Regulation of Patient Management Software in Canada

James Williams – BA, BSc, JD, MSc,
Privacy and Security Consultant, Blue Pebble,
Phd candidate, University of Victoria.

Objectives:

1. Review regulatory regime for patient management software (PMS) in Canada.
2. Provide an overview of process-based versus product-based requirements.
3. Outline weaknesses and gaps.

Overview:

- Main sources of law pertaining to PMS:
  - Privacy statutes.
  - Health information statutes.
  - Guidelines and statutes regulating professionals.
  - Certification regimes and standards.
  - Medical device law.

Overview: PMS.

- What do we mean by Patient Management Software?:
  - Scheduling and Billing Software.
  - Electronic Medical Records.
  - Electronic Health Records.
  - Personal Health Records.

Overview: EMRs.

- Extend basic scheduling and billing applications.
- Give providers ability to manage and process medical information for use in clinical care.
- Not designed for interoperability.
- May include decision support.

Overview: EHRs.

- Provides shared access to medical information, across a variety of settings.
- **Complete**: integrates information from providers.
- **Life-long**: stores histories.
- **Accessible**: can be accessed at a variety of locations.
- **Secure**: provides protection for PHI.
- May include decision support.

Overview: PHRs.

- Health record controlled by the patient, rather than by the provider.
- Patients decide what is included, and who can see it.
- Often deployed as a hosted service.

Overview: why do we care?

- Why should we care about PMS?
  - PMS may be a key element in solving information accessibility problems in health care.
  - PMS is used increasingly for a variety of purposes, many of which impact patients directly.

Issues with PMS:

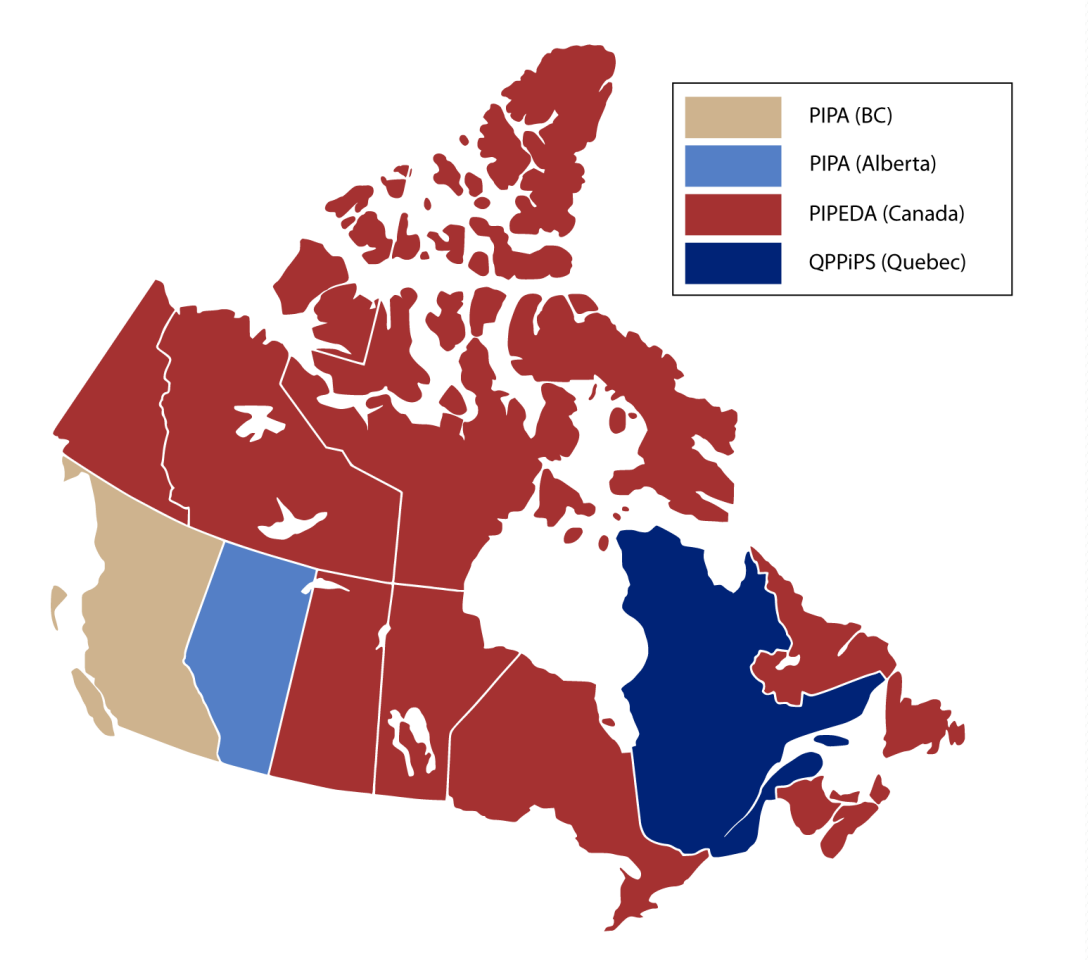
- human-computer **interface** difficulties
- system **inflexibilities** that prevent the integration of the system with existing workflows
- weak **privacy** and **security** safeguards
- failure to **integrate information** from all relevant information systems
- lack of **interoperability** mechanisms
- improper **customization** or configuration of features.
- Weak development **processes**.
- Composition and '**systems of systems**'.

