collection, use, disclosure, retention and secure destruction of personal health information that protects the confidentiality of personal health information and the privacy of the individual to whom the personal health information relates;
- (b) to enable personal health information to be shared and accessed, where appropriate, for the better provision of health services and the planning and management of the health care system;
- (c) to provide an individual with the right to examine and receive a copy of the individual's personal health information maintained by a custodian, subject to limited and specific exceptions, as set out in this Act;
- (d) to provide an individual with the right to request the correction of or amendment to the individual's personal health information maintained by a custodian, as set out in this Act;
- (e) to establish mechanisms to ensure the accountability of persons having custody or control of personal health information and to safeguard the security and integrity of the personal health information in their custody or control;
- (f) to provide for an independent review of decisions made by custodians and the resolution of complaints made with respect to custodianship of personal health information; and
- (g) to provide effective remedies for contraventions of this Act.

Custodians

As stated in the HIA, Custodians of PHI in PEI include:

- Public bodies
- Health care providers
- The Minister (of Health and Wellness)
- Island EMS
- Canadian Blood Services
- Information managers
- Researchers conducting an approved research project
- Health care facilities
- Nursing homes and community care facilities

Custodians cont.

- As a user of the EMR, you may not be a custodian of PHI. If you are an employee of Health PEI (HPEI) or working on behalf of HPEI, HPEI is the custodian of the PHI you can access. If you are an employee of a Fee-For-Service Physician, the Physician is the custodian and you are an agent of that custodian, accessing PHI on their behalf.
- Agents are responsible for complying with all the same requirements that custodians must follow, as per the HIA.

NOTE: Custodians are responsible for their agents. When agents collect, use or disclose information, they do so on behalf of custodians. When patients provide information to agents, it is as if they had given the information directly to the custodian. If an agent does something the HIA forbids them to do, it is as if the custodian performed the act. Agents must comply with the HIA and regulations as well as with the health information policies and procedures adopted by their custodians.

Terms to Remember - Personal Health Information (PHI)

Collect: in relation to personal health information, means to gather, acquire, receive or obtain the personal health information by any means from any source

Disclose: in relation to personal health information in the custody or under the control of a custodian or a person, means to make the personal health information available or to release it to another custodian or to another person, but does not include using the personal health information

Use: in relation to personal health information in the custody of or under the control of a custodian, means to handle or deal with personal health information or to apply the personal health information for a purpose and includes reproducing the personal health information, but does not include disclosing the personal health information

Consent: under the HIA (section 3) the consent (a) shall be a consent of the individual. If the individual is capable of granting consent, or the consent of a substitute decision-maker; (b) shall be knowledgeable; (c) shall be able to be withdrawn or withheld; (d) shall relate to the personal health information; (e) shall not be obtained through deception or coercion; and (f) subject to subsection (6), may be express or implied

Access: refers to situations of access for patients to their own PHI informally or by formal request

Protection: refers to safeguards that work to prevent:

- Unauthorized use, disclosure, copying, modification, destruction
- Inappropriate access
- Loss or theft

Examples of Collection, Use, Disclosure

Examples of collection:

- Taking a medical history
- Having a patient complete a form to provide health information
- Having a patient respond through surveys, questionnaires or polls for research purposes

Examples of use:

- Identifying and contacting patients
- Generating prescriptions

Examples of disclosure:

Health related disclosures

- To support the provision of care

Mandatory disclosures

- For audits being conducted
- For court requirements (e.g. subpoena, order)

Discretionary disclosures

- To assist with detecting or preventing fraud
- To assist with decisions at a correctional facility or psychiatric facility

Legislation, Policies, Procedures

- ***Health Information Act*** (HIA)
  https://www.princeedwardisland.ca/sites/default/files/legislation/h-01-41-health_information_act.pdf
- ***Freedom of Information and Protection of Privacy Act*** (FOIPP)
  https://www.princeedwardisland.ca/sites/default/files/legislation/f-15-01-freedom_of_information_and_protection_of_privacy_act.pdf
- **Privacy and Protection of Personal Health Information Policy**

