

PITO Privacy Guide

Version 1.2
Date: July 16, 2009

PITO Privacy Resource: Ruth Yeo

Table of Contents

SECTION 1: PITO Privacy Background	4
PITO Privacy Guide	4
PITO Commitment to Protecting Privacy	4
PITO Master Standing Agreement.....	4
Application Service Provider (ASP).....	5
Core Data Set	6
PITO Privacy Functional Requirements.....	6
PITO Privacy Working Group.....	6
PITO Privacy Implementation Activities	7
SECTION 2: Physicians and Privacy	8
What is Privacy?	8
Privacy Legislation Overview: FOIPPA and PIPA.....	8
Definition of Personal Information under PIPA	9
Definition of an Organisation under PIPA.....	9
Physician Obligations Under PIPA	10
How Do Physicians Become PIPA Compliant?.....	10
10 Steps for PIPA Compliance	10
Data Stewardship.....	11
SECTION 3: EMR Privacy Implementation Considerations	13
Privacy Officer.....	13
Privacy Best Practices.....	13
Security Safeguards	14
Roles-Based Access Model	15
Sample Roles:.....	16

Sample Permissions:	16
By Exception.....	17
Sample Roles Based Access Model Matrix.....	18
Account Management.....	19
Individual Disclosure Directives (Masking).....	19
Audit Trails and Auditing.....	20
The CMA Privacy Wizard.....	21
Privacy Impact Assessments (PIAs).....	22
PITO Privacy and Security Go-Live Checklist	22
SECTION 4: PITO Privacy References.....	23
SECTION 5: Roles-Based Access Model Template.....	25

SECTION 1: PITO Privacy Background

PITO Privacy Guide

The purpose of this Guide is to provide physicians and/or their staff an overview of privacy and an understanding of best practices for privacy, confidentiality and security of personal information during the transition of paper-based records to an Electronic Medical Record (EMR). The protection of personal information must be managed through a combination of administrative practices, technical security solutions, physical security, and organisational security, and this Guide will provide the background on legislative requirements, provincial standards, and best practices to consider for ensuring the integrity, confidentiality and availability of personal health information. It will also provide a link to the Canadian Medical Association (CMA) Privacy Wizard, an educational toolkit and resource to support compliance efforts. Additional privacy references will also be offered.

PITO Commitment to Protecting Privacy

PITO is committed to supporting PITO physicians in adopting adequate and reasonable privacy and security safeguards to protect personal health information and has demonstrated this through a number of initiatives and strategies.

These include:

1. Clear stipulations in the **PITO Master Standing Agreement (MSA)** between the Province and the PITO-approved EMR service providers.
2. Contractual arrangements to ensure privacy and security of the **Application Service Provider (ASP)** model.
3. A comprehensive set of **functional privacy requirements** which the EMR software must meet.
4. A **PITO Privacy Working Group**, reporting to the PITO Working Group and PITO Steering Committee, has been in operation since November 2006, providing guidance and oversight over PITO privacy activities.
5. A number of **privacy implementation activities** have been integrated into the overall PITO Implementation Activities.
6. Information sharing and collaboration with the College of Physicians and Surgeons of BC and the Office of the Information Privacy Commissioner (OIPC)

PITO Master Standing Agreement

The PITO Master Standing Agreement (MSA) between the Province (Ministry of Health) and the PITO-Qualified EMR service providers clearly articulates the privacy, security and confidentiality terms in three areas:

- i. Article 12: Privacy, Security and Confidentiality, of the Master Standing Agreement
- ii. Schedule 8: Privacy and Security Obligations
- iii. Schedule 11: Service-Provider – Physician Privacy Terms

These requirements reflect the need to meet provincial privacy legislation, BC College of Physician and Surgeon guidelines, Provincial eHealth policies, industry standards and best practices.

Key highlights of the privacy and security terms are as follows:

- At all times, personal patient information is under the custody and control of the physicians including while stored at the ASP data centre.
- The Province does not have custody or control, nor any access to data stored in an EMR or within the data centres, without the explicit knowledge and consent of the physician.
- Service providers cannot permit access to EMR data stored in the data centres by any party without the explicit knowledge and consent of the physician.
- Service providers only have access to systems as authorized by physicians, and for the purposes of support and maintenance.
- Service providers' obligations include establishing their own internal privacy policies, training their staff, ensuring physical and technical security safeguards are in place, and controlling access by employees and contractors to patient information hosted in the ASP data centres.
- Service providers may store, access and use patient personal information only under specific purposes and only within Canada. Support must also be from within Canada and performed by employees of Canadian entities. Exceptions may be made for foreign access only for a permitted and controlled purpose and in accordance with foreign access conditions. Specific procedures must be in place to permit these circumstances.

