



Information Just Keeps Going, and Going and ...

Dr. Ann Cavoukian

**Information and Privacy Commissioner
Ontario**

Ken Anderson

Assistant Commissioner (Privacy)

**National Association for Information Destruction – Canada
Conference**

February 1, 2007



Presentation Outline

- ▶ *Culture of Privacy... yes really!*
- ▶ *Hello... you've got what?*
- ▶ *Do I have to?*
- ▶ *Where will it go?*
- ▶ *Your Turn!*



1

Culture of Privacy... Not!

***IPC Health Order #2
(H0-002)***



The Incident

- When the patient entered the hospital, she informed the staff that she did not wish her estranged husband, an employee of the hospital, or his girlfriend, a nurse at the hospital, to be aware of her admittance or to access her PHI;
- Hospital treated the warning from the patient as a security matter – the Privacy Office was not notified;
- Following discharge, a conversation the patient had with her estranged husband indicated that he was aware of her admittance and details of her treatment;
- The patient then filed a complaint with the hospital.



Hospital's Response

- Upon receiving the complaint, the CPO put a “privacy flag” on the patient’s EHR, which would automatically send an audit report to the Privacy Office every time the patient’s EHR was accessed;
- CPO conducted an audit of all access to patient’s EHR – confirmed that the estranged husband’s girlfriend (the nurse) had inappropriately accessed the patient’s EHR;
- Hospital did not, however, take immediate steps to prevent the nurse from gaining any further access to the patient’s EHR;
- The EHR was again accessed inappropriately by the nurse on three separate occasions **after** the complaint had been filed and **after** the privacy flag had been placed on the EHR.



Hospital's Internal Investigation

- Hospital conducted an internal investigation and determined there had been a breach of *PHIPA*;
- Nurse was suspended without pay for four weeks (24-year previously unblemished record);
- Estranged husband was suspended without pay for 10 days (21-year previously clean record);
- Upon reading the hospital's report, the patient filed a complaint with the IPC.



Commissioner's Investigation

- Commissioner found that HR protocol trumped privacy – which was totally unacceptable;
- Privacy policies were not embedded into the day-to-day operational policies of the hospital;
- EHR alert system for unauthorized uses was considered weak – needed to be strengthened.



Commissioner's Order

- Hospital was ordered to review its practices and procedures relating to privacy and human resources to ensure compliance with *PHIPA*;
- Hospital was ordered to implement a protocol to ensure that reasonable and immediate steps are taken, upon being notified of an actual or potential privacy breach, to ensure that no further breaches are permitted; and
- Hospital was ordered to ensure that all agents are appropriately informed of their duties and obligations under *PHIPA*.



Quote from the Order

“I am taking this opportunity to remind all custodians of the importance of ensuring that their employees and agents are made fully aware and properly trained with respect to their obligations under the Act, as well as the need to create environments in which privacy issues are not only understood, but form an integral part of the culture of their institution. Despite the stellar efforts of this hospital’s Chief Privacy Officer, the hospital’s failure to follow through on its privacy policies at the time of the complainant’s admission, followed by priority being given to a Human Resources Protocol over preventing further instances of unauthorized access to the patient’s records, contributed in large part to the breaches reported.”



A More Appropriate Response to A Breach

- IPC investigated another case in which a hospital reported that an employee had inappropriately accessed a patient's chart (Report HI-050013);
- Hospital **immediately** removed employee's access rights pending an investigation;
- Employee was **immediately** suspended with pay;
- Following the internal investigation, the employee was dismissed due to serious confidentiality breaches; and
- IPC did not have to issue an order in this case as the hospital had already taken all reasonable steps to address the breach.



Culture of Privacy



Culture of Privacy

Lessons from Health Order 2

- Even the most rigorous privacy policies will be ineffective if they do not become an accepted part of an organization's institutional culture and its day-to-day operations;
- Organizations must ensure that they not only educate their staff about privacy practices as required by law, they must also ensure that privacy becomes embedded into their institutional culture;
- All organizations should feel obligated with the need to create environments in which privacy issues are not only understood, but form an integral part of the culture of their institution.



Redirecting Institutional Culture

What is apparent from the IPC investigation and the resulting Order HO-002 is that the organizational culture is difficult to re-direct.

The literature of business administration suggests that "change management" is very challenging and requires both a well-informed strategy as well as demonstrated commitment from the most senior levels of the organization.



Redirecting Institutional Culture (Cont'd)

Changing corporate culture requires an entire change in mindset and it isn't without risk;

“A company must challenge all its assumptions about how each task is handled. It must not be afraid to peel back the layers and examine itself in a way it has never had to be in the past ... It requires that some of the best and brightest people in the company devote a tremendous amount of time and energy to the task.”

