Privacy Update – Recent Updates in Privacy Law

Kathryn Frelick
Overview

1. Can you be sued for a privacy breach? Privacy class action update and the implications of Ontario’s new privacy tort
2. Recent developments under PHIPA and FIPPA
3. Recent cases – Freedom of information
Can you be sued for breach of privacy?

- In Canada, traditionally no independent action for breach of privacy
- Typically tied to something else (i.e. constructive dismissal, breach of contract, trespass, negligence, breach of fiduciary duty)
Can you be sued for breach of privacy?

- May be statutory basis (i.e. PHIPA)
- Increasing concern regarding risk of identity theft (i.e. fraud/credit monitoring, need for protective measures)
- Significant increase in privacy class actions in Canada
  - Loss/theft of PHI (i.e. Durham Health Region)
  - Business practices / unauthorized access by employee(s) (i.e. recent certification of class action lawsuits against Regional Health Authorities in Newfoundland and Nova Scotia)
Privacy Breach – Statutory Basis

- Limited recourse under PHIPA for breach of privacy
- Offences under the *Provincial Offences Act*
  - Significant fines
- Action for damages for breach of PHIPA
  - Statutory right to seek compensation from Superior Court for breach of privacy for *actual harm* suffered where order issued by IPC or conviction
  - damages for mental anguish capped at $10,000 (payable where willful or reckless)
Durham Health Region Class Action

- December 2009 - Nurse loses unencrypted USB key with PHI of 83,500 individuals immunized for H1N1
- January 2010 - IPC Order HO-007 – strong encryption for mobile storage devices
- December 2011 - Class action certification motion
  - $40 million damages (negligence, breach of statutory duty, breach of fiduciary duty)
  - Primary concern - identity theft
Durham Health Region Class Action

• July 2012 – class action settlement approved
  – $500,000 in costs to counsel, plus % of claims paid
  – Must demonstrate economic loss, otherwise, no damages
  – Opportunity to mitigate loss

• Mr. Justice Lauwers:
  – Risks from lost data “negligible”
  – No evidence of identify theft / minimal information
Class Actions – Unauthorized Access

• Recent class action law suits related to privacy breaches / unauthorized access to EHRs
• Hospitals notifying patients and managing breach
• Termination / discipline

• Early stages
  – Vicarious liability – is hospital responsible for *intentional* behaviour of employee?
  – Systems responsibilities - adequate training, policies and procedures and systems in place to monitor policies?
New Privacy Tort – Intrusion upon Seclusion

- Ontario Court of Appeal - *Jones v. Tsige*

- Bank employee accessing personal bank account of spouse’s ex-wife (another bank employee) 174 times over 4 year period

- Brought motion for summary judgment on the basis that Ontario law does not recognize tort of breach of privacy

- CA determined that there ought to be a right of action for ‘intrusion upon seclusion’ in certain situations where there has been a deliberate and significant invasion of personal privacy
Three elements - Intrusion upon seclusion

- Conduct must be intentional (or reckless)
- Individual must have invaded, without lawful justification, another’s private affairs or concerns
- A reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish
  - Objectively, only certain types of intrusions highly offensive i.e. involving financial or health information, employment, diary, personal correspondence
Damages for Intrusion Upon Seclusion

• No need to demonstrate harm to economic interests or actual loss

• Damages for intrusion upon seclusion will be relatively modest (i.e. capped at $20,000)
Implications for Health Industry Clients

• Extends beyond PHI to other types of personal information

• Actions may be contrary to organizational policy (employee discipline), but may still be exposed to potential law suits / class action law suits

• Significant public relations and legal risk, therefore, when and how individuals are notified is very important → ensure strong communication strategy
Implications for Health Industry Clients

• Risk management
  – Adequate policies and procedures
  – Privacy breach management
  – Training, monitoring and auditing compliance coming under increasing focus

• Consider risk transfer (i.e. privacy notification and look back programs, identity theft monitoring)
Review Orders/Decisions

• A review of Orders issued under PHIPA, as well as corresponding fact sheets and guidance documents reveal that many of these repeat the SAME THEMES …
  – Failure to use appropriate encryption or other safeguards when storing PHI on mobile devices
    • Limit ability to remove PHI unless adequate safeguards are in place
  – Improper disposal/destruction of PHI
    • Document management and retention policies
    • Contractual protections when relying upon third party
Recent Developments – PHIPA and FIPPA

• PHIPA Order HO – 011 – October 2011
  – Cancer Care Ontario in its role as a “prescribed person” (Ontario Cancer Screening Registry)
  – Delivery of screening reports to over 7000 physicians in paper format (sent by courier)
Recent Developments – PHIPA and FIPPA

• Key findings:
  – Need to evaluate privacy and security standards as they evolve over time
  – Consider whether the use of fax, mail and courier services are adequate given technological advances
  – Put practices in writing

• IPC Fact Sheet # 18 – August 2012 – Secure Transfer of Personal Health Information
Recent Developments – PHIPA and FIPPA

• July 2012 - Elections Ontario losing unencrypted USB key involving personal information of up to 2.4 million individuals
  – Failure to effectively implement and monitor privacy practices

• IPC White Paper - A Policy is Not Enough: It Must be Reflected in Concrete Practices – September 2012
Recent Decisions – Freedom of Information

• Carleton University (IPC, Feb. 2012)
  – **Presumption** that an access request for emails does not require routine search of backup tapes for deleted emails
    • Exception - unless there is a reason to assume that such a search is required
  – If individual requests search from backup tapes, must search and retrieve
Recent Decisions - Advice and Recommendation

• Ontario Court of Appeal – finding that IPC applying “advice and recommendation” exemption too narrowly
  – Entire deliberative process is protected (not necessary to go to final decision maker)
  – Presentation of range of options may be properly withheld

• leave to appeal to SCC filed (May 15, 2012)

Ontario (Finance) v. Ontario (Information and Privacy Commissioner)
Recent Decisions – Third Party Information

• Supreme Court of Canada decision - *Merck Frosst v. Canada (Health)*
  – Outlines procedural and substantive protections for third parties
  – Although deals with federal *Access to Information Act*, likely will apply more broadly
  – No single interest is paramount (i.e. duty to provide access equally important as duty to protect third party information)
Recent Decisions – Third Party Information

- Threshold to trigger notice obligation is low
  - no need to provide notice where information clearly exempt or clearly subject to disclosure, but otherwise, must provide notice

- While third party assistance may be required, the decision to disclose ultimately lies with institution - head must apply the exemption / conduct thorough analysis

- Only where third party believes decision is wrong does the onus shift to third party

- Decision also considers substance of tests and threshold for harms-based exemptions
Questions?

Thank you!