Statutes: Privacy

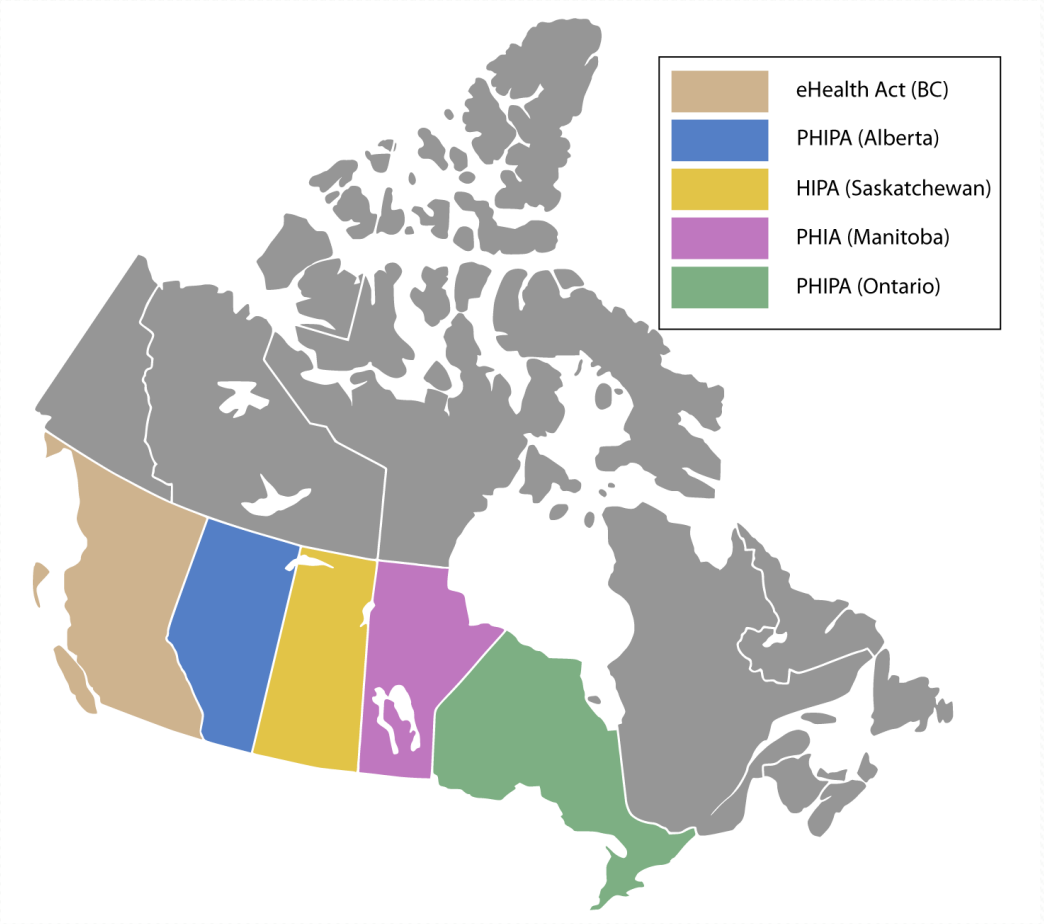
- The most important legislative instruments are the various **privacy** and **health information** statutes.
-
- Privacy legislation in Canada is based on a set of fair information practices:

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

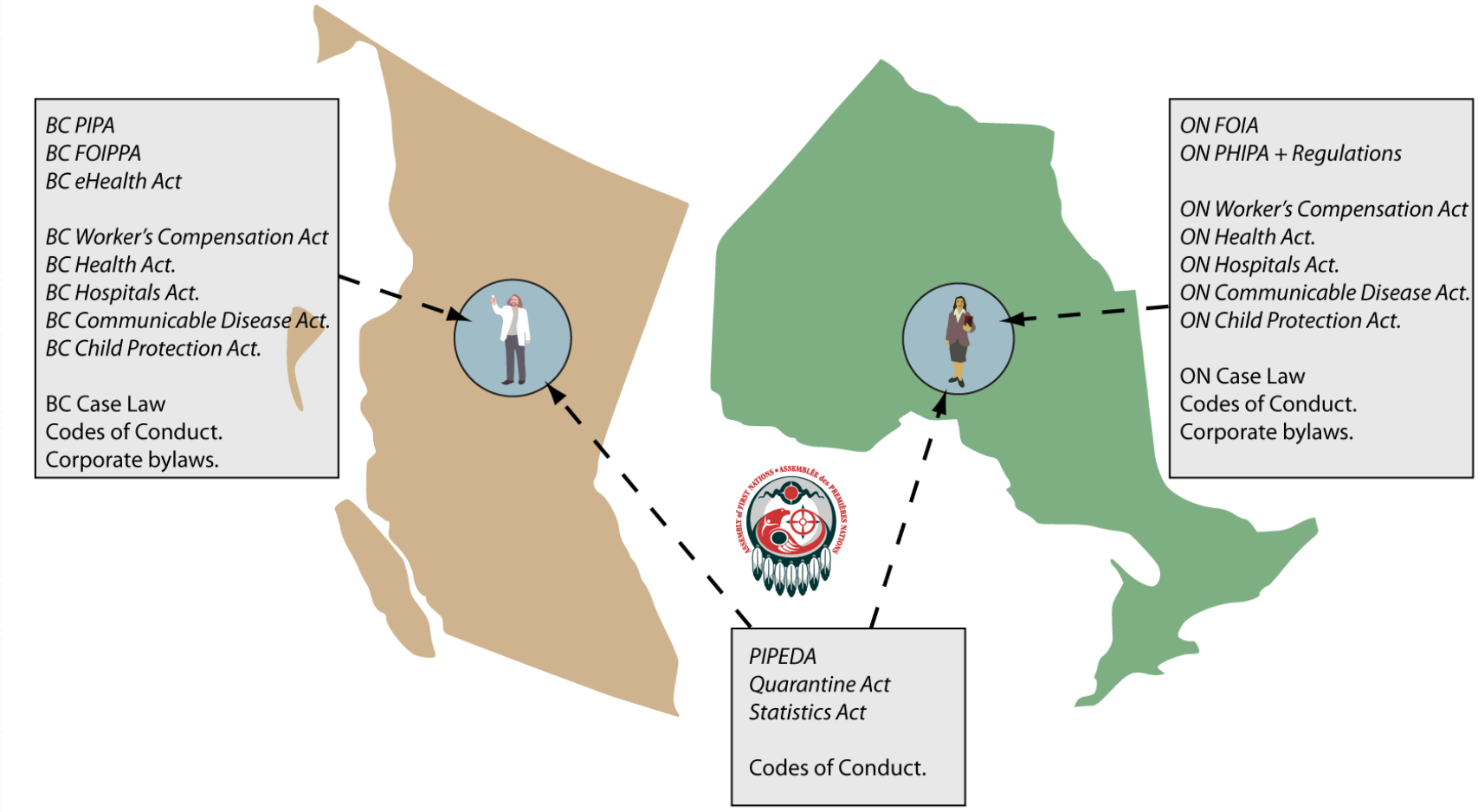
Private-sector privacy laws



Health information laws



The inter-provincial view:



Statutes: Privacy (cont)

- Import:
  - Imposes limits on collection, use, disclosure of PI/PHI.
  - Provides for rights of access and correction to PI/PHI.
  - Mandates certain administrative mechanisms.
  - Requires the use of 'reasonable' safeguards.
  - Requires organizations to maintain accuracy of information.