— William A. Wheeler, *Business Process Engineering: Breakpoint Strategies for Market Dominance*, 1993.

“Organizational learning theorists propose that it is not enough for leaders to design appropriate organization structures and continue to make well-reasoned decisions; instead, organizations must be characterized at all levels by attentiveness to changing conditions”.

— Amy C. Edmondson, Professor of Leadership and Management and Chair of the Doctoral Programs, Harvard Business School.



2

*What Were They
Thinking?*

*IPC Health Order #3
(H0-003)*



The Incident

- College of Physicians and Surgeons of Ontario notifies the IPC that medical and rehabilitation clinic (Clinic) ceased operations and abandoned records with personal health information (PHI);
- IPC's Registrar immediately contacts landlord and personally retrieves the records pursuant to 60(13) of *PHIPA*.



The Records

- The majority of records retrieved from the Clinic consisted of invoices; notes on patients; financial records relating to patient services; sign-in sheets and appointment books; and insurance carrier and benefits information.



Commissioner's Investigation

- Corporate search reveals Clinic owned and operated by numbered company solely directed by licensed doctor;
- Determined that landlord wrote to Clinic three times regarding abandonment and requested that the Clinic notify him if it wished to claim any property on the premises;
- No provision in the lease for storage and/or retention of records of PHI.



Commissioner's Review

- Owner's brother advised he arranged for transfer of 6000 to 7000 "medical" files to a professional storage company;
- He alleged that he contacted the College of Physiotherapists of Ontario (CPO) for advice respecting "non-active physio files", which CPO denies; he was not sure what to do with the files.



Commissioner's Review (Cont'd)

- The owner's brother had no knowledge of *PHIPA*, was unaware of the Clinic's obligations and what constituted records of PHI;
- As a result, records containing PHI were left behind, and their whereabouts were unknown to the Clinic until they were contacted by the IPC.



Commissioner's Order

- Enter into a written agreement with any record storage company used to retain records stipulating that PHI must be treated according to all aspects of *PHIPA*;
- Put in place practices and procedures to ensure that records of PHI are safeguarded at all times;
- Appoint a staff member to facilitate compliance with *PHIPA*.



Commissioner's Order (Cont'd)

- Enter into written contracts with health care practitioners acting as independent contractors outlining *PHIPA* obligations of both parties regarding records of PHI;
- If impending closure of the group practice of HICs, make available to patients a written statement that describes how their records will be retained or disposed of and how they may obtain access to or transfer of their records.



HO-003 Postscript Observations

- This case was truly regrettable and easily avoidable;
- The Custodian demonstrated a flagrant disregard for the privacy rights of his patients and clients.



*Out of Sight, Out of
Mind?*

*What To Do About
Abandoned Records*



Abandoned Records

- Records containing “personal health information” which apparently leaves the custody or control (but not responsibility) of a health information custodian (HIC);
- Expected treatment of these records upon a HIC’s:
 - Cessation of practice (retirement, revocation or suspension of licence, abandonment of practice, leaving the province, or eviction):
 - Bankruptcy;
 - Death.



Why are Abandoned Records an Issue?

- Problem not addressed fully in legislation, regulation, or by professional bodies;
- May lead to inappropriate, unfortunate outcomes for individuals:
 - Inability to access their records of personal health information;
 - Unauthorized uses and disclosures;
 - Inappropriate destruction.



Current Abandoned Records Scenarios

- Transfer of records to authorized or unauthorized third parties;
- Storage of records of personal health information in secure/insecure locations;
- Destruction/desertion of records of PHI;
- Unauthorized uses and disclosures of records of personal health information.



IPC Work with respect to Abandoned Records

- Consulting with stakeholders regarding policies and practices to address a HIC's cessation of practice, bankruptcy, death;
- Developing appropriate responses and products with respect to issues.



Finding Directions for Abandoned Records

- Work with regulatory colleges and professional associations to augment best practices and standards of practice;
- Provide clear guidelines for health information custodians and their agents;
- Change in legislation or regulations.



3

I Was Looking For That!

How To Avoid Records Ruin



Prevention, Detection, Treatment and Remedies of “Record Ruin”

- **Consider life cycle of personal health information or personal information:**
 - What happens to personal information from when it enters the system or institution to when it ultimately leaves;
 - What happens to personal health information upon changes in the practice;
 - Consider Privacy Impact Assessments and Threat and Risk Assessments for new technologies and information management systems;
 - Perform regular “audits” of privacy policies and procedures and security measures.