Application Service Provider (ASP)

PITO-approved EMR service providers will be operating via an Application Service Provider (ASP) model. Rather than implement individual servers within each private physician office environment – which would require separate and independent maintenance and safeguarding – each service provider is creating professionally managed data centre(s) to host the EMR databases on one or more servers within a secure and redundant environment with reliable and appropriate access from physician offices over a third party secure network.

Access to the ASP data centres will be controlled both contractually as well as through physical, procedural, and technical security measures.

Core Data Set

Appendix H of the Physician Master Agreement (PMA) included stipulations for the exchange of data elements defined as the Core Data Set. Any reference or contractual requirement related to that Core Data Set has been removed from the PITO Registration Agreement and PITO Policies. As such, this requirement of the PMA has been removed.

While the contractual requirement has been removed, many physicians see significant value in the exchange of structured electronic data to support referrals or shared care for enhanced patient care. As such, PITO is supporting local and regional physician groups who are proceeding with voluntary electronic referral (eReferral) and related initiatives, in consultation with the BCMA, College, Office of the Information Privacy Commissioner and the Ministry of Health Services. These initiatives create the ability for physicians to send specific data to another physician (for incorporation into their EMR) as part of a referral or other visit, in keeping with College policies and guidelines and BC legislation.

PITO Privacy Functional Requirements

EMR service providers must meet a comprehensive set of privacy functional requirements identified in the Request for Proposal (RFP) and any existing gaps must be compliance tested before the product may be presented to physicians as a PITO offering.

These privacy functional requirements include:

- Strong access control measures and roles-based access
- Tools to manage user accounts – creation, suspension, deletion, role changes
- Detailed audit functionality with no ability to modify audit trails, and audit reporting
- Ability to retain information as per legislation and regulatory guidelines
- Ability to mask and unmask data based on roles and permissions
- Ability to correct and annotate information while maintaining a history
- Ability to generate copies of patient records, severing restricted information if required, to support patient information access requests

PITO Privacy Working Group

A PITO Privacy Working Group (PWG) has been in operation since November 2006 and consists of representatives from the BC Medical Association, BC College of Physician and Surgeons, BC Ministry of Health, PITO team members, and practicing physicians.

The purpose of the Working Group has been to identify concerns, discuss issues, and provide feedback on privacy materials and privacy activities underway to support the implementation of EMRs.

PITO Privacy Implementation Activities

Privacy has been integrated throughout the PITO implementation activities.

- Privacy is a component of the PITO Readiness Assessment, a series of questions based upon the “BCMA 10 Steps for PIPA Compliance”. The intent is to assess state of existing privacy compliance within physician practices.
- The PITO Privacy Guide (this document) will review privacy concepts, legislation, PITO privacy expectations, specific EMR privacy requirements, and offer additional PITO Privacy References as supporting material. It will also link PITO physicians directly to the Canadian Medical Association’s (CMA) Privacy Wizard, a mandatory requirement for completion by each medical practice.
- Where applicable, a Privacy Impact Assessment (PIA) may be required if the implementation is considered complex and integrates multiple practices onto one EMR database.
- The PITO Privacy and Security Go-Live Checklist must be completed to ensure a reasonable and acceptable level of compliance prior to implementation of an EMR.

SECTION 2: Physicians and Privacy

What is Privacy?

Privacy is the right of an individual to have knowledge and control over their personal information. Privacy applies to individuals in any context – as a patient, employee or citizen.

Privacy Legislation Overview: FOIPPA and PIPA

There is no specific health privacy legislation in BC. The BC Freedom of Information and Protection of Privacy Act (FOIPPA) governs public bodies (health authorities, government etc) while the BC Personal Information Protection Act (PIPA) governs private sector (private medical practices , private labs etc). The Federal Personal Information Protection and Electronic Documents Act (PIPEDA) governs federally regulated commercial activities, such as selling information for profit, and does not apply to the health sector. PIPEDA applied to private sector prior to PIPA being introduced in 2004.

