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

Coffee Talk – Directors Series

Protecting Privacy: Obligations of Directors

Kathryn Frelick
kfrelick@millerthomson.com
416.595.2979

Agenda

1. Overview of key concepts, privacy legislation, Board obligations and information governance
2. Identifying new and evolving privacy and cyber risks
3. Strategies and best practices to manage and reduce risk and liability

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 (*Public Hospitals Act* and Regulation 965)

Key Concepts: Privacy

- **Privacy** – the right of an individual to control who has access to his or her personal information and under what circumstances

  → Informational Self Determination

Key Concepts: Confidentiality

- **Confidentiality** – obligation upon organization/person to protect information that has been entrusted in its care for a specific purpose, and to ensure that only accessible to authorized persons

  → Legal, professional, ethical and employment obligation

Key Concepts: Security

- **Security** – The preservation of the confidentiality, integrity and availability of personal information
- **Means** of safeguarding privacy and confidentiality

Board Responsibility for Privacy

- Corporate responsibility for reasonable policies and procedures and “systems” oversight
- Legislative compliance
- Privacy protection of personal information is a corporate obligation

Privacy Legislation – PHIPA

- Establishes 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**

Privacy Legislation – PHIPA (cont'd)

- Relates to personal health information (PHI) in custody or control of health information custodian (HIC)
- HIC = "person who operates … "

→ **ultimately this is the Board**

Privacy Legislation – 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
- **New Requirements**
  - Reinforce obligations on HICs and agents
  - HIC must notify College where agent terminated, suspended, or disciplined as a result of unauthorized c/u/d, retention or disposal of PHI

PHIPA 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

PHIPA Obligations (cont'd)

- Accuracy of PHI
- 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

PHIPA 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

Privacy Legislation – FIPPA/MFIPPA

- Provides a **right of access** to information held by institutions
  - Information should be available to public
  - Exemptions must be limited and specific
  - Independent body to review decisions on disclosure of government information (IPC)

FIPPA/MFIPPA

- Requirements to **protect the privacy** of individuals whose personal information is held by an institution and provide a right of access
  - Limits institution's collection, use and disclosure of PI
  - Personal information banks

FIPPA Obligations

- Right to request access to any document/record in custody or control of institution
- Must produce subject to limited exclusions/exemptions

FIPPA Obligations (cont'd)

- Process driven – specified timelines for response, manner of corresponding, dealing with third party information
- Significant case law around exemptions
- Statutory right of appeal for refusals (to IPC)
- Personal Privacy – Specific rules relating to access, collection, use, disclosure of personal information/accuracy and security

FIPPA Obligations (cont'd)

- Practically speaking, one of the biggest impacts relates to document management processes
  - How we document
  - What we document
  - How we store and retrieve information
  - Retention and destruction of information
- Directory of Records
  - Obligation to provide Minister of Government Services with information about the types of records in the custody or control of the institution annually

FIPPA Obligations (cont'd)

- "**Head**" of institution is responsible for:
  - Decisions made under FIPPA by the institution
  - Overseeing the administration of the Act
- Head for public hospital = **Chair of the Board**

Delegation

- Head may **delegate** powers or duties
  - Must be in writing – senior leadership/FOI
  - May be subject to limitations, restrictions
- Head must adhere to delegation of authority
- Head remains accountable for actions taken and decisions made

Information Governance

- Privacy and security fit within broader framework of information governance
- Organization wide framework for managing information throughout its life cycle and for supporting the organization's strategy, operations, regulatory, legal, risk and environmental requirements (AHIMA)

Goals of Information Governance

- Ensure legislative and regulatory compliance
- Increase accountability and transparency
- Minimize litigation risks
- Preserve organizational history
- Ensure business continuity
- Reduce operating costs and improve efficiency
- Safeguard essential information and preserve corporate memory

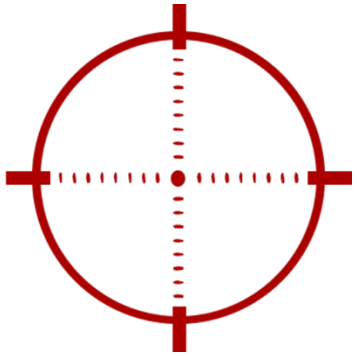
New and Evolving Privacy and Cyber Risks

- 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

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**

Why Healthcare?



- PHI is valuable
- Slow to adapt
- Wealth of information
- Vulnerable to human error
- Wide range of communications technologies
- Investments in IT security and privacy training not keeping pace

Privacy and Cyber Risk Trends

- Significant increase in cyber attacks
- Increasing concern regarding 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
  - Loss/theft of PHI, unauthorized access (snooping)
- **Reputational Risk**

Strategies to Reduce 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

Strategies to Reduce Risk (cont'd)

- 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

Strategies to Reduce Risk (cont'd)

- 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 (cont'd)

- 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