



Ontario

Leading the Way in Health Information Privacy

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario

“Breakfast with the Chiefs”

Toronto, Ontario

October 5, 2006



Presentation Outline

- 1. Health Privacy*
- 2. PHIPA: The First Year*
- 3. IPC Complaints and Investigations*
- 4. The First Order*
- 5. The Second Order*
- 6. “Initiate” Privacy Investigation*
- 7. Keeping HIC’s Informed*



Health Privacy is Critical

The need for privacy has never been greater:

- Extreme sensitivity of personal health information;
- Prior to Ontario's new law there was a patchwork of rules across the health sector; with some areas unregulated;
- Increasing electronic exchanges of health information;
- Multiple providers involved in health care of an individual – need to integrate services;
- Development of health information networks;
- Growing emphasis on improved use of technology, including computerized patient records.



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.



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.



Scope of *PHIPA*

Who is Covered?

- Health information custodians (HICs) that collect, use and disclose personal health information (PHI);
- Non-health information custodians that receive PHI from a HIC (use and disclosure provisions);
- “Agents” acting on behalf of health information custodians.



Mandate of the Legislation

- Requires consent for the collection, use and disclosure of PHI, with necessary but limited exceptions;
- Requires that health information custodians treat all PHI as confidential and keep it secure;
- Codifies an individual's right to access and request correction of his/her own PHI;
- Gives a patient the right to instruct health information custodians not to share any part of his/her PHI with other health care providers;
- Establishes clear rules for the use and disclosure of personal health information 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.



Health Care Defined

- Any observation, examination, assessment, care, service or procedure that is conducted for a health-related purpose and:
 - Is carried out or provided to diagnose, treat or maintain an individual's physical or mental condition;
 - Is carried out or provided to prevent disease or injury or to promote health.



Health Information Custodians

Definition includes:

- Health care practitioner;
- Hospitals and independent health facilities;
- Homes for the aged and nursing homes;
- Pharmacies;
- Laboratories;
- Home for special care;
- A centre, program or service for community health or mental health.



General Rules for Custodians

- Must take reasonable steps to ensure accuracy and security of personal health information (e.g., locked file cabinets and offices);
- Must have a contact person to ensure compliance with the legislation and to respond to access/correction requests, inquiries and complaints from public – in a small office, the nurse may perform these duties;
- Must have written information practices that comply with PHIPA and are available to the public – see IPC’s short notices products for examples;
- Must obtain consent before PHI is collected, used or disclosed, unless permitted without consent – in most cases consent can be implied;
- Must be responsible for actions of agents – to train and educate all staff on privacy and security.



PHIPA Consent

- Consent is required for the collection, use, disclosure of PHI, subject to specific exceptions;
- Consent must:
 - be a consent of the individual;
 - be knowledgeable;
 - relate to the information;
 - not be obtained through deception or coercion;
- Consent may be express or implied.



Implied Consent

- Custodians may imply consent when disclosing personal health information to other custodians for the purpose of providing health care to the individual;
- Exception – if the individual expressly withholds or withdraws consent (lock box).



Implied and Express Consent

Implied Consent:

HICs → HICs

Express Consent:

HICs → non-HICs



PHIPA:
First Year at the
Commissioner's Office



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.



PHIPA Implementation

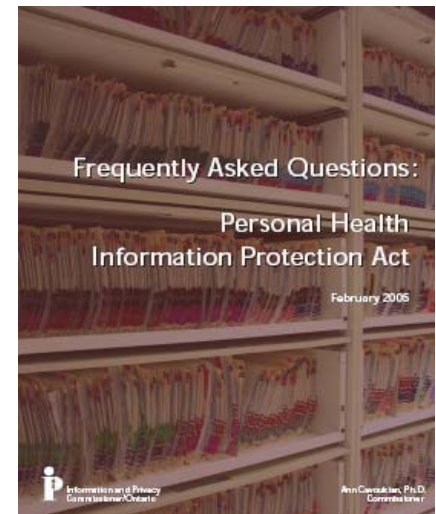
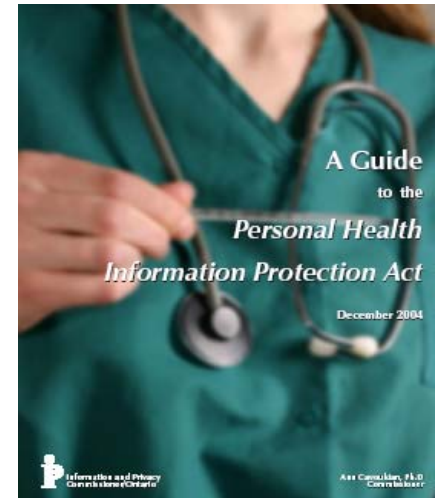
- The implementation has been a surprisingly smooth process;
- Custodians have done an excellent job, with a high level of cooperation with IPC in resolving issues;
- Relatively few complaints to the IPC – most complaints are being handled effectively by the custodians themselves.