Privacy Breaches & Confidentiality

- A breach occurs when a patient's personal health information is collected, used or disclosed without authorization, or PHI is lost or stolen
- This includes sharing information with other staff who are not part of the team providing care for the patient or accessing information about a patient to whom you are not providing care
- A proven breach in privacy will be subject to discipline and possible termination of employment

Examples of Privacy Breaches

- Misdirected emails/faxes
- Improper destruction of PHI
- Staff members discussing the patient, outside of patient care
- Sharing personal health information on social networks (e.g. Facebook)
- Unauthorized access (snooping) – you must NOT look at a patient's record if you are NOT providing care

Privacy Breach – Best Practices

- In the event of a suspected privacy breach, you should take action to stop or contain the breach if it is ongoing and report the incident according to appropriate policy. If you are not a Custodian, you should notify the appropriate Custodian of the information you believe was breached as soon as possible

- As with other sections of this document, consult the appropriate policy (HPEI or policy manual of your clinic) such as a privacy breach protocol for details on appropriate steps

Maintaining Confidentiality/Privacy

Avoid	Avoid discussing personal health information in public area (e.g. cafeteria, hallway, other patient rooms)
Leave	Never leave charts, computers, or other devices containing PHI unattended or in clear view of others. File information or put charts away in their proper place. Transport charts or other PHI face down or in envelopes
Do NOT share	Do NOT share passwords. Always log off-of the computer. You are responsible for activity under your credentials.
Do NOT engage in	Do NOT engage in conversations about patients or their personal health information with family, friends, neighbors, etc.

Maximizing privacy of patient PHI: the 10 principles

- The CSA Model Code for the Protection of Personal Information lays out 10 principles for collection, use, and disclosure of personal information

1 - Accountability	An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.
2 - Identifying Purposes	The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.
3 - Consent	The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4 - Limiting Collection	The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.
5 - Limiting Use, Disclosure, and Retention	Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.
6 - Accuracy	Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.
7 - Safeguards	Personal information must be protected by appropriate security relative to the sensitivity of the information.
8 - Openness	An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.
9 - Individual Access	Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10 - Challenging Compliance	An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with privacy legislation, usually their Chief Privacy Officer.

When Can You Share Personal Health Information?

- When access and sharing PHI, use the "Need to Know" principle:
  - Only access the PHI that is relevant for the patient care you are providing. This helps maintain privacy
  - Only share PHI with healthcare providers that are directly involved in the provision of care to a patient

Security

The increasing concern over the security of health information stems from the rise of EMRs, increased use of mobile devices such as the smartphone, medical identity theft, and the widely anticipated exchange of data between and among organizations, clinicians, agencies, and patients. If patients' trust is undermined, they may not be forthright with the physician. For the patient to trust the clinician, records in the office must be protected. Medical staff must be aware of the security measures needed to protect their patient data and the data within their practices.

Computer workstations are rarely lost, but mobile devices can easily be misplaced, damaged, or stolen. Encrypting mobile devices that are used to transmit confidential information is of the utmost importance.

Another potential threat is that data can be hacked, manipulated, or destroyed by internal or external users, so security measures and ongoing educational programs must include all users. Some security measures that protect data integrity include firewalls, antivirus software, and intrusion detection software. Regardless of the type of measure used, a full security program must be in place to maintain the integrity of the data, and a system of audit trails must be operational.

Audit trails. With the advent of audit trail programs, organizations can precisely monitor who has had access to patient information.

End users should be mindful that, unlike paper record activity, all EMR activity can be traced based on the login credentials. Audit trails do not prevent unintentional access or disclosure of information but can be used as a deterrent to ward off would-be violators.

