# Privacy in Healthcare:

Presentation for : CIAJ, October 16, 2014

By: Robin Gould-Soil, Director Privacy and Access
Chief Privacy Officer,  University Health Network

UHN
Toronto General
Toronto Western
Princess Margaret
Toronto Rehab
COURAGE LIVES HERE

# Presentation Overview

- **PIPEDA - PHIPA -differences**
- **Changing business drivers**
- **Increased Privacy and Security risk**
- **Changing life of a healthcare CPO**
- **Challenges that we are seeing**
- **What we can do**

UHN Toronto General Toronto Western Princess Margaret Toronto Rehab
COURAGE LIVES HERE

# PIPEDA - PHIPA – Differences

- PHIPA provides more detailed rules and provides some additional flexibility in privacy practices for the health sector
  - custody and control
  - applies generally to only personal health information
  - provides more workable consent procedures for the collection, use and disclosure of personal health information
  - requires everyone to establish a role and their legal authority
  - provides for more options for using and disclosing personal health information without the client's consent
  - clients have the right to be advised of privacy breaches
  - Information Technology (IT) suppliers to custodians must comply with certain standards.
  - provides for a more health-specific system for client access and correction of their records.
  - Commissioner has broad powers of investigation and can order a custodian to comply with their PHIPA obligations.
  - Custodians are also subject to prosecution for breaches of PHIPA and to civil actions for damages, including a maximum of $10,000 for mental anguish
  - rules around specific type of data use – research and fundraising

# Changing Business Drivers

1. **Ontario's Transforming Health Care System**
   - Community Health Links provides coordinated, efficient and effective care to patients with complex needs
   - Shared electronic systems to support these activities

2. **Changing Healthcare Actors**

   - Employers - Wellness programs
   - Health Equity
   - Community Services – supporting services being provided by non-regulated professionals
   - Technology Companies - Apple, Facebook; Global innovation – funding projects

3. **Patient Perspective**
   - Patients and families engaged as Partners in Care

4. **Research Profile Changing**
   - Big Data – ethics
   - Integration of clinical trials (research) with clinical care

# Increased Privacy and Security risks

1. **Shared Electronic Systems with Shared Accountability**
   - Hospital Information Custodians – maintain accountability of the information, but they do not have the same authority
   - Increased risk of unauthorized access
   - Patient understanding their rights as we transition to new models

2. **Changing Roles**
   - Convergence of private sector models and healthcare models

3. **Old Rules Are Being Challenged**
   - Who owns what part of what data
   - Record retention – destruction, termination, training
   - What is an electronic health record?