In addition to protecting privacy, PIPA also provides rights for patients to protect their information; allows them access to their information; and allows for review and correction or annotation of their information. Physician practices must have policies and procedures in place to support these requirements.

Express consent is not a requirement under PIPA for direct patient care purposes or other consistent purposes and implied consent is the norm for continuity of care. However, implied consent must be ‘informed, knowledgeable’ consent and physician practices must communicate the ways in which they respect the privacy of patients and how they safeguard personal information (e.g. patient privacy notice).

While PIPA states that personal information should only be retained for as long as necessary to fulfill the purposes(s) for which it was collected, when considering the destruction of medical records, physicians should be aware of the College of Physician and Surgeons of BC’s retention guidelines, the provisions of the Limitations Act, and any requirements of their insurers.

Patients may complain to the Office of the Information and Privacy Commissioner of BC (OIPC) if they believe their personal information has not been collected, accessed, used or disclosed in compliance with PIPA . Further, the OIPC can investigate complaints made to it and can also initiate its own investigation if they believe an organization is not complying with PIPA.

Definition of Personal Information under PIPA

Personal information as defined under PIPA is information that can identify an individual (e.g. name, home address, home phone number, ID numbers), and information about an identifiable individual (e.g. physical description, educational qualifications, blood type).

Personal information includes, but is not limited to:

- Name, address, telephone number
- Race, national/ethnic origin, colour, religion, or political beliefs and associations
- Age, sex, sexual orientation, marital status
- Identifying number or symbol
- Fingerprints, DNA, blood type
- Health care history
- Educational, financial, criminal, employment history
- Anyone else's opinions about an individual and an individual's personal views/opinions unless about someone else

Personal information includes employee personal information but **does not include** business contact information, work product information, and aggregate/anonymous information. Employee personal information is information that is collected, used or disclosed solely for the purpose of establishing, maintaining, managing or terminating an employment relationship between an employee (including a volunteer) and an organization. This may include information such as name, home address, educational history and employment history. This does not include contact information or work product information (see below).

Contact information means information that allows an individual to be contacted at work. It includes the name, position name or title, business telephone number, business address, business e-mail and business fax number for the individual.

Work product information is information that is prepared or collected by an employee as part of that individual's work responsibilities, but does not include information about an individual who did not prepare or collect the information.

Definition of an Organisation under PIPA

An organization includes:

- a corporation
- a partnership
- an individual involved in a commercial activity (for example, an individual running a small renovation business that is not incorporated)
- an association that is not incorporated
- a trade union

- a non-profit organization, such as a charity, club, religious organization or amateur sport association
- a trust, except for a private trust for the benefit of friends or family of the individual who sets up the private trust.

Physician Obligations Under PIPA

Physicians in private practice are governed by PIPA. PIPA governs how a medical practice collects, handles, stores and discloses personal information, including personal information about employees or volunteers. Physicians are expected to take adequate and reasonable measures to protect personal information from risks such as unauthorized collection, access, use and disclosure. The physician's duty to protect confidentiality of personal patient information is irrespective of the form in which the information is stored or transmitted (e.g. paper, electronic).

In addition to PIPA, physicians are also obligated to comply with professional and regulatory standards and codes of ethics. It is expected that employees/staff of physicians also adhere to the same levels of privacy responsibilities. Physicians are accountable for any privacy breach that occurs including any breach committed by an employee under their authority.

How Do Physicians Become PIPA Compliant?

Approaches to compliance will be based on a number of factors including¹:

1. the nature of the organisation's business
2. the organisation's size
3. the kind of information the organisation collects, uses and discloses
4. how the organisation stores and secures information
5. the expectations of the individuals who deal with the organisation
6. whether the organisation transfers personal information across provincial or national borders
7. the reputation the organisation wishes to promote

The more complex the scenario, the more risks may be involved, requiring multiple mitigation strategies. It is useful to perform a Privacy Impact Assessment (PIA), a method for analyzing privacy and security issues, in these circumstances. PIAs are explained further later in this document.

10 Steps for PIPA Compliance²

When PIPA came into effect January 1, 2004, the BCMA developed "10 Steps for PIPA Compliance" as a practical guide for physicians. Following these steps provide a straight forward way for practices to move forward in their compliance efforts.

