



Confidence in a connected world.



Strategizing Privacy in Health Care

Constantine Karbaliotis, LL.B., CIPP, CIPP/C

April 18th, 2007

1 Introduction

2 Legislative Directions

3 IT & Personal Information in Health Care

4 Strategic Approaches

5 Conclusion



Confidence in a connected world.

Introduction

Stolen laptop a sign Canada complacent about ID theft: Ontario privacy czar



- TORONTO (CP) - Hospitals and businesses need to do a better job of ensuring personal information doesn't fall into the wrong hands - especially as increased mobility leaves organizations even more exposed to breaches of security, Ontario's privacy commissioner warned Thursday....The commissioner issued an order Thursday urging the Hospital for Sick Children to introduce new protective measures following the theft of a laptop in January that contained information about 2,900 patients.

<http://www.cbc.ca/cp/health/070308/x030811A.html>

Teens Arrested In VA Laptop Theft



Two Maryland teens were arrested early on August 5th in connection with the theft of a laptop belonging to the Veterans Administration (VA), which contained unprotected personal data on 26.5 million veterans...

The analyst who had taken the laptop home with him and was burglarized had not previously been identified, due to the ongoing investigation. The *Washington Post* identified him as Wayne Johnson, a government worker who had been with the VA for more than thirty years.

Johnson had been taking data home to work on for as long as three years without authorization, according to a scathing report by VA Inspector General George Opfer on the agency's data security practices.

Although Johnson immediately notified the agency of the theft, VA Secretary Jim Nicholson did not hear about it for several days, and did not inform the public until several days after he himself found out, according to the *Post*.

www.consumeraffairs.com: August 6, 2006

Commissioner launches immediate investigation into disclosure of actual patient records to film company



- Ontario Information and Privacy Commissioner Ann Cavoukian launched an investigation Monday morning into how patient records ended up on being strewn across Toronto streets to help a film company make the site look like New York City after 9/11.
- www.ipc.on.ca: **October 3, 2005**

Medical records turn up on real estate flyers



- Toronto — An investigation is underway after medical test results from Ottawa ended up on the back of real estate flyers delivered to Toronto homes this week.

One flyer showed pictures of houses for sale on one side, and the results of a mammogram done at the Ottawa Hospital on the other.

- **www.cbc.ca - February 20, 2003**



Confidence in a connected world.

Legislative Directions

Legislation: Privacy and the Canadian Public Sector



- Governments have been subject to privacy longer than the private sector:
 - Federal Government: Privacy Act (1983)
 - Imposes obligations on federal government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information
 - Gives individuals the right to access and request correction of personal information about themselves held by these federal government organizations
 - Ontario: Freedom of Information and Privacy Protection Act (FIPPA)
 - Alberta: Freedom of Information and Protection of Privacy Act (FOIP)
- Privacy legislation is often being extended by policy and development guidelines:
 - Ontario:
 - Privacy Impact Assessment Guidelines
 - ESD Standards
 - Privacy Design Guidelines
 - Canada:
 - Treasury Board Secretariat's Comprehensive Assessment of Risks Related to the Patriot Act (January 24, 2005)

- Alberta and British Columbia passed their own privacy legislation in 2004, which has been recognized as providing ‘substantially similar’ protections as PIPEDA: *Personal Information Protection Act (PIPA)*
- Quebec has had its own privacy law since 1994 (also recognized as substantially similar)
- Ontario passed the *Personal Health Information Protection Act (PHIPA)* which came into force on November 1, 2004; Saskatchewan and Manitoba also have their own health privacy legislation

Legislation: Common Themes



- Most Canadian legislation requires that individuals' consent to a organization holding personal information for a specific use
- Lack of consent means that the organization must obtain consent or delete personal information unless otherwise obligated to retain it
- All private information must be protected from unauthorized access
- Organizations must have an active privacy policy, processes, staff awareness, compliance and training programs to enforce a comprehensive privacy program
- Organizations must also have a means of removing any private information which an individual no longer wishes the organization to have access to, or for which there is no longer a valid reason to retain, except where otherwise required by law to retain it
- Businesses can face fines, audits, and more seriously, possible deletion of databases or other data stores
- More seriously: non-compliance with relevant privacy legislation can seriously affect the public confidence and the organization's reputation

