FORWARD TOGETHER

MILLER THOMSON

AVOCATS | LAWYERS

WELCOME

VANCOUVER CALGARY EDMONTON SASKATOON REGINA LONDON KITCHENER-WATERLOO GUELPH TORONTO VAUGHAN MARKHAM MONTRÉAL

MILLER THOMSON
AVOCATS | LAWYERS

FORWARD TOGETHER

Privacy and Cyber Risk and Governance for FHTs

Kathryn Frelick

October

Presenter Disclosure

- **Presenters:**
- Declan Friel, HUB International;
- Kathryn Frelick, Miller Thomson;
- Vanessa Foreman, Hamilton FHT

- **Relationships with commercial interests:**
  - **Not Applicable**

Disclosure of Commercial Support

- **This program has not received financial or in-kind commercial support.**
- **In support of this program, there are no potential conflicts of interest**

Overview

- Evolving Concepts of Privacy
- Application of PHIPA to FHTs
- Trends - Privacy and Cyber Risk
- Managing privacy and cyber risk - ERM

Evolving Concepts of Privacy

- No traditional right to privacy in Canada
  - could not sue for breach of privacy
- In health sector, focus on confidentiality and professional obligations
  - access to and disclosure of health records

Evolving Concepts of Privacy

- *Personal Health Information Protection Act, 2004* (Ontario) (PHIPA)
  - established rules for the collection, use and disclosure of PHI about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information …. while facilitating the effective provision of health care

Application of PHIPA to FHTs

- PHIPA applies to Health Information Custodians (HICs) that collect, use or disclose PHI
  - HIC - a person or organization (in one of the enumerated groups) who has custody or control of PHI as a result of or in connection with performing their powers or duties

HIC (Enumerated Groups)

- Health practitioner or person who operates a group practice of health practitioners
- Home or community care service provider
- Person who operates a:
  - Hospital
  - Psychiatric Facility
  - Long Term Care Home
  - Retirement Home
  - IHF
  - Laboratory
  - Pharmacy
- Centre, program or service for community health or mental health whose primary purpose is the provision of health care

FHTs, CHCs, NPLCs are not specifically enumerated

Board Responsibility for Privacy

- Corporate responsibility for reasonable policies and “systems” oversight
- Legislative compliance
- Privacy protection of personal information → corporate obligation
- “Person who operates” = corporation (HIC)
- Obligation rests with the HIC – whether corporation or individual

HIC Obligations

- Must comply with PHIPA
- Must adopt information practices (policies and procedures) that address:
  - when, how and the purposes for which PHI is c/u/d, retained, destroyed
  - administrative, technical and physical safeguards
- Reasonable steps to protect against theft, loss and unauthorized use or disclosure, unauthorized copying, modification or disposal

HIC Obligations (Cont'd)

- Must notify patient (or SDM) at first reasonable opportunity where PHI is stolen or lost or if it is used or disclosed without authority
  - entitled to make a complaint to IPC
- October 1, 2017 – New requirement to notify the IPC of the theft or loss or of the unauthorized use or disclosure of PHI in prescribed circumstances

HIC Obligations (cont'd)

- Must designate a contact person
  - Facilitate compliance
  - Inform agents of their obligations
  - Address inquiries, access and correction requests and receive complaints
- Written statement
  - Description of information practices
  - Contact person
  - How to access PHI/request correction
  - How to make a complaint

PHIPA Agents

- Agent - acts for or on behalf of the custodian in respect of PHI for the custodian's purpose …
- HIC is responsible for the actions of its agents
- Health practitioner is not a HIC where he or she is acting as an agent of a HIC (i.e. health professional employed by FHT or operator is HIC)
- New Requirement – must notify College where agent terminated, suspended, or disciplined as a result of unauthorized c/u/d, retention or disposal of PHI

How does PHIPA apply to FHTs (CHCs/NPLC)?

- Who is the Health Information Custodian?
  - PHIPA does NOT prescribe
  - Custody or control of PHI
- Ownership vs. custody
  - Ownership is not determinative of status under PHIPA
- Patient enrolled to designated physician or group of physicians and not FHT
- OntarioMD funding terms and conditions

Who is the Health Information Custodian?

- Wide variation depending on configuration …
  - Physician model – FHT and each physician is a HIC
  - Community model – physicians / NPs / other health practitioners employed by HIC
  - May designate FHT or practitioner to be the HIC
  - Combination – may retain separate responsibilities as HICs, but designate the FHT or lead physician to carry out certain common functions as agent

Implications?