4. **Security Threats are changing**

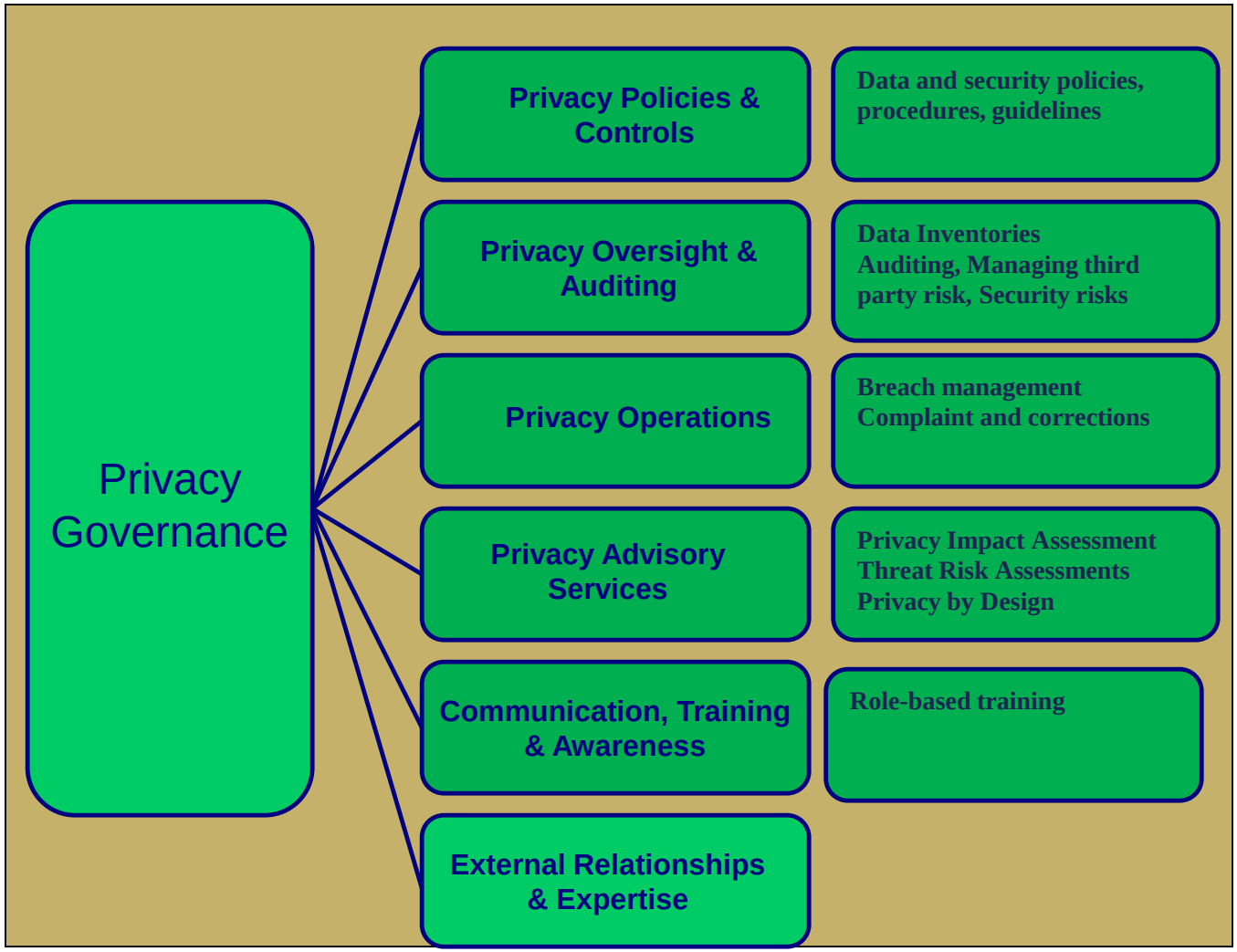
5. **Class Actions**

6. **Growing Compliance  Activities**

7. **Changing of Guards**

# Changing life of a CPO - Constant Framework

Privacy strategy and direction for the enterprise, and decisions on key privacy issues.



# Changing life of a Healthcare CPO

| Function | Current State | Future State = Current plus…. |
|---|---|---|
| **Privacy Policies & Controls** | • Organizational policies | • Shared electronic system policies outlining in detail roles and responsibilities |
| **Oversight and Monitoring** | • Employee signs organizational confidentially agreement<br>• Ensure notices were up and running<br>• Limited compliance reviews – mostly done through accreditation reviews | • Increased compliance monitoring in departments<br>• Introduction of attestation processes<br>• Multiple end-user agreements for shared systems |

# Changing life of a Healthcare CPO

| Function | Current State | Future State = Current plus |
|---|---|---|
| **Operations** | • Organizational incident management<br>• Audits review completed<br>• Complaint and correction<br>• Access Requests<br>• Consent directives management<br>• Notice | • Increased audits on existing systems and people<br>• New audits from shared systems<br>• Coordinated complaint and correction handling<br>• Additional notification to patients on consent directive<br>• Changed notices |
| **Advisory Services** | • PIA and TRA's<br>• Contract reviews | • Less impact on whether agree with mitigation plans because run through governance committee<br>• Privacy by Design in technology solutions |
| **Training and Awareness** | • One time organizational training | • Refresher training<br>• shared system training – role based and more detailed |

# Challenges that were seeing

1. Implementing a privacy program that will meet regulators' expectations or contractual requirements such as governance, training, vendor management, secure retention & disposal, change management, or responding to incidents

2. Small sites are having difficulties resourcing the new operational and technical controls required to support a shared electronic system

3. Contracts becoming very complicated and require extensive legal review

4. Uses that were not anticipated in shared systems
   - Training
   - De-identification for other uses
   - Benefits analysis
   - Administration of the system

5. Networks participating in Shared Electronic Systems

6. Different interpretation of business rules – or the solution not evolving at the same pace

7. Transition into new models – impact on business and patients

8. What should be the penalty for non-compliance with policies

# What can be done

1. Funding a transition strategy for organizations to move towards the model – technology, process and people
2. Standard contract language for all shared electronic systems
3. Governance body that includes membership from all relevant stakeholders
4. Contracts that include responsibilities for managing privacy program
5. Harmonized policies and procedures for all shared electronic systems that contain clear roles and responsibilities for all participants
6. Investment in standardized security controls
7. Harmonized training for all shared systems
8. Legislative reform

# Questions?

# Appendix - Health Information Network Provider obligations

| | |
|---|---|
| 1 | Perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to:<br>• threats, vulnerabilities and risks to the security and integrity of the personal health information;<br>• how the services may affect the privacy of the individuals who are the subject of the information |
| 2 | Notify every health information custodian at the first reasonable opportunity if it accessed, used, disclosed or disposed of personal health information in an unauthorized manner |
| 3 | Provide to each health information custodian a plain language description of the services provided and safeguards that have been implemented to protect personal health information against unauthorized use or disclosure |
| 4 | Make available to the public a plain language description of the services provided and safeguards that have been implemented to protect personal health information against unauthorized use or disclosure and any directives, guidelines and policies that apply to the services provided (in addition to the services & safeguards employed by a participating HIC) |
| 5 | Retain and provide to the health information custodian, upon request, an electronic record of all accesses and transfers of personal health information associated with the health information custodian |
| 6 | Ensure that any third parties retained to provide or assist in providing services also comply with the necessary restrictions and conditions to allow providers to comply with its requirements |
| 7 | Enter into a written agreement with each health information custodian describing the services provided; describing the administrative, technical and physical safeguards in place to protect the confidentiality and security of the personal health information; and requiring the provider to comply with PHIPA and its regulations |
| 8 | Make available to the public a plain language description of the services provided and safeguards that have been implemented to protect personal health information against unauthorized use or disclosure and any directives, guidelines and policies that apply to the services provided (in addition to the services & safeguards employed by a participating HIC) |