Privacy and Security Principles

- Within the HIA, privacy of PHI is balanced with the need to share PHI across the health system to ensure Islanders receive the highest standard of care possible
- As established by the Canadian Medical Association's (CMA) Principles for the Protection of Patients' Personal Health Information, below are privacy principles to bear in mind when collecting, using, or disclosing PHI:

Trust

Confidentiality

Consent

Custodian as data steward

Trust

Being debatably the most important determinant of the level of control patients want with their medical records, trust is crucial to foster and maintain patient privacy. This can be achieved by collecting and sharing information only for the purpose of the care of that patient.

Confidentiality

Confidentiality and trust go hand in hand. Patients expect and have a right to confidentiality of their medical records, meaning that custodians and their agents do not share the health information with anyone outside of the patient's circle of care, unless authorized to do so by the patient.

Consent

Consent, in the context of the HIA, can be express or implied.

Type of consent	Description
Express consent	Express consent provided by an individual for the collection, use or disclosure of PHI is consent that is explicit, clear and direct. It may be given verbally, in writing or by electronic means, depending on the policies of the custodian collecting the consent. Express consent is required when: • a custodian proposes to disclose the PHI to a non-custodian (i.e., an insurance company or an employer); or • a custodian proposes to disclose the PHI to another custodian, other than the Minister, for a purpose other than the provision of health care.
Implied consent	Implied consent permits custodians to assume from the surrounding circumstances that an individual would reasonably agree to the collection, use or disclosure of their PHI. For example, when an individual discloses his or her PHI for the purposes of filling a prescription, a pharmacist can reasonably assume that the individual has consented to the collection of that PHI.

NOTE: in the case of request for access to PHI of mature minors (ages 13-17) by parents or guardians, staff can encourage the minor and parent/guardian to **co-sign consent**

Custodian as data steward

- A data steward (e.g., physician, institution or clinic) holds the physical medical record in trust for the care and benefit of the patient. A custodian, in most circumstances, should allow patients to access their medical records

- Certain exceptions apply, such as if the custodian believes that patient knowledge of the PHI could reasonably be expected to endanger the patient or another person

Preventing Privacy and Security issues

- Privacy and security issues when using the EMR are largely preventable. By employing preventive privacy and security practices, you can ensure that most issues are avoided
- Best practices include both physical and IT practices to avoid privacy breaches or security issues
- Not all practices may apply to you depending on your role at your workplace. For example, only some system users can access patient charts

Physical Practices

- You should safeguard PHI in oral form by taking reasonable steps to prevent overhearing of conversations with patients, clients or residents by other persons. Reasonable steps will vary dependent on the physical environment and the level of sensitivity of the PHI being discussed

- If possible or desired, it is good practice to use "sound masking" with natural or artificial sounds at a site in various rooms to prevent confidential conversation from being overheard. This technology may be of assistance in clinics where conversations are overheard at the reception area or sound passes from one exam room to another easily

- Do not leave devices unlocked with patient information visible. Always lock computer screens prior to leaving workstations to avoid privacy breaches

Physical Practices cont.

- A simple step to avoid unwanted viewing of PHI is ensuring that screens are tilted
- Prevent theft of devices by locking the door to the room or office in which the laptop is located, or by storing the laptop in a locked drawer or a safe
- Desks should be clean, meaning that there is no PHI exposed to a potential privacy breach
- Passwords are not visible (i.e. on bulletin boards, computer monitor)
- Use a shredder when disposing of PHI documents that are not required to be saved in the patient chart according to records management policies
- Place fax machines and printers out of sightline and reach of public areas
- Dispose of equipment in a secure manner that prohibits the recovery of any PHI

IT (virtual) Practices - Passwords

Passwords for devices should be strong to avoid security breaches. As system users, you are all responsible for ensuring the security of your passwords.

When selecting a password, ensure you:

- Do not choose anything obvious, such as birth date, or spouse and children's names
- Do not share your password with anyone
- Do not write your password down, place under your keyboard, or save it to your internet browser
- Your password is case sensitive and has to be 8 or more characters and should contain one special character
- Use both upper and lower-case letters
- Use at least one number
- Use at least one special character (such as the @, * or %)
- Do not begin or end the password with a number
- Make the password at least eight characters long

IT (virtual) Practices cont.