Statutes: Professional

- Self-regulated professions are empowered by legislation.
- Professionals are bound not only by guidelines and codes of conduct, but by statutory obligations.
- Eg: Ontario Medicine Act.
  - Only permits physicians to store patient records in an information system if certain conditions are met.
  - Audit trails.
  - Security safeguards.

Standards and Certification

- Two main certification regimes:
  - Canada Health Infoway:
    - Voluntary. Set up for "*client registries, consumer health application & platforms, Immunization registries, and provider registries*"
    - Main focus is on **privacy** and **security**.
    - Interoperability assessed against CHI's architecture.
    - Details guarded very carefully, and not available to us.
  - Provincial:
    - Concerns EMRs only.
    - Basic privacy/security and data interoperability.

Other sources

- **Case Law:**
  - Eg: Patient has right of access to their own health record. (*McInerney v MacDonald*).
- **Codes of Conduct:**
  - Eg: Canadian Medical Association, *Health Information Privacy Code* (1998).
- **Corporate bylaws:**
  - Hospital policies and procedures.
  - Municipal Information Acts.
- **Best Practices**
  - COACH Guidelines for the Protection of Health Information.

Medical Device Law:

- Canada has a fairly detailed medical device regime.
- Uses a risk management approach. Devices classified according to risk level:
  - Class I: Low risk. Tongue depressors.
  - Class II: Low-Med risk.
  - Class III: Med-High risk.
  - Class IV: High risk. Pacemakers.
- Devices also classified by type: active, invasive, etc.
- PMS is an active device.

Lifecycle of a Medical Device:

- The World Health Organization provided a phased model of a device's lifecycle:

  1) conception and development
  2) manufacturing
  3) packaging and labeling
  4) advertising
  5) sale
  6) use, and
  7) disposal

- (where is maintenance in this list?)

Basic Structure of CDN approach:

- A variety of controls:
  - Pre-market.
  - Market.
  - Post-market
- Applies to products ‘sold’ in Canada.
  - Broad definition.
  - But not ‘custom made’, ‘imported for special access’, or used for investigational testing.

Controls: pre-market

safety and effectiveness requirements.

- attempt to reduce the **risks** inherent the **device** itself.
- deal with the **design**, **manufacture** and **labeling** of the device.
- Included in the requirements are provisions relating to **safety**, **performance**, **deterioration**, and risk management. Most concepts relate to hardware.
- Manufacturers are obligated to maintain records demonstrating that the safety and effectiveness requirements are met by their products.

Controls: pre-market (cont)

- **12.** A medical device shall **perform as intended** by the manufacturer and **shall be effective** for the medical conditions, purposes and uses for which it is manufactured, sold or represented.
- **20.** If a medical device consists of or contains **software**, the software shall be designed to perform as intended by the manufacturer, and the performance of the software shall be **validated**.

Controls: pre-market (cont)

- **10.** A medical device shall be designed and manufactured to be **safe**, and to this end the manufacturer shall, in particular, take reasonable measures to
- (*a*) identify the **risks inherent** in the device;
- (*b*) if the **risks** can be **eliminated**, eliminate them;
- (*c*) if the risks cannot be eliminated,
  - (i) **reduce** the risks to the extent possible,
  - (ii) **provide for protection** appropriate to those risks, including the provision of alarms, and
  - (iii) provide, with the device, **information** relative to the risks that remain; and
- (*d*) **minimize the hazard** from **potential failures** during the projected useful life of the device.

Controls: pre-market (cont)

- Licensing:
  - Establishment License:
    - Section 44 of the Medical Devices Regulations prohibits a person from importing or selling a medical device without a license.
    - Valid for one year.
  - Device License:
    - Required for class II and above.
    - Requirements vary with risk level, and with type.

Controls: pre-market (cont)

Device License Requirements for Class II devices:

- 32(2) An application for a Class II medical device licence shall contain, in addition to the information and documents set out in subsection (1), the following:
  - (*a*) a description of the **medical conditions**, purposes and uses for which the device is manufactured, sold or represented;
  - (*b*) a list of the **standards** complied with in the manufacture of the device to satisfy the safety and effectiveness requirements;
  - (*c*) an attestation by a **senior official** of the manufacturer that the manufacturer has **objective evidence** to establish that the device meets the safety and effectiveness requirements;
  - …
  - (*f*) a copy of the **quality management system certificate** certifying that the quality management system under which the device is manufactured satisfies National Standard of Canada CAN/CSA-ISO 13485:03, *Medical devices — Quality management systems — Requirements for regulatory purposes*.