- Roles and responsibilities are NOT CLEAR under PHIPA - must clearly set out in contractual agreements
  - Datasharing and access – driven by PHIPA
  - Administrative and operational functions
  - Infrastructure, technology, equipment, software licensing, funding, information security
  - Termination/withdrawal/change in practice

Datasharing or Access Agreements

- HICs sharing PHI to facilitate provision of health care = datasharing agreement
  - Shared EMR, eHealth initiatives
- Permitting a HIC or non-HIC access to PHI for a specific purpose = access agreement
  - physician HIC allowing FHT access to records of PHI
  - any time a vendor/supplier/third party will have access to PHI

Professional Obligations

- CPSO Medical Records Policy

  Security

  Data sharing agreements incorporating the requirements in this policy must be established among physicians and organizations who will be sharing patient health information with each other. This is especially important for physicians who share records (electronic or paper) with hospitals and other care facilities or that allow entries into the record by multiple health-care providers.

- OntarioMD
  - EMR and Data Migrations – Your Privacy and Security Obligations
  - Frequently Asked Questions – Privacy for Ontario Physicians and Staff

Privacy and Cyber Risk

- Very prevalent areas of risk today
- Exponential growth in use of technology, electronic medical records, electronic communications, medical devices and monitoring technologies, etc.
- Complex regulatory environment, evolving standards and resource constraints

What to Expect in 2017-2018?

Top 5 Trends to look out for:

1. Mandatory breach notification is here (PHIPA) or coming (PIPEDA)
2. Continued growth in cybersecurity and privacy litigation
3. Significant and continued growth of ransomware attacks
4. Vendor Management – Beware of the weakest link
5. Accelerated adoption of cyber insurance

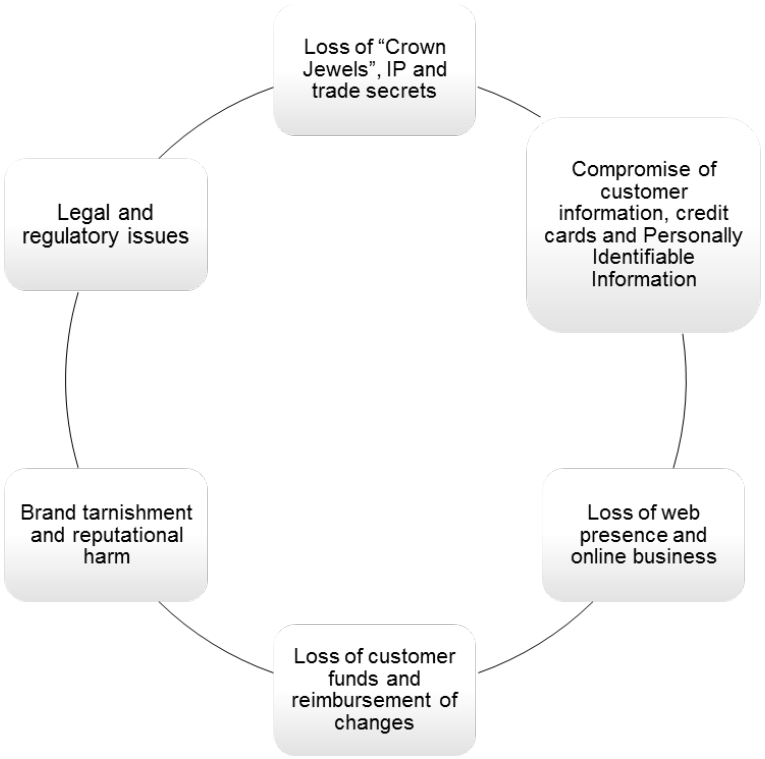
What information do you collect?