¹ Private Sector Privacy: PIPA Implementation Tool 1, Ministry of Management Services, Government of British Columbia, 2004

² http://www.bcma.org/public/news_publications/publications/PrivacyToolkit/TenSteps.htm

1. Each medical practice must appoint a Privacy Officer responsible for PIPA compliance. The BCMA recommends that this individual be a physician.
2. The Privacy Officer, physicians and employees must understand their privacy and confidentiality obligations under PIPA, in addition to any professional and regulatory standards and codes of ethics.
3. Practices must routinely review how they handle and manage personal information in their day to day activities.
4. Practices must consider if they meet PIPA obligations and if not, make the necessary improvements.
5. Practices must assess information handling practices in light of transitioning from paper to electronic records.
6. Practices must establish an office privacy policy and privacy notice for patients.
7. Employees must be trained about privacy and how to confidentially manage personal health information regardless of format (paper or electronic).
8. Practices must develop or revise forms and communication materials that inform patients about the privacy policy and information practices.
9. Contracts with third parties must require compliance with PIPA and any policies developed to adequately and appropriately manage personal information held by the practice.
10. PIPA requires that there be a process for privacy complaints. Having an effective complaints process is an important aspect of managing privacy risks within a practice.

Data Stewardship

Data stewardship is the management of personal health information by a health professional and includes the collection, use, disclosure, and management of that information. Physicians are legally obligated to maintain a medical record of the care provided, while the physician-patient relationship requires a patient's confidence and trust in the management of their information.

While patients own their personal (health) information, physicians are custodians of personal information they collect. Organizations have custody and control of personal information when it is in their offices, facilities, file cabinets and computers.

With the transition of paper-based records to electronic medical records, there is an opportunity to improve the quality and efficiency of care; however, there are risks if personal health information is accessed inappropriately, mismanaged, or compromised. While technology is changing and influencing the future of health care, data stewardship is a professional responsibility and not a technology issue³.

The implementation of EMRs creates a natural stress point for physicians due to the changing natures of circles of trust. Historically, there has been generally accepted circle of trust between

³ Data Stewardship Framework, Committee on Privacy and Data Stewardship, BC College of Physicians and Surgeons, July 31 2007

physicians and between physicians and other health professions in the exchange and disclosure of information for continuity of care. The EMR, and further, the Electronic Health Record (EHR), has expanded the circle of trust, where the disclosure is prospective to future information needs, where the communication is roles-based rather than a directed communication and where the disclosure is systematic, rather than individualized⁴.

As medical records evolve from being paper-based to electronic, it can create uncertainty in the sharing and management of information. On a periodic basis, it is recommended that physicians⁵:

- Evaluate their practices information management processes
- Develop/revise the practice's data stewardship policies and guidelines
- Update the processes supporting the use of the medical record
- Evaluate the availability and uses of external medical records

The BC College of Physicians and Surgeons have recently released the Data Stewardship Framework to guide physicians through the transition from paper to electronic records.

This document is available at www.cpsbc.ca.

⁴ Data Stewardship Framework, Committee on Privacy and Data Stewardship, BC College of Physicians and Surgeons, July 31 2007

⁵ Ibid.

SECTION 3: EMR Privacy Implementation Considerations

The introduction of EMRs does not change a physician's responsibilities for appropriately and ethically accessing patient information for the purposes of providing direct patient care. Physicians remain custodians of patient information and continue stewardship of data regardless of format (paper, electronic) and regardless of where the information may be stored (file cabinets, off-site in an ASP model).

Protecting the privacy and confidentiality of patient information, particularly in practices implementing an EMR, requires a combination of physical, technical, and administrative safeguards.

Such examples of safeguards include:

- Physical security: locked file cabinets, locked down workstations, printers in non-public areas, alarms
- Technical security: unique user IDs and passwords, encryption, firewalls, audit trails, access controls
- Administrative controls: staff training, office policies and procedures, confidentiality agreements, contractual agreements with third parties, account management, patient privacy notices

Privacy Officer

Your organization (practice) must designate one or more individuals as a "Privacy Officer" to make sure that your practice adheres to PIPA. This individual may also be the contact person for answering questions about PIPA and for handling information access requests and complaints under PIPA. Other individuals in your organization may be delegated to act in the place of the appointed individual. The Privacy Officer may also be responsible for reviewing audit trails and routinely ensuring that users are accessing patient information in an appropriate manner.

To support the Privacy Officer functions, additional resources, which may include field resources, are referenced in Section 4, or are under development through the PITO Program.

Privacy Best Practices

There are a number of privacy best practices that should take into consideration.

If your practice sends electronic information to another business to process or store it for your business, the information is still under your control even though you have sent it to your contractor or service provider. You must make sure that the other business protects it the same way that you would. Your organization must use contractual or other means to provide a comparable level of protection while the information is being stored or processed by a third party.

Your practice should develop policies, procedures and patient notices to protect personal information.

These policies and procedures should include the following:

- What information you collect
- Why you collect personal information
- How you obtain consent for collecting, using and disclosing personal information
- What the limits are on your collecting, using, and disclosing personal information
- How you ensure that the personal information is correct, complete and current
- How you ensure that adequate security measures are in place
- How you respond to inquiries and complaints
- How you process information access requests

Additionally your practice must educate staff on the organisation's privacy policies, practices and protocols. It is also recommended that staff sign confidentiality agreements.

Security Safeguards

Under PIPA, organisations must make "reasonable security arrangements" to protect personal information from "unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks".

Industry has shown that while the threat of hackers is often seen as the major security threat, most instances of privacy and security breaches occur within organisations by personnel with legitimate access.

The following safeguards should be considered:

Physical security

- Enhance exterior security such as alarms and lighting.
- Locking file cabinets and areas where files are stored when no one is there.
- Allowing only employees who need access to the storage areas or filing cabinets to have access to them.
- Positioning computer monitors so that personal information displayed cannot be seen by unauthorized individuals (e.g. the public).

Technical security

- Ensuring your computers and network are secure from intrusion, including by using firewalls and, where appropriate for sensitive personal information, by encrypting personal information to prevent unauthorized access.
- Placing printers and fax machines in non-patient accessible areas of the office.
- Using strong and secure passwords to make sure that only authorized users have access to information on computers. Passwords should be changed on a regular basis.
- Ensuring that audit trail capabilities are activated to record user accesses.

- Completely erasing the hard-drive of any computer you sell or discard, particularly ones that may contain personal information or, ideally, physically destroying the hard-drive.
- Mobile devices such as laptops and PDAs must be password protected and encrypted.
- E-mails containing personal information must be encrypted.
- Adequate virus protection must be in place to ensure data is not modified or destroyed by external processes or sources.

Administrative/Procedural security

- Confirm fax numbers before you press send.
- Shredding papers containing personal information rather than just placing them in a garbage can or recycling bin.

Roles-Based Access Model

A roles-based access model supports the **balance between access to information and protection of privacy**, and enforces the trust relationship of the physician/authorized care providers to the patient by ensuring that access is based on the ‘need to know’ principle.

The goal is to identify all possible roles to which a standard set of functional areas and permissions would be assigned. This allows for ease of account management as each authorized user would then be assigned to a role. To support business and clinical workflow, **exceptions** to these standard permissions may be considered for users with unique roles as long as it is authorized and necessary to perform job functions.

Guiding principles⁶ for access include:

1. Access to personal information within the EMR will be roles-based.
2. Access to personal information is based on the ‘need to know’ principle.
3. Access to personal information within the EMR will be permitted for the purposes of providing direct patient care only (this includes clerical and financial access to support day-to-day operations of the practice)
4. A user with multiple roles will have the appropriate permissions to support each of those roles.
5. Service provider access will be controlled contractually and through roles-based access.
6. All accesses made to patient information are audited for compliance monitoring purposes.

Additionally, access should not be provided until each user is authorized by a physician, completes EMR training, is provided with privacy education, has signed a confidentiality agreement, and is made aware of office privacy policies. Due to their data stewardship responsibilities, physicians assume responsibility for the accesses made to patient information, including those accesses made by staff and delegates.

⁶ Guiding principles adapted from Provincial eHealth Policy on Access and Permissions, BC Ministry of Health

Ongoing account management is also critical to ensuring appropriate access, and it is the responsibility of each practice to ensure that one individual (and designate) is responsible for adding, modifying and deleting users on a timely basis.

The following criteria should be considered when defining roles, functional areas of information access, permissions and exceptions.