Controls: pre-market (cont)

- ISO-13485:
  - based on the generic ISO-9001 quality management standard
  - a *process-focused* approach to quality management, as opposed to a *product-focused* approach
- Obligations include:
  - (a) maintain a set of **key documents**
  - (b) assign defined **management responsibilities**
  - (c) maintain a **focus on quality**, throughout the development of human and infrastructure resources
  - (d) utilize **relevant communication processes**, such as customer complaint procedures and advisory notices.
- The standard prescribes aspects of technical as well as non-technical product lifecycle processes, such as installation and purchasing.
- ISO-13485 requires manufacturers to assign products **unique identifiers** (for tracking returned products), and to establish **traceability** between product documentation and the uniquely identified products themselves, which are conforming to the documentation.

Controls: pre-market (cont)

Minister can order tests:

- 36(2) The Minister may set out in a medical device licence terms and conditions respecting
  - (*a*) the **tests** to be performed on a device to ensure that it continues to meet the **safety and effectiveness requirements**; and
  - (*b*) the requirement to submit the results and protocols of any tests performed.
  - (3) The Minister may **amend the terms and conditions of the medical device licence** to take into account any new development with respect to the device.
  - (4) The holder of the medical device licence shall comply with the terms and conditions of the licence.

Controls: pre-market (cont)

Minister can also:

- Compel production of information (section 39)
- Suspend a license. (section 40).

- Vendors must:
  - Provide annual reports. Describing any changes, and attesting that their document is still correct.
  - Apply for a change to their license, if the device has changed.

Controls: pre-market (cont)

- **Application for a Medical Device Licence Amendment**
- **34.** If the manufacturer proposes to make one or more of the following changes, the manufacturer shall submit to the Minister, in a format established by the Minister, an application for a medical device licence amendment including the information and documents set out in section 32 that are relevant to the change:
  - (*a*) in the case of a **Class III or IV** medical device, a **significant change**;
  - (*b*) a change that would affect the **class** of the device;
  - (*c*) a change in the **name** of the manufacturer;
  - (*d*) a change in the **name** of the device;
  - (*e*) a change in the **identifier** of the device, including the identifier of any medical device that is part of a system, test kit, medical device group, medical device family or medical device group family;
  - (*f*) in the case of a **Class II** medical device, a **change in the medical conditions, purposes or uses for which the device is manufactured, sold or represented**.

Controls: market

These attempt to address the way in which the device is advertised and sold.

Establishment licensing is a form of market control, giving Health Canada full information on the players in the marketplace.

Another control concerns advertising. Misleading claims and the like.

Controls: post-market

Uncovering new information about a device by monitoring the performance of medical devices that are in use

Requirements in the Canadian regulations:

- **Complaint** Handling
- **Distribution** records (sufficient for rapid withdrawal)
- **Problem** reporting.
- **Recall** (must have plans in place).

Evaluation

- Some major themes:
  - Security/Privacy
  - Safety
  - Effectiveness

Eval: Security/Privacy

- Contained largely in privacy legislation, and in odds and ends like the Ontario Medicine Act.
- Unclear whether security and privacy concerns are 'risks' with respect to medical device regulation.
- Gaps:
  - No unified vision for information security.
  - Incorporating P+S concerns into lifecycle. Privacy by design is a start, but not enough.
  - Lack of precision with respect to security.

Eval: Safety

- MDR clearly addresses safety and risk.
- In addition, some requirements will help process maturity.
- Gaps:
  - Software safety is not the same as hardware safety.
  - Lifecycle controls not adequate. No requirement to relicense.
  - No attention paid to source code. Validation requirements help, but the source code is the ultimate source of information about the true design.

Eval: Effectiveness

- Licensing regimes require demonstrations of effectiveness.
- Gaps:
  - No guidance on how to evaluate effectiveness of PMS.
  - Interoperability not addressed. Section 18 states "*a medical device that is part of a system shall be compatible with every other component or part of the system with which it interacts and shall not adversely affect the performance of that system.*" But it does not deal with dynamically configurable systems.
  - Labeling requirements and purpose specification.

Eval: misc

- Other issues:
  - Hosted versus non-hosted.
  - Customized versus COTS.
  - Recall. Not so easy for PMS.
  - Monitoring. Approach may not be sufficient.
  - Enforcement and incentives.