

PITO PHYSICIAN INFORMATION TECHNOLOGY OFFICE

PITO Privacy Orientation

Last revised: May 14, 2008

PITO PHYSICIAN INFORMATION TECHNOLOGY OFFICE

All you ever wanted to
know about EMR/PITO
Privacy.....and more!

Learning Objectives

- Identify and understand the impact of privacy legislation on the implementation of an Electronic Medical Record (EMR)
- Comprehend privacy principles, security safeguards and best practices
- Understand the challenges of implementing the EMR in a privacy environment
- Understand the PITO privacy activities as part of the overall PITO implementation activities

What is Privacy?

- “Privacy, including informational privacy, is grounded in man’s physical and moral autonomy and is essential for the well-being of the individual.”

La Forest J.

- “Privacy is the right to be let alone.”

Judge Thomas Cooley

What is Health Privacy?

- Ingrained in the Hippocratic Oath, 4th Century, BC

"Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not be raised abroad, I will keep silence thereon, counting such thing to be as sacred secrets."

- The right of a patient to exercise choice and control over the collection, use and disclosure of health information
- Patients always had a reasonable expectation that their medical records be kept secure and confidential

Privacy, Security & Confidentiality

- Privacy relates to people, process, accountability. It provides individuals with the ability to have control over their personal information.
- Security is an organisational control that prevents unauthorized access, use and disclosure. Security can be in the form of physical, technical, and administrative safeguards.
- Confidentiality is the obligation to protect information
- A *combination of privacy and security* methods along with *confidentiality awareness* are required to protect personal health information.

Privacy Challenges to consider when implementing an EMR

- Electronic collection and sharing of health information
- Sensitivity of personal health information
- Multiple users with greater access points
- Changes in locations/control of patient information
- Maintaining clear custody and control
- Accountability

Catalysts for Action

- ↑ introducing new technology & processes
- ↑ public awareness
- ↑ patient expectations
- ↑ high profile privacy breaches
- ↑ concerns over secondary uses of health data

Patient Attitudes

- A recent 2007 Canadian survey by Canada Health Infoway on Electronic Health Information and Privacy revealed:
 - 74% want strong penalties for unauthorized access
 - 77% want audit trails
 - 66% want privacy policies to protect health information
 - 55% want the ability to hide/mask sensitive information
 - 7 in 10 want to be informed and would like procedures in place to respond to privacy and security breaches

Legislative Framework

<p>BC Freedom of Information and Protection of Privacy Act (FOIPPA) governs public sector organisations (e.g. government, health authorities, hospitals).</p>	<p>BC Personal Information Protection Act (PIPA), governs private sector organisations (e.g. private physician offices, private labs).</p>	<p>Federal Personal Information Protection and Electronic Documents Act (PIPEDA) governs federally regulated commercial activities and does not apply to the health sector.</p>
---	--	---

Fair Information Principles

- Legislation is interpretable and interpretations vary
- Most privacy legislation is built around the 10 fair information principles

1. Accountability	6. Accuracy
2. Identifying Purposes	7. Safeguards
3. Consent	8. Openness
4. Limiting Collection	9. Individual Access
5. Limiting Use, Disclosure, Retention	10. Challenging Compliance

How Do Physicians Become PIPA Compliant?

- BCMA 10 Steps for PIPA Compliance
- The first 5 steps:
 1. Appoint a Privacy Officer (preferably a physician)
 2. Physicians and staff must understand PIPA and professional / regulatory standards and codes of ethics
 3. Review personal information handling practices
 4. Make necessary improvements
 5. Assess information handling practices in light of paper to electronic records transition

BCMA 10 Steps for PIPA Compliance cont'd...

The next 5 steps:

6. Establish an office privacy policy and patient privacy notice
7. Employees must receive privacy training
8. Revise forms and communications tools to inform patient about privacy and information practices
9. Ensure contracts with third parties include PIPA compliance requirements
10. Establish a process for privacy complaints

PITO Privacy Overview

- **PITO has been and is committed to supporting physicians in adopting adequate and reasonable privacy and security safeguards to protect personal health information**
- **Strategies include:**
 - Clear stipulations in the PITO Master Standing Agreement (MSA)
 - Contractual arrangements to ensure privacy and security of the Application Service Provider (ASP) model
 - Formation of the PITO Privacy Working Group
 - Comprehensive functional privacy requirements for the EMR software
 - Privacy activities integrated into the PITO Implementation Activities
 - Description of the Core Data Set and expectations in the PITO Registration Agreement
 - Information sharing and collaboration with the College of Physicians and Surgeons of BC & the Office of the Information Privacy Commissioner