1. What are all the possible roles (Physician, MOA, Clinic Coordinator etc.) that would require access to patient information?
2. What are all the possible functional areas of information access (e.g. clerical, clinical, financial/billing) and can these broad areas be broken down further to manage access to what is most appropriate for the performance of each role?
3. What are all the possible permissions that could be assigned (e.g. create, read only, update, delete, authorize)?
4. What are all the other additional functions that a role may or may not have the ability to perform (e.g. print, mask data, unmask data)?

Sample Roles:

Groups	Roles
Physician	Physician, Psychiatrist, Nurse Practitioner
Nurse	Registered Nurse, Licensed Practice Nurse, Pharmacist
Allied Health	Nutritionist, Physiotherapist
Counsellor	Mental Health Counsellor, Addictions Counsellor, Social Worker
MOA	Clinical Assistant
Clerk	Registration and Booking Clerk
Coordinator	Clinic Coordinator
Manager	Clinic Manager
System Administrator	System Administrator

Sample Permissions:

Permissions
C=Create
R=Read Only
U=Update
D=Delete
A=Authorize
A*=Authorize with Restrictions
M=Mask/Unmask

By Exception

By Exception refers to circumstances where standard permissions associated with a role need to be modified because of a user's unique function within a practice. A physician must authorize all 'exceptions' required to customize permissions associated with an individual's user account.

The following criteria should be considered when determining what permissions and functions should be assigned to each role as a standard setting.

1. Can existing users currently access all of this information?
2. Do each of these roles truly require access to all areas of information?
3. Are the users unable to carry out the requirements of their job if they do not have access to this information?
4. Can harm be caused to the patient if the users do not have access to this information?
5. Are there professional practice standards that require the user to have access to this information?
6. Is this information required to support the care of the patient across the continuum of care?
7. Does this individual require regular access to this information or only on an occasional basis where other methods of access or the availability of other personnel who would more justifiably require such access would suffice?

See the following page for a sample roles-based model matrix.

Sample Roles Based Access Model Matrix

ROLES-BASED ACCESS MODEL MATRIX

FUNCTIONAL AREAS	ROLES								
	Physician	Nurse	Allied Health	Counsellor	MOA	Clerk	Coordinator	Manager	System Administrator
<i>Patient Registration</i>	RU	RU	RU	RU	RU	RU	R	R	-
<i>Appointment Scheduling</i>	CRUD	CRUD	CRUD	CRUD	CRUD	CRUD	R	R	-
<i>Patient Check-In</i>	RU	RU	RU	RU	RUD	RUD	R	R	-
<i>Patient Assessment</i>	CRUM	CRU	CRU	CRU	R	-	R	R	-
<i>Care Plan</i>	CRUM	CRU	CRU	CRU	R	-	R	R	-
<i>Encounter Notes</i>	CRUM	CRU	CRU	CRU	R	-	R	-	-
<i>Counselling Notes</i>	RM	R	R	CRUD	R	-	-	R	-
<i>Problem List</i>	CRUDAM	CRUDA*	CRUDA	CRUDA	R	R	R	R	-
<i>Outgoing Referral</i>	CRUDA	CRUDA*	CRUDA*	CRUDA*	CRU	-	R	R	-
<i>Immunizations</i>	CRUDA	CRUDA*	CRUDA	R	R	-	R	R	-
<i>Alerts</i>	CRUDA	CRUDA*	CRUDA	CRUDA	CRUD	CRUD	CRU	R	-
<i>Allergies</i>	CRUDA	CRUDA*	CRUDA	CRUDA	R	R	R	R	-
<i>Prescriptions</i>	CRUDAM	CRUDA*	CRU	R	R	-	R	R	-
<i>Incoming Results</i>	CRUDAM	CRUD	CRUD	CRUD	CRUD	-	CRU	CRU	-
<i>Billing</i>	CRUD	CRUDA*	-	-	CRUD	-	CRUD	CRUD	-
<i>User Account Management</i>	-	-	-	-	-	-	CRUDA	CRUDA	CRUDA
<i>Auditing</i>	-	-	-	-	-	-	CRU	CRU	CRU
<i>Reporting</i>	R	R	R	R	R	R	CRUD	CRUD	CRUD

Account Management

Once the access model has been designed and implemented, it is important to ensure that only legitimate users have access to patient information in the EMR and that each user has the appropriate level of permissions.