Retention of Documents



- Canadian organizations, both public and private sector, are under a number of differing laws relating to the retention of patient and business records
- Limitation periods for legal actions provide the underlying requirement to keep documents for the period of time needed to defend such actions
- Organizations which operate across multiple jurisdictions may face differing requirements for retaining records
- Federal and provincial laws often differ
- Privacy legislation creates two conflicting pressures:
 - Positive obligation to retain records to be able to honour the deal made with the individual
 - Also, to get rid of the personal information when it's no longer needed for the original purpose for which it was gathered, or not otherwise required to be retained by law



Confidence in a connected world.

IT & Personal Information in Health Care

- Patient systems contains information about the entire history of dealings with a patient, in addition to possibly others (family members, physicians)
- While security/access is based on role, in general within individual systems there is no roles-based access that limits what can be seen or accessed
 - In health care, need to access information for patient care can outweigh the value of password protecting systems
- Information is mobile:
 - In Canadian subsidiaries of US corporations, important systems information are often in the US, while the balance can be accessed from the US or are backed-up in the US
 - A lot of information is 'portable' – contained on laptops, USB devices or PDA's used by physicians, staff and IT professionals and move around the country and across the border every day

- Unstructured information (Word documents, e-mails) on mail and file servers on local office LANs as well as WANs
- Web, e-commerce systems collect personal information and preferences, and utilize technologies such as tracking cookies, and are often centralized
- Backup systems and disaster recovery systems are 'snapshots' of the whole network, maintained for years – sometimes in another jurisdiction

Outsourcing and Sub-contracting



- There is the illusion that one can shift the burden of responsibility concerning privacy:
 - Requests are arising to confirm compliance with applicable privacy legislation and with privacy policies presented by the business partner/outsourcer
 - These issues create potential conflicts with suppliers, business partners, and outsourcing companies unless responsibilities are clearly defined
- BUT responsibility for privacy cannot be outsourced:
 - If you permit the collection of information about individuals under your organization's name or authority, you cannot blame sub-contractors for their failure to adequately protect the privacy of individuals
 - Public and private sector organizations remain responsible for the information processed by third parties on their behalf

- Personal Information of Canadians (customer and HR), held in the USA or accessible from the USA, exposes Canadian organizations to liability and adverse publicity under Canadian privacy legislation if disclosed pursuant to the Patriot Act
 - Report of the Information and Privacy Commissioner of British Columbia, David Loukidelis (October 2004)

- British Columbia Supreme Court decision found that outsourcing was not in violation of BC privacy legislation, because of restrictions on location of data, management structures (governance), and provisions relating to safeguarding of data, employee training, fines, and other *contractual* provisions
 - BC Govt Serv. Empl. Union v. British Columbia (Minister of Health Services)

- Conflict of values, approaches, public perception issues put Canadian and US companies in a potential 'no-man's land'



Confidence in a connected world.

Strategic Approaches to Privacy

- Corporate governance and the operationalization of security and privacy:
 - Define and appoint someone to a security/privacy officer role, with real ability to affect organizational policy
 - Establish policies and a regular review
 - Develop an internal capacity to address maintenance of policies, respond to access and removal requests, handle breaches, interface with regulators
- Separation of duties:
 - For instance: DBA's should not be able to alter logging of accesses, and those in charge of monitoring should be unable to control databases themselves
- Addressing 'human factor' in risks to protection for an organization:
 - Background checks for staff, especially those in position to access and alter personal information
 - Privacy and security training for new hires and on a regular basis, including recording the fact of such training
 - Make security and privacy protection part of job descriptions, and part of performance objectives
- Documenting security and privacy efforts
 - Allows regulators to assess compliance activities, recognize failures as human error rather than systemic problems
 - Allows organization defence to possible claims