PITO Privacy Implementation Activities

1. PITO Readiness Assessment
2. PITO Privacy Guide
3. PITO Privacy References
4. CMA Privacy Wizard
5. Privacy Impact Assessment (PIA)
6. PITO Privacy and Security Go-Live Checklist

PITO Readiness Assessment

- Evaluates existing PIPA compliance within physician practices
- Questions are based upon the BCMA 10 Steps to PIPA Compliance
- Helps practices understand current state and areas for improvement

PITO Privacy Guide

- An overview and understanding of best practices for privacy, security and confidentiality in light of the EMR
- Describes how PITO has responded to privacy risks, issues and concerns
- Describes the methods and strategies PITO has planned and implemented to support PITO sites in mitigating these risks

PITO Privacy References

- The PITO Privacy Working Group has reviewed a number of additional and optional privacy references that may be of use and of interest
- These are included in the PITO Privacy Guide as optional material

CMA Privacy Wizard

- The Canadian Medical Association developed the Wizard to support physicians in their privacy compliance efforts
- An educational tool that generates the following:
 - Office privacy policies and procedures
 - Patient privacy notice
 - Confidentiality agreements
 - Additional Privacy Enhancements
- Licensed by PITO as a PITO requirement
- 20 minutes to complete
- Physicians may obtain CME credits for completing

Privacy Impact Assessment (PIA)

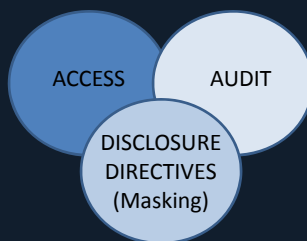
- PIAs are risk assessments completed for projects or initiatives that involve personal information
- Analyzes how personal information is collected, used, accessed, disclosed and ensures compliance with legislation, standards, best practices
- PIAs are mandatory for government, a best practice for public sector, but are not mandatory under PIPA
- PITO recommends a PIA when a site is deemed to be more complex, therefore increasing the privacy risks
- ↑ risks require ↑ due diligence

PITO Privacy and Security Go-Live Checklist

- A PITO Privacy and Security Go-Live Checklist must be completed prior to go-live
- The Checklist will ensure:
 - That a practice is reasonably compliant with PIPA
 - That privacy and security requirements and expectations have been taken into account in the design and implementation of the EMR

Provincial eHealth Privacy and Security

- Provincial eHealth Privacy, Security and Legislation Office of the BC Ministry of Health has spent the past year developing provincial privacy policies to guide Provincial eHealth, in collaboration with external stakeholders. The three key policies are:



PITO EMR Privacy: Roles-Based Access

- Appropriately accessing personal health information is an important aspect of privacy
- Access to an EMR is controlled through a roles-based access model defined by each physician practice
 - Supports the *balance between access to information and protection of privacy*
 - Ensures that access is based on 'need to know'
- Standard roles and associated permissions to ensure that authorized users have the appropriate access to support their job functions
- 'Exceptions' to these permissions may be required for users with unique roles as long as it is authorized and necessary to perform job functions

Who 'Needs to Know'??



Questions to Consider

1. Can existing users currently access 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?

PITO EMR Privacy: Account Management

- Timely and ongoing account management (create, modify, suspend and delete user IDs and passwords) is necessary to reduce the risks of password sharing and inappropriate access
- An individual (and delegate) must be appointed with the account management responsibility
- Access should not be provided until a user:
 - Completes EMR training
 - Is provided with privacy education
 - Signs a confidentiality agreement
 - Is made aware of office privacy policies and procedures

PITO EMR Privacy: Disclosure Directives

- Individuals must have the ability to control access to their personal health information in an EMR
- Individual Disclosure Directives allow individuals to 'mask' a portion or all of their personal health information from view/access
- Only under certain circumstances (e.g. Emergency or with consent) can information be temporarily 'unmasked' by an authorized user with the appropriate permissions
- Patient requests to apply restrictions must be considered carefully
- Physicians should explain advantages and disadvantages and take into account legal and ethical factors

PITO EMR Privacy: Auditing

- Audit trails are a functional requirement of EMRs that record when a patient record is accessed, by whom and when
- As audit trails are not modifiable, auditing can act as a strong deterrent to inappropriate access and can support privacy breach investigations and complaints
- They do not monitor compliance by themselves; a Privacy Officer is typically responsible for spot checks and routinely verifying that accesses made are appropriate

Final Thoughts

- While privacy risks are "*here, there, and everywhere*" they can be managed and reduced
- It is a balancing act: appropriate access and protection of privacy
- Use common sense - it's not as difficult as you think!