Think Secure Records Destruction is Boring?

Think Again – Avoid Becoming the Next Hit

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Association of Records Managers and Administrators

Canadian Region Conference

May 29th, 2006

Presentation Outline

1. *The Ontario Incident*
2. *The Investigation*
3. *The Order*
4. *Five Recent Incidents*
5. *Solutions*
6. *Conclusion*

IPC

The Ontario Incident

IPC

"The Incident"
October 1, 2005

- I was contacted by a newspaper reporter from the Toronto Star who advised me that patient health records were being blown around the streets of downtown Toronto;
- The records were being used as props on the location for a film shoot about the September 11, 2001 terrorist attacks on New York's World Trade Center;
- The seriousness of such an incident, coupled with the potential devastating impact on patient privacy, prompted the need for immediate action.

IPC

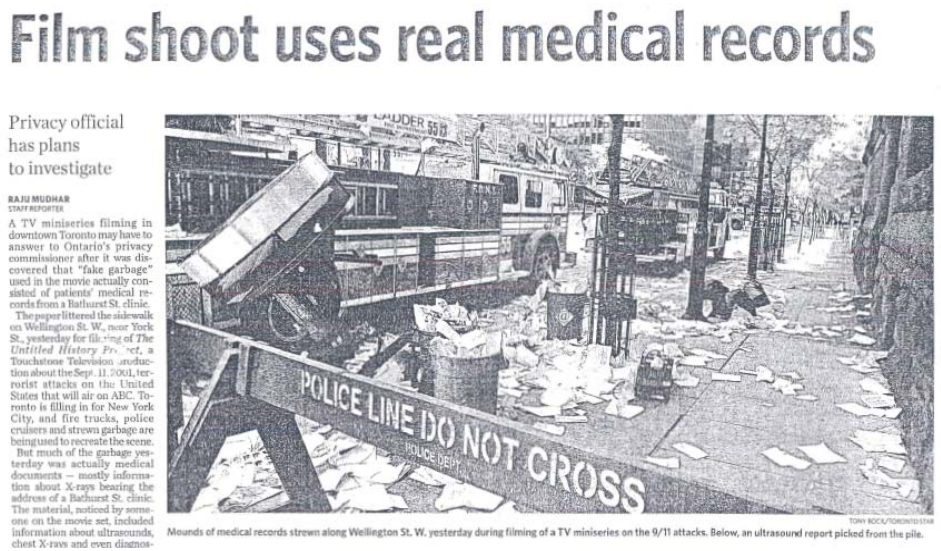
"The Incident"
October 1, 2005 (Cont'd)

- I conducted an immediate site visit and personally attended at the film location;
- When I arrived, the medical records had been retrieved, as the reporter indicated might be the case;
- While I found no evidence of patient health records on the streets, I did retrieve a one page memo that, while containing no personal health information, involved some sensitive information;
- I immediately alerted the Executive members of my office and initiated an investigation.

IPC

"The Incident"
October 2, 2005

- The Toronto Star ran a story describing the incident, along with a picture of the film set littered with what would appear to be patient records;



Film shoot uses real medical records

Privacy official has plans to investigate

RAJU MUDHAR
STAFF REPORTER

A TV miniseries filming in downtown Toronto may have to answer to Ontario's privacy commissioner after it was discovered that "fake garbage" used in the movie actually consisted of patients' medical records from a Bathurst St. clinic.

The paper littered the sidewalk on Wellington St. W., near York St., yesterday for filming of *The Untitled History Project*, a Touchstone Television production about the Sept. 11, 2001, terrorist attacks on the United States that will air on ABC. Toronto is filling in for New York City, and fire trucks, police cruisers and strewn garbage are being used to recreate the scene.

But much of the garbage yesterday was actually medical documents — mostly information about X-rays bearing the address of a Bathurst St. clinic. The material, noticed by someone on the movie set, included information about ultrasounds, chest X-rays and even diagnos-

POLICE LINE DO NOT CROSS

TONY ROCK/TORONTO STAR

Mounds of medical records strewn along Wellington St. W. yesterday during filming of a TV miniseries on the 9/11 attacks. Below, an ultrasound report picked from the pile.

- A close-up of one patient health record from an X-ray and ultrasound clinic also appeared with the story;

- The patient's name had thankfully been removed from the photograph of the actual health record.

IPC

"The Incident"
October 3, 2005

- A member of the public also called my office and indicated that he had picked up a patient's health record from the film set and wanted to alert us;
- Based on the information provided, I immediately initiated a review (investigation) pursuant to section 58(1) of the *Personal Health Information Protection Act, 2004* (the *Act*).

IPC

The Investigation

IPC

The Investigation:
First Steps

- My office's "privacy breach protocol" was immediately implemented;
- On the first day of the review, two IPC investigation teams attended the relevant sites to recover all personal health information and to start the process of determining how this incident could have occurred;
- The teams were in regular contact with my office throughout the day, and with one another, as they undertook the first step of containment and began the investigation.

IPC

Commissioner's Investigation

- The investigation determined that the health records originated with a Toronto X-ray and ultrasound clinic;
- Boxes containing the records were removed, without notice, from a locked storage area by the Toronto Clinic's landlord and placed near the building's common parking area;
- A Toronto Clinic staff member, realizing that the records were not secure, placed them in her vehicle and drove them to a Richmond Hill clinic owned by the same corporation;

IPC

Commissioner's Investigation
(Cont'd)

- From there, the boxes were picked up by the Paper Disposal Company that provided shredding services for both clinics;
- Because of a misunderstanding on the part of an employee of the Paper Disposal Company, some of the boxes were marked for recycling, not shredding;
- These boxes were passed on to a recycling company who subsequently sold the records – intact – to a film company for use on its set.

IPC

Findings of the Investigation

- The information in the records qualified as personal health information as defined in the *Act*;
- The Paper Disposal Company was an "agent" of the Toronto Clinic as defined in the *Act*;

The Toronto Clinic failed to:

- Take reasonable steps to ensure the security of the personal health information in its custody or control;
- Ensure the security of the personal health information within its custody and control;
- Comply with the requirements of section 17(1) of the *Act* which makes it responsible for ensuring the proper handling of personal health information by its agent, the Paper Disposal Company.

IPC

The Order

IPC

Commissioner's Order
The Toronto Clinic

The Toronto Clinic was ordered to:

- Review its information practices to ensure that records of personal health information in its custody or control are securely stored and protected against theft, loss and unauthorized use or disclosure;
- Put into place a written contractual agreement with any agent it retains to dispose of personal health information records. The agreement must set out the obligation for secure destruction and require the agent to provide written confirmation through an attestation once secure destruction has been conducted;
- Put into place a written contractual agreement with any health information custodian for whom it will shred personal health information that includes the obligation for it to shred securely and irreversibly and to provide an attestation of destruction.

IPC

Commissioner's Order
The Paper Disposal Company

The Paper Disposal Company was ordered to:

- Ensure that any handling of personal health information by a third party company be documented in a written contractual agreement that binds the third party to the requirements of the *Act* and its contractual agreement with the health information custodian;

- Put into place procedures that prevent paper records containing personal health information designated for shredding from being mixed together with paper that is being disposed of through the recycling process.

IPC

Impact of the Order

"This Order will establish the practice to be followed by all health information custodians and their agents in Ontario, with respect to the Commissioner's expectations for the secure disposal of health information records under Ontario's new Health Information Privacy Law."

— Order HO-001, October 2005

IPC

Five Recent Incidents

IPC

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.

IPC

Blowing in the Wind

- British Columbia's privacy commissioner is opening an investigation after scores of confidential and highly personal documents were found blowing around the streets of downtown Vancouver in April 10, 2006.
- A home video shot from an apartment balcony showed hundreds of documents blowing around a downtown Vancouver street;
- The papers were found to contain confidential information, including names, addresses, phone numbers, health care numbers and psychological assessments;
- **It is believed that the files came from a Vancouver law office that handles personal injury claims.**

IPC

Alberta: Law Firms

- **July 2005**, a privacy investigation conducted by Alberta's Privacy Commissioner, Frank Work, found that two law firms and their corporate clients breached Alberta's *Personal Information Protection Act* (PIPA) in the course of a transaction;
- At issue was the disclosure of employees' personal information – home addresses and social insurance numbers – which were posted onto the publicly accessible SEDAR website;
- Although all parties involved were found to be accountable, the Commissioner was less forgiving of the two law firms, finding that neither had exercised adequate diligence in the handling of the personal information;

Commissioner's recommendations to both law firms:

- In-house privacy training for all lawyers and staff;
- Continuing legal education in the area of privacy;
- Review of processes involving business transactions where personal information is involved;
- Appoint a privacy officer and implement a privacy policy.

IPC

Dumpster Divers

Shop violated customers' privacy: Dumped receipts end up in criminals' possession, The Edmonton Journal, April 20, 2006.

- An Edmonton beauty supply shop failed its customers by allowing personal credit and debit information to end up in criminal hands;
- In the summer of 2005, Monarch Beauty Supply threw out more than 2,600 sales receipts with customers' credit and debit card numbers into a ***dumpster***;
- The Alberta Information and Privacy Commissioner, Frank Work, has launched an investigation into Monarch's security practices after Edmonton police alerted him of a woman who complained that she discovered a $500 laptop computer purchase on her credit card bill;
- Further, a confidential informant "well-placed" within the criminal community handed the Edmonton police a bundle of Monarch receipts taken from the dumpster;

IPC

Gone With the Wind

- ***Police documents found blowing in the Winnipeg wind*, CBC News, April 27, 2006;**

- Winnipeg police are investigating how confidential documents were found blowing in the wind outside the city's main police station;

- A pedestrian found crumpled, papers, held together by a crushed paper clip, outside the Public Safety Building in downtown Winnipeg and turned them over to the CBC;

- The documents were found to contain sensitive information from the Winnipeg police crime division;

- The police acknowledged that they were unaware the documents were missing until they were contacted by the CBC;

- Irene Hamilton, Manitoba 's Ombudsman, has called for the City of Winnipeg to launch an investigation into the matter.

IPC

Solutions

IPC

Need for Industry Standards

- The facts of these cases demonstrate the critical need for the secure destruction of records containing personal information;
- Industry standards would clarify that secure destruction means permanently destroying the records by irreversible shredding or pulverizing, thus making them completely unreadable;
- ***Recycling can never be equated with secure disposal;***
- Reliance on a third party to dispose of records must include a written agreement setting out the obligation for secure destruction and requiring the third party to provide written confirmation once the destruction has occurred.

IPC

International Examples

Article 17 of the European Union's Directive on Data Protection:

- When one person or body retains another to process personal data (including the destruction of such data) on its behalf, it must choose one that provides "sufficient guarantees governing the processing to be carried out;"

- Further, such processing of personal data must be governed by "a contract or legal act" that stipulates, among other things, that the person or body processing the data shall act only on instructions from the person or body that retained it.

IPC

United States – Examples

United States Department of Health and Human Services:

- *Standards for Privacy of Individually Identifiable Health Information* "Privacy Rule": which implement the privacy requirements of the *Health Insurance Portability and Accountability Act of 1996* (HIPAA);
- The Privacy Rule establishes a set of national standards for the protection of health information, and the use and disclosure of such information by certain health-related service-providers;
- Among other things, the Privacy Rule requires a covered entity to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of health information;"
- In addition, it creates certain obligations on the part of a covered entity that retains a "business associate" (generally, a person or organization outside the covered entity's workforce that provides services involving health information for the covered entity or on its behalf).

IPC

United States – Examples
(Cont'd)

Federal Trade Commission – *"FTC Disposal Rule"*

- On June 1, 2005, new regulations came into effect stemming from the *Fair and Accurate Credit Transactions Act* and outline the duties of persons and companies when disposing of consumer credit reports and information derived from those reports;
- The regulations require "reasonable" disposal measures so that personal information is rendered permanently destroyed;
- Examples of reasonable measures given are burning, pulverizing or shredding such information, and destroying or erasing electronic media containing such information.

IPC

United States – Examples
(Cont'd)

Some states have specific requirements for the destruction of records containing personal information, including when businesses retain disposal companies to dispose of records on their behalf:

- **Georgia**: a business cannot "discard" a record containing a customer's personal information unless it first shreds the record, erases the personal information in the record or makes the personal information unreadable;
- **Texas**: when a business disposes of a record containing a customer's personally identifying information, it is required to make the information "unreadable or undecipherable;"
- **New Jersey**: businesses are required to "destroy, or arrange for the destruction of," records that contain personal information "by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or non-reconstructable."

IPC

Responsibility and Obligation

- Every organization, whether in the public or private sector, needs to follow responsible, secure procedures for the destruction of records containing personal information;
- In many cases, it's not just a matter of being responsible, protecting one's reputation, or preventing identity theft – ***it's the law;***
- All three of Ontario's privacy laws (FIPPA, MFIPPA, PHIPA) and federal legislation (PIPEDA) covering private sector organizations — require that personal information, including personal health information, be disposed of in a secure manner, whether it is in paper or electronic format.

IPC

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*
www.ipc.on.ca/userfiles/page_attachments/fact-10-e.pdf

IPC

Outsourcing Records Destruction

- If you are engaging an external business to destroy records, be selective;
- Look for a provider accredited by an industrial trade association;
- Look for a provider willing to commit to upholding its principles, including undergoing independent audits;
- Look for a provider that will provide a “certificate of destruction;”
- Check references, and insist on a ***signed contract*** detailing the terms of the relationship.

IPC

Service Provider Contract

The contract should:

- Set out the responsibility of the service provider for the secure destruction of the records involved;
- Specify how the destruction will be accomplished, under what conditions, and by whom;
- Require that a certificate of destruction be issued upon completion, including the date, time, location, and method of destruction and the signature of the operator;

IPC

Service Provider Contract (Cont'd)

- Include a provision that would allow you the option of witnessing the destruction, wherever it occurs, and to visit the service provider's facility;
- State that employees must be trained in and understand the importance of secure destruction of personal information;
- Require that if any of the work is subcontracted to a third party, the service provider must notify you ahead of time, and have a written contractual agreement with the third party, consistent with the service provider's obligations to you;
- Specify a time within which records collected from you will be destroyed, and require secure storage pending such destruction.

IPC

NAID Certification

- National Association for Information Destruction offers a voluntary annual operations certification program to its member companies — only security professionals with the Certified Protection Professional (CPP) accreditation conduct the audits;
- The CPP accreditation is issued by the American Society for Industrial Security;
- The NAID Certification Program establishes minimum standards for employee hiring and screening, operations, the destruction process, and insurance as well as other security factors;
- When a NAID Member passes the audit, they are issued a certificate, showing the company name, NAID Certification level, and the specific location of the NAID Certified operation.

IPC

Fair Information Practices

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

IPC

The “Forgotten” Principles

- **Limiting Collection**:
  The collection of personal information shall be limited to that which is necessary for the identified purposes;

- **Limiting Use, Disclosure, and Retention**:
  Personal information shall be retained only as long as necessary for fulfillment of those purposes.

IPC

Costs of A Privacy Breach

- Loss of client confidence and trust;
- Diminution of brand and reputation;
- Loss of customers, competitive edge;
- Penalties and fines levied;
- Legal liabilities, class action suit;
- Costs of crisis management, damage control, review and retrofit of information systems, policies and procedures.

IPC

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.*

IPC

Conclusion

- Build “end-to-end” information management practices – from collection to secure destruction: Privacy and security are both essential;
- Secure destruction means permanently destroying all paper records by irreversible shredding or pulverizing, thus making them completely unreadable;
- ***Recycling can never be equated with secure disposal;***
- Match the destruction method to the media;
- If you are engaging an external business to destroy records, be selective and insist on a signed contract, detailing the terms of the relationship;
- When faced with a breach, lead with openness and transparency: Contain the damage first, then notify affected parties;
- Think strategically about secure destruction: it makes good sense – ***good business sense.***

IPC

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

IPC