Best practices: Contract



- Internal agreements:
 - Agreements between related organizations to enforce privacy requirements of jurisdictions where information is being processed centrally
- Third party issues: outsourcing does not alter privacy responsibilities:
 - Technology requirements (such as encryption, firewalls, access restrictions) can be required of partners to ensure adequate safeguarding of personal information
 - Audit and review provisions to assess compliance with privacy-related contract provisions
 - Audits must actually be conducted
- Jurisdictional issues:
 - Be aware of jurisdictional requirements and how different laws may be engaged
 - Management of multiple jurisdictions' privacy requirements by adherence to the highest standard
- Staff and contractors:
 - Ensure staff have privacy and confidentiality as requirements of employment
 - Similarly, provide by contract that contractors adhere to corporate standards

Best practices: Consent and Notice



- Informed consent is key to obtaining and using personal information:
 - Informing individuals as to the intended use of their personal information
 - Obtain their consent to use it
- BUT:
 - Organizations cannot unilaterally alter privacy agreements
 - Must be careful to anticipate business uses because secondary uses not reasonably contemplated at time of consent will not be covered by notice
 - Consent cannot be overbroad: “We can do anything we like with it” – and consent must be specific for it to be meaningful
- Privacy statements are ‘contracts with the world’
 - Important to manage and understand how they constrain secondary uses
 - Privacy statements are a very public thing, and law/regulation is not the operative consideration
 - Must be reasonable in light of intended use, and the nature of the service being provided

- Technology strategies can require a variety of investment ranges:
 - Audit/logging requirements which would permit client to know if PI were accessed but still allow unfettered access to care providers
 - Requirements to keep personal information linked ‘pseudonymously’ to non-identifiable information
 - Encryption of personal identifiers or sensitive information, with keys retained in Canada
 - Access controls to limit access over networks, knowledge-sharing systems to ‘need-to-know’ – including limits by geography (features of document management systems)
 - Firewalls prohibiting access internally to US parent or related companies to data on Canadian LANs
 - Utilization of technologies to support secure access to information remotely, while not allowing the information to become mobile

Best Practices: Records Management



- Records management and media management is critical to ensure the availability of documents required to evidence what health care decisions were made, and the basis on which they were made, as well as ensure that records are maintained for appropriate retention periods
- Message management allows a record of communications affecting material decisions to be maintained and searchable, as well as ensure that communications are managed, monitored and controlled
- Records and message management are critical to honouring the obligation to act on the personal information received, to retain it for the purpose for which it was intended, and to be able to systematically and effectively destroy it when it is no longer required
- Involvement of legal counsel is critical, especially since many corporations operate in specialized regulatory environments such as the health sector have their own rules about document retention, as well as operating across different jurisdictions that also have different limitation periods.



Confidence in a connected world.

Conclusion

Privacy requires Strategy



- Understand jurisdictional issues
 - Privacy obligations arise under not only public sector laws but private sector
 - It is possible for private sector partners to have multiple laws which apply to them
- Patriot Act and other jurisdictional concerns must be addressed by reducing the *ability* of outsourcers/subcontractors to comply with disclosure demands
- Privacy risks are about risk management:
 - *There is never a perfect solution, only a reasonable one*
 - *There is not one solution, only a set of tools that must be applied in different ways in different circumstances*



Confidence in a connected world.

Thank You!

Constantine Karbaliotis

constantine_karbaliotis@symantec.com

416.774.0124

© 2006 Symantec Corporation. All rights reserved.

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED AS ADVERTISING. ALL WARRANTIES RELATING TO THE INFORMATION IN THIS DOCUMENT, EITHER EXPRESS OR IMPLIED, ARE DISCLAIMED TO THE MAXIMUM EXTENT ALLOWED BY LAW. THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.

- Canadian Senior Compliance Business Specialist
 - called the Bar of the Province of Ontario in 1986
 - practiced law in the areas of litigation, intellectual property for ten years

- Ten years consulting experience with small to large law firms, public legal sector, as well as other public sector and private sector organizations

- Certified Information Privacy Professional (2004), Certified Information Privacy Professional/Canada (2006)