Setting The Record Straight

- Prepare policies and procedures that protect PI or PHI in advance of transferring or sharing;
- Apply privacy best practices - consider the fallibility of people and technologies;
- Incorporate privacy practices in advance of outcomes – don't wait for a crisis, avert it;
- Integrate privacy policies and procedures into the culture/behaviour of an organization.



IPC Fact Sheets

- *Safeguarding Personal Health Information*
www.ipc.on.ca/images/Resources/up-1fact_01_e.pdf
- *Privacy and Confidentiality When Working Outside the Office*
www.ipc.on.ca/images/Resources/up-num_20.pdf
- *Reducing Your Roaming Risks – A Portable Privacy Primer*
www.ipc.on.ca/images/Resources/up-bmo_ipc_priv.pdf



4

Disposing of Electronic Media



Confidential Child Data Found in Nigeria

Toxic Trade News, *Confidential Wisconsin child data found on Nigerian hard drive, October 27, 2005.*

- Members of an environmental group who purchased computer hardware at a Nigerian marketplace found confidential data from Wisconsin's child protective services agency still saved on the hard drive;
- Basel Action Network purchased the hard drive for about \$20 from a marketplace in Lagos, Nigeria, as part of an effort to track the hazardous disposal of computer and electronic refuse overseas;
- The Wisconsin Department of Health and Family Services could not confirm or deny it was their hard drive because the type of data found is also used by other state agencies.

— www.ban.org/ban_news/2005/051027_data_found.html



Health Records Sold at B.C. Public Auction

March 4, 2006: *“Thousands of B.C. private health records sold at public auction: Government tapes contain information on conditions such as HIV status, mental illness.”*

— Vancouver Sun

Personal Information among the files included:

- Records showing medical status of individuals such as mental illness, HIV or substance-abuse problems;
- Details of applications for social assistance, and whether or not people are fit to work;
- Social insurance numbers and medical conditions;
- Hundreds of caseworker entries divulging extremely intimate details of people's lives;
- A document containing more than 65,000 names along with social insurance numbers, birthdays and amounts paid to each person for social support and shelter.



Match the Destruction Method to the Media

- **Paper:** cross-cut shredding is recommended, not simply continuous (single strip) shredding, which can be reconstructed. Consider going further for highly sensitive records and ensuring that pulverization or incineration of the records takes place;
- **Electronic and Wireless:** destruction means either physically damaging the item and discarding it. If re-use of electronic media within the organization is preferred, employ wiping utilities provided by various software companies. *However*, wiping may not irreversibly erase every bit of data on a drive;
- **Remember:** Consider not only the “official” files but any duplicate copies of documents made for in-office use (documents should carry “shred after” dates or “do not copy” warnings).

IPC Publication – *Secure Destruction of Personal Information* Fact Sheet

http://www.ipc.on.ca/images/Resources/up-fact_10_e.pdf



GigaByter/MaSeR

- April 2005, staff from the IPC visited GigaByter/MaSeR at their plant in Barrie, Ontario, to view a new system called “**The Fractionater**” which ensures absolute secure data destruction;
- The process is called **delamination** – separating the data-bearing material from the disc;
- Further, all other materials in computers, peripherals, circuit boards, power cords and other electronic scrap can be processed together by crushing to yield recyclable steel, aluminum, copper, precious metals and mixed plastic scrap;
- The Barrie plant consists of two production lines designed to process up to **40 million pounds** of electronic scrap annually;
- MaSer and Gigabyter are the same company. MaSer is responsible for the recovery and recycling technology while GigaByter is responsible for the commercial dealings.



Shredding is the First Option

- Drives are destroyed as functioning units;
- Drives can be shredded to small particle sizes;
- Shredding is cheaper and faster than overwriting or degaussing;
- **But Shredding Alone Does Not Completely Destroy Data:**
 - Shredding simply makes large particles smaller, and substantial data can reside on small particles;
 - Because shredding does not absolutely destroy the magnetic medium on the drive platter, a forensic tool (magnetic force microscope) can see and recover data from platter particles.

— 2005 IAATAM Annual Conference



What is Delamination?

- A process whereby materials bonded during manufacturing by lamination or with fasteners are physically liberated for higher value recycling;
- The bonded materials are called “composites” and the recovered materials “fractions”;
- The cobalt chromium layer where information resides is separated from the aluminum platter that carries it;
- The magnetic field is destroyed;
- *All information is destroyed.*

— 2005 IAATAM Annual Conference



The Case for Delamination

- Exceeds the capabilities of drive overwriting, degaussing, and shredding;
- Can eliminate the need for overwriting and degaussing;
- Generates valuable commodities;
- Most cost effective data destruction methodology;
- Does not require burning, exporting, or land filling and is therefore a sustainable solution.