- **Patient / physician / employee information**
  - Financial and health info is deemed to be “sensitive” under privacy laws
- **Confidential & proprietary business information**
  - Intellectual property, research
  - Internal investigations
  - Business plans
- **Supplier or Purchaser confidential & proprietary information**

Understanding Privacy and Cyber Risk

- Risk of financial loss, disruption, stakeholder dissatisfaction, legal consequences or damage to the reputation of an organization relating to:
  - the collection, use, retention, disclosure of PHI (Privacy Risk)
  - some sort of failure of your information technology systems (Cyber Risk)
- Cyber threat may involve PHI and trigger privacy obligations

Risks to Organization



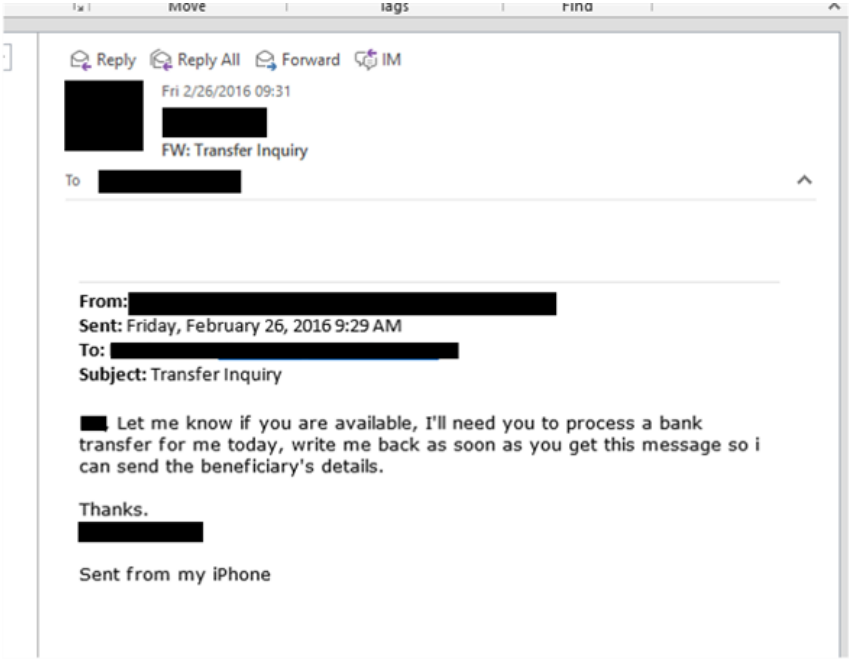
- Director and Officer liability
- **Legal liability including litigation**
- **Regulator enforcement and investigations**
- Failure to meet key contract terms
- Economic harm (e.g. loss of confidential information/IP)
- **Reputational harm**
- **Business interruption**
- Physical harm

Types of Privacy Breaches

- Unauthorized collection of PHI
  - Video camera, camera phones, personal devices
- Unauthorized disclosure of PHI
  - Lost or stolen laptop, computer equipment, storage devices
  - Inappropriate “recycling” or destruction of PHI
  - Intercepted video monitoring / wireless devices
  - Facebook / social media
  - Intentional behavior – selling PHI
- Unauthorized use of PHI
  - Staff inappropriately accessing health record

Types of cyber breaches

- **Classic cyber-attack:** Breaking into a network
- **DDoS attack:** Directing junk traffic to a site and bringing it down
- **Phishing attack:** Email with malware
- **Whalling attack:** Targeting senior management + fraud
- **Social Engineering:** Targeting specific individuals based on publicly available info.



Ransomware - Erie County Medical Center

- Ransomware attack in April, 2017
  - Hackers used “brute-force” computing to identify weak passwords and gain entry to the system
  - Encrypted files to make it more difficult to recover data
  - Demanded $44,000 ransom
  - More than 6,000 computers affected

Erie County Medical Center

- What happened?
  - The hospital did not pay the $40,000 ransom
  - Spent $5 million on new hardware, software and services to recover data and protect itself
  - Another $5 million in costs for overtime, loss of business, etc.
  - Ongoing expenses for investments in tech upgrades and employee education

What about in Canada?

'Doctors are under attack': Group says medical offices are regularly hit by ransomware

In the best-case scenario after the incidents, medical offices spend two or three days restoring their systems from backup sites

CMPA - The ransomware threat: Are you prepared?

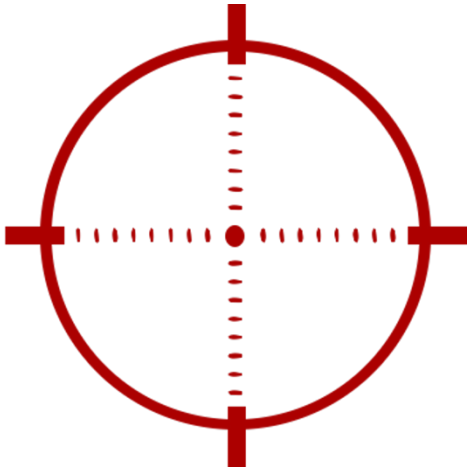
*https://www.**cmpa**-acpm.ca/.../**the-ransomware-threat-are-you-prepared***

A routine day at a busy community clinic suddenly turns frantic when its computer screens display an ominous message and accompanying instructions: “Your files are ...

Source: National Post

Why Healthcare and why now?

- **Health sector experiencing significant increase in intentional attacks**
- PHI is valuable
- Slow to adapt
- Wealth of information
- Vulnerable to human error
- Wide range of communications technologies



Privacy and Cyber Litigation

- Risk of identity theft
- Emerging privacy torts for breach of privacy
  - “intrusion upon seclusion”; “public disclosure of private facts”
- Significant increase in privacy class actions across Canada (still early stages)
  - Loss/theft of PHI (Durham Region, Rouge Valley)
  - Unauthorized access (snooping) (PRHC, North Bay)
- Reputational risk

Privacy and Cyber Litigation

- How you manage a breach will likely come under intense scrutiny - containment, notification, investigation and remediation
- Vicarious liability?
- Due diligence defence?

Amendments to PHIPA

- Penalties - fines for offences doubled
  - $100,000 - individual; $500,000 -corporations
- Prosecutions - removal of limitation period
- Amendments to privacy breach notification provisions and obligations re: agents
- Mandatory reporting - professional colleges
- Mandatory notification - IPC as of October 1, 2017

Preventing Privacy and Cyber Risk

- Prevention is the best strategy
  - Know where you stand – identify, assess, monitor and report on risks
  - “Systems” responsibilities
    - Information practices – policies, procedures and systems to address privacy and security
    - Information lifecycle – protect your informational assets from creation, storage, disposal, destruction

Preventing Privacy and Cyber Risk

- Monitoring and auditing compliance – not enough to have privacy and security policies
  - Audit trails, regular and random privacy audits, security testing
- Need to evaluate privacy and security standards as they evolve over time (i.e. use of fax, mail and courier, encryption, wireless systems)
  - Engage appropriate subject matter experts and ensure use of reputable vendors
  - Require vendors to demonstrate compliance

Preventing Privacy and Cyber Risk

- Training and education - **privacy and cyber risks are as much about people as they are technology!**
- Service provider management
- Risk assessment tools for new programs, systems, technologies including PIAs and TRAs
- Internal reporting – systems for identifying and preventing breaches

Privacy and Cyber Risk Management

- Well suited to enterprise risk management framework
- Align management's responsibility to manage operational risk and the Board’s responsibility to ensure risk oversight
- Management of risk within organization’s risk tolerance

ERM Strategies for Managing Risk

Risk Management Strategy	Examples
Avoid	Do not start or terminate program or activity (i.e. technology or software that does not meet organizational privacy and security standards)
Remove	Discontinue obsolete or faulty software or system
Change Likelihood (prevent or reduce)	Enhanced training, policy development or system improvement, PIA, TRA
Change Consequences	Privacy breach protocol / notification process
Risk sharing or risk transfer	Insurance Outsource or contract out
Retain Risk (informed decision)	Legacy systems and technologies

… still breaches can happen …

- Who to contact and what to do? At minimum …
  - Privacy Breach Protocol which addresses containment, notification, investigation and remediation
    - IPC – What to do when faced with a Privacy Breach – Guidelines for the Health Sector
  - Cyber incident plan
  - Crisis and disaster management
  - Data recovery

Best Practices for Reducing Liability

- Responding to privacy or cyber breaches can be extremely costly and time consuming!
- Early engagement of experienced legal counsel is critical (establish privilege for investigations)
- Significant public relations and legal risk, therefore, when and how individuals are notified is very important →ensure strong communication strategy

Best Practices for Reducing Liability

- Consider risk transfer and specialized insurance (i.e. D&O and cyber insurance)
  - First party coverage - system failure, forensic costs, privacy notification and look back programs, identity theft monitoring, computer extortion)
  - Some programs provide access to legal and other experts who have expertise managing these situations (breach coaches)
  - Third party – civil actions and class actions

Conclusion

- Awareness and engagement by the Board and senior leadership to foster effective decision-making
- Identification and prioritization of privacy and cyber risks and organizational priorities
- Allocation of resources (financial and human resources) to manage risks

FORWARD TOGETHER

MILLER THOMSON

AVOCATS | LAWYERS

MILLERTHOMSON.COM