Common principles for account management include:

1. Every user must have a unique user ID and password that is changed regularly through enforced password controls
2. Audit trail functionality must be activated to record actions taken by each user
3. Authorization policies must be developed so that procedures are available to authorize access and exceptions
4. An individual (and designate), must be responsible for ongoing and timely account management (creation, modification, suspension, deletion) to reduce instances of password sharing and inappropriate access
5. Users must complete privacy training, sign a confidentiality agreement, and be made aware of office privacy policies before gaining access

Individual Disclosure Directives⁷ (Masking)

It is important that individuals have the ability to control access to their own personal health information that is stored within the EMR. This should be accomplished through the mechanism of individual disclosure directives, whereby some or all of an individual's personal health information is "masked" (not available to users of the system) at the individual's request. While not a legislated requirement in BC, disclosure directives has become the provincial standard as the province moves forward with electronic health initiatives such as the provincial Electronic Health Record. Individuals who do not wish to restrict access to their information do not have to prepare a disclosure directive.

Only with their consent (which could be in the form of a Personal Information Number (PIN) or keyword similar to PharmaNet), or in an Emergency, can this information be unmasked by an authorized user with the appropriate permissions.

Patient requests to suppress or apply restrictions to their personal information should be considered carefully. Best practices recommend that a physician explain the advantages and disadvantages to the patient, in addition to taking legal and ethical factors into consideration.

⁷ Provincial eHealth Disclosure Directives Policy, eHealth Privacy Working Group, BC Ministry of Health

Audit Trails and Auditing⁸

Audit trails are a functional technical requirement of EMRs providing the ability to track when a patient record is accessed, by whom, and when. No personal health information is captured in the audit trail; only user transactional activity is recorded identifying the “who, what, when, where” associated with access. Auditing can act as a deterrent to inappropriate access, ensuring that only users with a legitimate “need to know” are accessing information. It also supports the investigation of potential unauthorized access. As patients have become more aware of the existence of audit trails, patient access requests for copies of their audit report are becoming more common.

Typical data elements and activity transactions that are recorded include, but are not limited to:

- Username
- Patient name
- Date/time of access
- Screens accessed/viewed
- Masking/unmasking of data
- Printing

The audit trail cannot be modified and the ability to view and print audit reports should be limited to a few authorized individuals.

Audit trails do not, in and of themselves, monitor compliance. It is the responsibility of the Privacy Officer (and designate) to proactively verify and monitor that accesses made are appropriate. However, the EMR software may be able to support the ability to flag unusual, non-routine accesses based on business rules such as accessing masked data or browsing after regular office hours, which can assist in monitoring compliance.

Examples of business rules to consider when reviewing audit trails include:

1. Lookup of family members (e.g. same last name match between user and patient)
2. What patient records were unmasked?
3. Accessing patient data after regular office hours
4. What users accessed a particular patient record?
5. What patients did a user access?

While there is no provincial standard for how frequently proactive audits should be performed, it is recommended that monitoring of audit trails be scheduled in accordance with the organisational environment (e.g. high turnover of staff may require a more frequent view – biweekly vs. monthly). Any suspected inappropriate use should initiate an investigative process and confirmed breaches

⁸ Provincial Audit Policy, eHealth Privacy Working Group, BC Ministry of Health

should result in disciplinary action or referral to the appropriate professional regulatory body. Reactive auditing should also be conducted based on an incident or complaint.

The CMA Privacy Wizard

Best privacy practices suggest that privacy policies and procedures, staff confidentiality agreements, contractual obligations/clauses, privacy training for employees, and privacy information for patients, are important steps in meeting professional and legal requirements for the protection of personal information.

The Canadian Medical Association (CMA) Privacy Wizard was developed by the CMA to help physicians in their privacy compliance efforts. While it is an educational tool, it also assesses existing privacy practices, and helps produce the following:

1. A patient privacy notice that can be posted in the office
2. An office privacy policy for staff to follow
3. A list of privacy enhancements to further support compliance efforts
4. Confidentiality agreements/clauses

The Wizard was designed specifically for physician offices and provides a practical first step in making a private physician practice ready for the introduction of an EMR.

PITO has made the Wizard a mandatory requirement for completion prior to go-live. The Wizard takes approximately 15-20 minutes to complete. Physicians can also acquire CME credits for completing it.

One individual (or group of individuals) from each practice should complete the Wizard so that the output generated is consistent. The list of privacy enhancements will be reviewed with a PITO Relationship Manager and issues requiring mitigation in order to meet PITO requirements will be put into a plan of action.

The URL link to the CMA Privacy Wizard www.cma.ca/pito

Privacy Impact Assessments (PIAs)

A Privacy Impact Assessment (PIA) is an exercise to assess the risks associated with any initiative that may impact how personal information is collected, used, accessed and disclosed. Since the physician is ultimately accountable in all cases of privacy breaches, the process of completing a PIA ensures that 'due diligence' has been performed to mitigate risks and liabilities associated with privacy issues within the practice.

PIAs are not a legislated requirement under PIPA; however, PITO has deemed it a mandatory requirement if a site has been deemed to be more complex than the standard implementation (e.g. multiple organisations sharing a single instance of a database). A Relationship Manager will assist sites in determining if a PIA is necessary, and if so, a PIA template will be provided.

PITO Privacy and Security Go-Live Checklist

The final step of the PITO privacy implementation activities, the PITO Privacy and Security Go-Live Checklist will review the 10 Steps for PIPA Compliance as well as ensure that all PITO EMR specific privacy and security requirements are met. These include the implementation of a roles-based access model, the development of up-to-date office privacy policies, patient privacy notices, and the appointment of a Privacy Officer.

SECTION 4: PITO Privacy References

The following additional privacy references have been collated by the PITO Privacy Working Group as sources for further information. These have been provided as optional resources and do not reflect the views of PITO.

[BC Office of the Information and Privacy Commissioner \(OIPC\):
Office of the BC Information and Privacy Commissioner](#)

Provincial Privacy Legislation:

[Personal Information Protection Act \(PIPA\)](#)

[Freedom of Information and Protection of Privacy Act \(FOIPPA\)](#)

[Privacy Legislation for the Private Sector](#)

[BC Ministry of Management Services: PIPA Implementation Tools](#)

[BC Medical Association: Physicians and New Privacy Legislation \(PIPA\)](#)

Data Stewardship:

[BC College of Physicians and Surgeons: Data Stewardship Framework](#)

[Canadian Medical Association: Data Stewardship: Working Principles](#) 

Privacy Toolkits:

[BC Medical Association Privacy Toolkit](#)

[Vancouver Coastal Health Primary Care Privacy Toolkit](#)

[Canadian Medical Association Privacy Wizard](#)

Resources for Physicians/Practitioners:

[Canadian Medical Association: Protection of Health Information](#)

[Privacy Resources for Physicians' offices](#)

[Physicians and Security of Personal Information](#)

[Key Steps for Physicians in Responding to Privacy Breaches](#)

[Privacy in Practice: A Handbook for Canadian Physicians](#)

[Computerized Medical Records/Requirements](#)

[Fax - Use of Facsimile Transmission and E-mail by Physicians](#)

[Medical Records in Private Physician Offices](#)

[Medical Records - Maintenance of Security](#)

[Prescribing Practices – Countersigning Prescriptions and Internet Prescribing](#)

[COACH Guidelines for the Protection of Health Information 2007](#)

[Physician-Patient E-mail Communication: Legal Risks Information Letter](#)

[Safeguarding Privacy in a Mobile Workplace](#)

[Reduce Your Roaming Risks](#)


Privacy Codes, Ethics, Principles:

[Health information privacy code](#) 

[Plain language guide for physicians to CMA health information privacy code](#)

[Plain language summary \(CMA health information privacy code\)](#)

[Canadian Medical Association Code of Ethics](#) 

[Principles concerning physician information \(2002\)](#) 

SECTION 5: Roles-Based Access Model Template

FUNCTIONAL AREAS	ROLES									
	Physician	Nurse	Allied Health	Counsellor	MOA	Clerk	Coordinator	Manager	System Administrator	Other...
<i>Patient Registration</i>										
<i>Appointment Scheduling</i>										
<i>Patient Check-In</i>										
<i>Patient Assessment</i>										
<i>Care Plan</i>										
<i>Encounter Notes</i>										
<i>Counselling Notes</i>										
<i>Problem List</i>										
<i>Outgoing Referral</i>										
<i>Immunizations</i>										
<i>Alerts</i>										
<i>Allergies</i>										
<i>Prescriptions</i>										
<i>Incoming Results</i>										
<i>Billing</i>										
<i>User Account Management</i>										
<i>Auditing</i>										
<i>Reporting</i>										
<i>OTHER...</i>										