Provincial Policies and Procedures

British Columbia:

- *Core Policy and Procedures Manual*, Office of the Comptroller General – www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm

Alberta:

- *Security Policy for Disk Wiping Surplus Computers*, Office of the Corporate Chief Information Office – www.im.gov.ab.ca/index.cfm?page=policies/index.html
- *Policy for Maintaining Security of Government Data Stored on Electronic Data Storage Devices*, Office of the Corporate Chief Information Officer – www.im.gov.ab.ca/index.cfm?page=policies/index.html

Ontario:

- *Operating Procedures for Disposal, Loss and Incident Reporting of Computerized Devices*, Ministry of Government Services – <http://intra.ops.myops.gov.on.ca>
- *Information and Information Technology Security Directive*, Ministry of Government Services – [http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/\(vwReadResourcesByRefId_Content\)/sec2006.07.18.10.01.27.JFY_res/\\$File/I&IT_Security-Dir.pdf](http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/sec2006.07.18.10.01.27.JFY_res/$File/I&IT_Security-Dir.pdf)



European Union

- European Union: **DIRECTIVE 2003/98/EC** on The Re-Use Of Public Sector Information;
- Requires manufacturers of electric and electronic equipment to help dispose of such equipment when it is used and the owners do not want it any more;
- This is intended to reduce the problem of waste, especially highly polluting waste that is common with some electronic devices.

http://europa.eu.int/information_society/policy/psi/docs/pdfs/directive/psi_directive_en.pdf



United Kingdom

January 2007, *Waste Electric and Electronic Equipment Regulations (WEEER) 2006:*

- Aims to minimize the impact of electrical and electronic goods on the environment, by increasing re-use and recycling and reducing;
- It seeks to achieve this by making producers responsible for financing the collection, treatment, and recovery of waste electrical equipment, and by obliging distributors to allow consumers to return their waste equipment free of charge.

www.dti.gov.uk/files/file35992.pdf



Should Canada Have Similar Laws?

Questions

- Should they be federal or provincial laws?
- Would there be a problem imposing such rules on foreign manufacturers?
- Would importers have to bear the burden, and is that a problem where such importers are numerous and generally unregulated?
- Should voluntary assistance be sought from manufacturers and others instead?
- Some business equipment chains now recycle printer cartridges, for example. Is it worth trying to expand such programs?



Symposium on Electronic Waste in Canada

Not all Canadian provinces have moved forward with end-of-life programs for the disposal of electronics. A symposium has been organized to discuss this issue. Details are set out below.

"The Integrated Circuit: A Symposium on Electronic Waste in Canada"

March 5th 2007, Fauteux Hall at the University of Ottawa.

Jeremy Hessing-Lewis, University of Ottawa,
Information Technology Law Society

613-236-5160

jhess033@uottawa.ca



5

What Can I Do?



Privacy Breach Protocol

Alert Your Incident Response Team

- **Containment:** *Identify the scope of the potential breach and take steps to contain it;*
- **Notification:** *Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify those individuals accordingly;*
- **Investigation:** *Conduct an internal investigation into the matter, linked to the IPC's investigation and with law enforcement if so required;*
- **Remediation:** *Address the situation on a systemic basis where program or institution-wide procedures warrant review.*



Breach Notification Assessment Tool

- **Breach Notification Assessment Tool,**
 - www.ipc.on.ca/images/Resources/up-ipc_bc_breach.pdf
- Assists to make key decisions if a privacy breach occurs;
- **Must be read along with:**
 - *What to do if a privacy breach occurs: Guidelines for government organizations,*
 - www.ipc.on.ca/images/Resources/up-1prbreach.pdf
 - *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector,*
 - www.ipc.on.ca/images/Resources/up-3hprivbreach.pdf



Breach Notification

The *Breach Notification Assessment Tool* guides organizations through four decision-making steps regarding notification:

Step 1: Notifying Affected Individuals;

Step 2: When and How to Notify;

Step 3: What to Include in the Notification;

Step 4: Others to Contact.



Breach Notification Details

- Some notification automatically required, other cases based on risk;
- Notification should be as soon as possible may be direct/indirect based on criteria;
- Notice to include information to help reduce/prevent harm caused by breach;
- Contact other authorities or organizations.



Conclusion

How Can NAID Members Help?

- Expand range of services, e.g. data management, certification, transfer and storage agency, digital archiving and access controls, anonymization (and reuse/resale) of data;
- Education: spread the word on the importance of proper information management and secure data destruction which complies with existing laws and best practices;
- Develop and promote standards/best practices for information management and secure data destruction;
- As agents, assist clients with privacy breach protocols.



How to Contact Us

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca