PHIPA:

Update from the Commissioner's Office

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

College of Dental Technologists of Ontario

Toronto, Ontario

October 25, 2006

IPC

Presentation Outline

1. *Brief PHIPA Refresher*
2. *What The IPC Has Done*
3. *Order #1*
4. *Order #2*
5. *Conclusion*

IPC

Personal Health Information Protection Act (PHIPA)

- Applies to organizations and individuals involved in the delivery of health care services (including the Ministry of Health and Long-Term Care);
- The only health sector privacy legislation in Canada based on consent: implied consent within the "circle of care," otherwise, express consent;
- The only health sector privacy legislation that was declared to be substantially similar to the federal *PIPEDA* legislation, in 2005.

IPC

Ontario's *Personal Health Information Protection Act* (PHIPA)

- Came into effect November 1, 2004
- Based on Canada's Fair Information Practices*:

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

*CSA Standard CAN/CSA-Q830, *Model Code for the Protection of Personal Information*; *PHIPA* has been deemed to be substantially similar to *PIPEDA*.

IPC

Requirements of PHIPA

- Requires consent for the collection, use and disclosure of PHI, with necessary but limited exceptions;
- Requires that PHI be kept confidential and secure
- Requires a statement of information practices be made available to the public;
- Codifies individuals' right to access and request correction of their own PHI;
- Gives patients the right to instruct health information custodians not to share any part of their PHI with other health care providers;
- Establishes clear rules for the use and disclosure of PHI for secondary purposes including fundraising, marketing and research;
- Ensures accountability by granting an individual the right to complain to the IPC about the practices of a health information custodian; and
- Establishes remedies for breaches of the legislation.

IPC

Dental Technologists Under *PHIPA*

- Considered to be health information custodians under *PHIPA*;
- Required to follow all of the general rules that apply to health information custodians, even if they may not have direct contact with patients;
- Personal health information may be received from other health information custodians such as dentists for the purpose of providing health care;
- Can rely on implied consent for the collection, use and disclosure of personal health information for the purpose of providing health care.

IPC

What the IPC Has Done

IPC

IPC Philosophy
Encapsulated in the 3C's:

Consultation

- Opening the lines of communication;

Collaboration

- Working together to find solutions;

Co-operation

- No confrontation in resolving privacy issues.

IPC

PHIPA Implementation

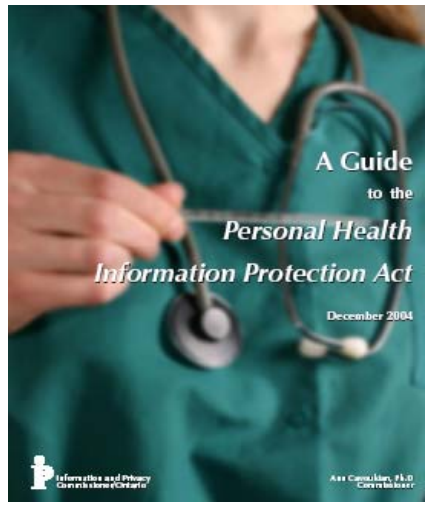
- The implementation has been a surprisingly smooth process;
- Custodians have done an excellent job, with a high level of cooperation with IPC in resolving issues;
- Relatively few complaints to the IPC – most complaints are being handled effectively by the custodians themselves.

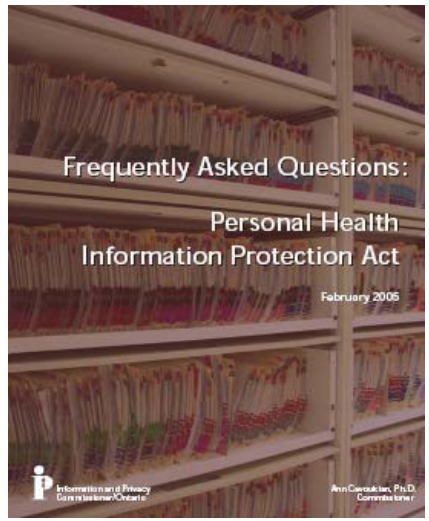
IPC

IPC Publications

Public Education Program

- Frequently Asked Questions and Answers available on IPC website (including hard copies);
- User Guide for Health Information Custodians available on IPC website (including hard copies);
- IPC PHIPA publications distributed to Colleges and Associations of the Regulated Health Professions;
- IPC/MOH brochure for the general public:
  - may be placed in reception areas;
  - to be distributed to patients.





IPC Publications

Public Education Program (Cont'd)

- OHA Toolkit – IPC participated in its development;
- IPC/OBA "short notices" working group:
  - Developing concise, user-friendly notices and consent forms to serve as effective communication tools;
- On-going meetings with Regulated Health Professions, the Federation of Health Regulatory Colleges and Associations;
- IPC PHIPA awareness article distributed to Colleges and Associations for inclusion in their members' Magazines and Newsletters;
- IPC Training Video;
- IPC Privacy Impact Assessment Tool;
- *PHIPA* Conference hosted by the IPC to celebrate the 1st anniversary of the *Act*;
- Meeting with Dr. Mark Vale – Chief Information and Privacy Officer.

IPC

IPC *PHIPA* Fact Sheets

- Health Information Custodians Working for Non-Health Information Custodians;
- Secure Destruction of Personal Information;
- Long-term Care Homes: Consent and Access under the Personal Health Information Protection Act, 2004;
- Lockbox;
- Disclosure of Information Permitted in Emergency or other Urgent Circumstances;
- Reporting Requests under *PHIPA;*
- Consent and Form 14;
- Fundraising under *PHIPA;*
- Ontario Regional Poison Information Centres and the Circle of Care;
- Your Health Information: Your Access and Correction Rights;
- Safeguarding Personal Health Information.

Health Information Short Notices

- The goal is to develop easy to read items containing the necessary elements regarding the collection, use and disclosure of personal health information, but not to overwhelm individuals with so much information that they will **not** read them;

- The language of the notices must be accessible and easily understood — ***plain language is key.***

IPC

Health Information Short Notices Working Group

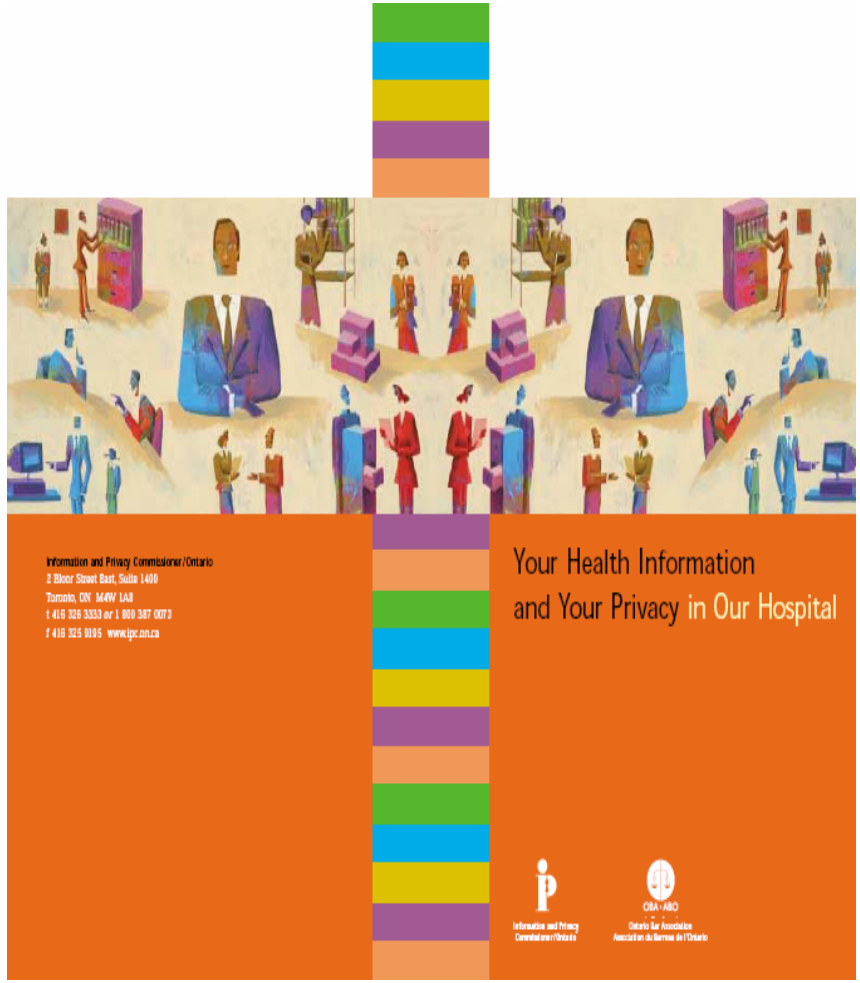
- Information and Privacy Commissioner/ Ontario;
- Ontario Bar Assoc Privacy and Health Law sections;
- Ministry of Health and Long-Term Care;
- Ontario Dental Association;

One of only several projects around the world focusing on short notices in the health sector:

- The IPC looks forward to engaging members of the health and legal profession in further improving the multi-layered approach in communicating with the public.

IPC

Short Notices Products



Complaints and Investigations

IPC

Status of *PHIPA* Complaints

As of October 25, 2006

- **Total number of *PHIPA* complaints = 417;**
- 347 are closed (83%); 70 are open (17%);

PHIPA complaints by category (open and closed):

TOTAL PHIPA COMPLAINTS (OPEN+CLOSED)	No.	%
Access/Correction	154	37%
Collection/Use/Disclosure	111	26%
HIC-Reported Breach	111	27%
IPC-Initiated Complaint	41	10%
Total Complaints	**417**	**100%**

IPC

The First 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

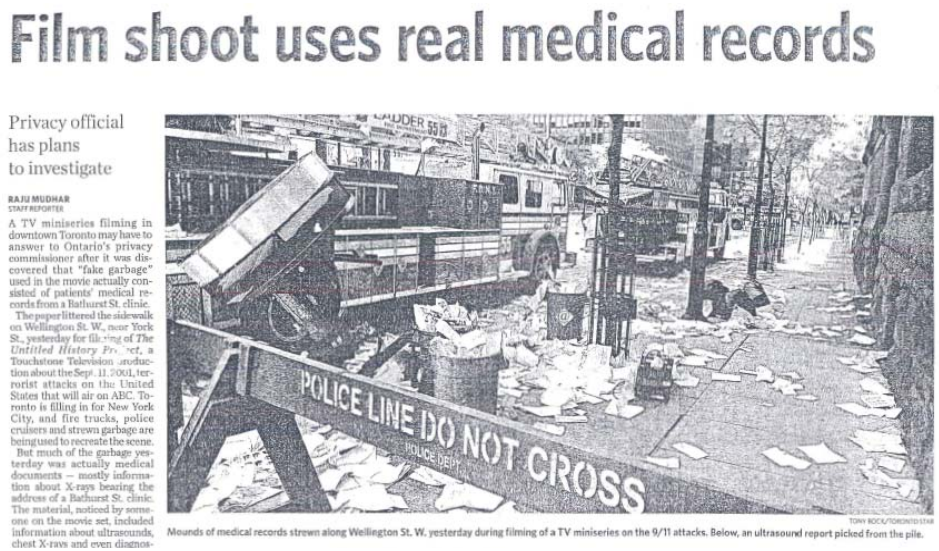
"The Incident"
October 1, 2005 (Cont'd)

- 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 pursuant to s.58(1) of the *Personal Health Information Protection Act (PHIPA)*.

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-

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.

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

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

The Order

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

The Incident Led to a Fact Sheet

The incident led to a Fact Sheet on Secure Destruction of Personal Information – principles have also been incorporated into draft regulation under *PHIPA*.

IPC

The Second Incident

IPC

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.

IPC

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.

IPC

WARNING

You are attempting to access what is considered to be a VIP patient or patient whose information has been deemed highly sensitive by the TOH Chief Privacy Officer.

Any attempt to view VIP or highly sensitive patients is closely monitored for potential violations of patient privacy.

The monitor will only be triggered if you proceed beyond this point.

Do you wish to continue?

Yes | No

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.

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.

IPC

Order #2

(HO-002)

IPC

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.

IPC

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."

IPC

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.

IPC

Keeping HICs Informed

- Summaries of all mediated cases and reports are available on our website;
- Orders are public documents and available on our Web site;
- Relevant data are regularly made available to the public and to health professionals (*number of complaints*, *examples of successful mediations*, *common issues*, *etc.*).

IPC

Conclusion

- Minimize the collection, use and disclosure of personal health information;
- Educate and train staff on privacy and security policies and procedures;
- Establish agreements with service providers;
- Embed privacy into the organizational culture;
- Develop a protocol for dealing with privacy breaches;
- Check the IPC website for more information.

IPC

How to Contact Us

Ann Cavoukian, Ph.D.

Information and 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