Wireless network practices (where applicable):

- Ensure all devices have antivirus, firewall protection
- Change the factory default password of the wireless router to a strong, complex password
- Use the strongest form of encryption for your network, implementing Wi-Fi Protected Access (WPA)2 where possible
- Use secure wireless network connections to prevent unauthorized access to the information you send and receive across networks
- Configure your devices so that any wireless connection is off by default (i.e. Wi-Fi and Bluetooth). Turn on wireless connections only when it is required

IT (virtual) Practices cont. 2

- Set devices to automatically lock after five to 15 minutes of inactivity
- Change your password immediately if you think someone has inappropriately accessed your account and report any inappropriate access or your suspicion of such to your Privacy Officer or healthcare professional responsible for the PHI

Handheld Device Practices

Handheld device practices (where applicable):

- Ensure all handheld devices are password protected using strong passwords
- Enable remote wipe on handheld devices to force a device to delete its contents in the event the device is lost or stolen
- Configure devices to automatically wipe after 10 failed login attempts
- Enable encryption on your handheld device(s) to protect unauthorized access to your data
- Only install applications from trusted sources. Avoid downloading free software and applications from the Internet without a high level of assurance that the product is safe and contains no adware, spyware, or viruses
- Ensure your handheld devices have anti-virus, malware and spyware software installed and enabled

Phishing: Prevention Tips

Phishing refers to cyber attacks that can target your work email address. The goal of phishing in health care settings is to trick you into giving sensitive information such as your username, password, or medical data. A common tactic is to prompt you to click on website links that may install malware on your device or prompt you to enter information on spoofed sites (i.e. a fake Telus site or a fake Government of PEI site).

Good prevention tips concerning phishing include:

- As a rule, be suspicious of solicitations with hyperlinks
- It is always good practice to double-check the email address of suspicious emails. Note that the name displayed in your inbox is often different than the name of the actual email address. Phishing campaigns may attempt to trick subordinates into sharing information by posing as managers/supervisors
- Always second guess emails that ask for personal information, offer rewards, or include dire warnings
- Whenever you suspect phishing, you should report it to your clinical lead or Privacy Officer as applicable

Your Collaborative Health Record: Privacy and Security

When using the Collaborative Health Record, there are key steps you can take to maximizing the protection of PHI.

Access to the CHR

- Ensure that the role-based access to the CHR is followed. You should NEVER use the EMR when signed in as another person

- Ensure that all clinic staff have signed a confidentiality agreement (including contractors, interns, volunteers, cleaning staff, temporary employees, etc.)

- Access privileges: You have specific access permissions in the CHR based on your employment responsibilities and the configuration of the CHR. You can **request** a change to your level of access to the EMR by requesting a change to your role with the EMR Program. Each site's clinical lead will discuss and/or approve role changes in collaboration with the EMR Program when required

- Never access information in the CHR for a purpose other than providing health care or for other authorized purposes related to your job duties. Ensure that all information gathered from the CHR is treated as confidential

Access to Patient Charts (if not originally your patient) in the CHR

In order to gain access to a patient's chart (whose primary care location is not a location you are a member of) users will need to enter a reason and password confirmation to open, see and add content to the patient record.

1. Search for a patient normally and select the patient from the list.
2. The chart will open if the patient's location matches one of your assigned locations.
3. If you are required to access a patient in another location, you will be asked to enter a concise, legitimate reason for access. You will then need to enter your CHR login password when prompted and you will have access to the record.
4. The forced access feature expires at midnight on the day the chart was opened. If you require additional access, you will need to repeat these steps to reopen the patient's chart.

You should never force access to a patient if you are not providing care to the patient. Such action would be a privacy breach as you do not need to know that information.

NOTE: those who do not have access to patient charts in general cannot force access to view a patient chart, even in emergency situations. However, role changes can be requested through the EMR Program.

CHR Functionality: Privacy and Security Considerations

Two-factor authentication

- Two-factor authentication is a method of additional login security. This method requires an additional login credential other than your username and password. With the CHR, two-factor authentication helps to prevent unauthorized sign-in. This is required upon each sign-in to the CHR
- This additional step is required as it helps to prevent cyber attacks by requiring additional information from a system user
- Without this mechanism, a user may fall victim to phishing or other cyber attacks intended to steal login credentials

NOTE: Two-factor authentication is not currently supported but will be supported when integrations with the CHR are complete

CHR Functionality: Privacy and Security Considerations

Double-checking documents

- It is crucial that documents coming in and out of the CHR are the intended documents
- You should always verify that the document you are downloading, uploading, saving, printing, or sending outside of the CHR is what you intended

NOTE: When uploading, downloading, saving, printing, or sending PHI outside the CHR, there are no warnings configured in the CHR to ensure that users double-checked the applicable file. These reminders will eventually be a part of the CHR.

PrescribeIT: Privacy and Security

PrescribeIT

- Canada Health Infoway is working with Health Canada, the provinces and territories, and industry stakeholders to operate and maintain a national e-prescribing service, PrescribeIT

- PrescribeIT will be integrated with the CHR

PrescribeIT – privacy and security considerations

- Do not let anyone other than yourself use your PrescribeIT account
- Do not use devices to access PrescribeIT that are not authorized
- Do not use unauthorized software on the device with PrescribeIT
- Do not send PHI over unencrypted email
- Click on the logout button when you are finished for the day or will be away for a while
- Be aware that any information in clinical communication would be included as part of a patient's access or correction of PHI request

PrescribeIT – privacy and security considerations cont.

- Example privacy or security incidents to avoid (but report if it occurs!):

- A pharmacy sending a renewal request when specifically instructed not to by a patient
- A PrescribeIT user sending a prescription to an unintended recipient or location
- Malicious software, such as a virus or malware, on the computer running PrescribeIT

The Future

- Health care is increasingly information-intensive. The combination of Provider expertise, data, and decision support tools will improve the quality of care
- Information technology can support the physician decision-making process with clinical decision support tools that rely on internal and external data and information
- It will be essential for physicians and the entire clinical team to be able to trust the data for patient care and decision making
- Creating useful electronic health record systems will require the expertise of physicians and other clinicians, information management and technology professionals, ethicists, administrative personnel, and patients

Conclusion

- Electronic Medical Records can provide many benefits to physicians, patients and healthcare services
- It is crucial that you and your team continue to follow laws, rules, principles, and best practices to ensure appropriate collection, use, disclosure and protection of PHI. In doing so, you will help protect the privacy of your patients while providing appropriate care

Security covers a large expanse of topics. Below are links to documentation that can help answer questions, provide direction on numerous topics, and outline the do's and dont's associated with maintaining a high-security mindset.

- *Health Information Act* (HIA)
- Guide to the Prince Edward Island Health Information Act
- *Freedom of Information and Protection of Privacy Act* (FOIPP)
- *Archives and Records Act*
- Privacy and Protection of Personal Health Information Policy
- Government Information Security Policy (GISP)
- Information Security Guide for Employees
- Standard Procedure for Email and Instant Messaging Security
- Incident Management Process
- Acceptable Use Policy
- PIPEDA fair information principles
- CMA principles on Privacy

Contact and types of support	Contact information
EMR Support Team: enrollment, use, support security and privacy	emrprogram@gov.pe.ca
Office of the Information and Privacy Commissioner for PEI: PIA submission and review, HIA compliance and privacy incident investigations	InfoPrivacy@assembly.pe.ca 902-368-4099
College of Physicians & Surgeons of PEI: Privacy issues involving physicians, ownership of patient records or patient records retention	cpspei.ca 902-566-3861

Link to Moodle to complete required quiz:

https://moodle.gov.pe.ca/