IPC 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*.



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.



Why Short Notices are Important

Short Notices:

- Ensure that people are well informed about what an organization does with their personal information; and
- Allow people to become empowered with a choice over their personal information.



Short Notices

International Efforts

- 2003, the movement to establish a global short notice was officially recognized at the International Conference of Data Protection Commissioners in Sydney, Australia;
- 2004, in Berlin, a working group of Commissioners (including the IPC), business leaders, lawyers and privacy practitioners met and prepared a memorandum recognizing that a new architecture was needed for privacy notices;
- 2004, the EU Article 29 Working Group issued the position paper *WP100* on the use of “multi-layered notices.”



Berlin Memorandum

Effective privacy notices should be delivered within a *framework* with the following core concepts:

- **Multi-layered** – Privacy information should not be conveyed solely in a single document;
- **Comprehension and Plain Language** – All layers should use language that is easy to understand;
- **Compliance** – The total notices framework (all the layers taken together) should be compliant with relevant law;
- **Format and Consistency** – Consistent format and layout will facilitate comprehension and comparison;
- **Brevity** – The length of a privacy notice makes a difference (*maximum of seven categories*);
- **Public Sector** – These concepts have equal applicability to government collection and use of personal 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*.



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.




Short Notices Products

Health Information Privacy in our Hospital





NO CHARGE TO YOU NO COST TO YOU FOR THIS SERVICE	Description of the Information you provide to the information technology services in our hospital. The information that you provide to the information technology services in our hospital is used to provide you with the services you need. This information is used to provide you with the services you need. This information is used to provide you with the services you need.
HOW CAN YOU ACCESS YOUR INFORMATION? HOW CAN YOU ACCESS YOUR INFORMATION?	Description of the Information you provide to the information technology services in our hospital. The information that you provide to the information technology services in our hospital is used to provide you with the services you need. This information is used to provide you with the services you need. This information is used to provide you with the services you need.
WHAT ARE THE RIGHTS OF ACCESS TO YOUR INFORMATION? WHAT ARE THE RIGHTS OF ACCESS TO YOUR INFORMATION?	Description of the Information you provide to the information technology services in our hospital. The information that you provide to the information technology services in our hospital is used to provide you with the services you need. This information is used to provide you with the services you need. This information is used to provide you with the services you need.
IF YOU ARE A PATIENT OR VISITOR, HOW CAN YOU ACCESS YOUR INFORMATION? IF YOU ARE A PATIENT OR VISITOR, HOW CAN YOU ACCESS YOUR INFORMATION?	Description of the Information you provide to the information technology services in our hospital. The information that you provide to the information technology services in our hospital is used to provide you with the services you need. This information is used to provide you with the services you need. This information is used to provide you with the services you need.
HOW CAN YOU ACCESS YOUR INFORMATION? HOW CAN YOU ACCESS YOUR INFORMATION?	Description of the Information you provide to the information technology services in our hospital. The information that you provide to the information technology services in our hospital is used to provide you with the services you need. This information is used to provide you with the services you need. This information is used to provide you with the services you need.
WHAT ARE THE RIGHTS OF ACCESS TO YOUR INFORMATION? WHAT ARE THE RIGHTS OF ACCESS TO YOUR INFORMATION?	Description of the Information you provide to the information technology services in our hospital. The information that you provide to the information technology services in our hospital is used to provide you with the services you need. This information is used to provide you with the services you need. This information is used to provide you with the services you need.
HOW CAN YOU ACCESS YOUR INFORMATION? HOW CAN YOU ACCESS YOUR INFORMATION?	Description of the Information you provide to the information technology services in our hospital. The information that you provide to the information technology services in our hospital is used to provide you with the services you need. This information is used to provide you with the services you need. This information is used to provide you with the services you need.
WHAT ARE THE RIGHTS OF ACCESS TO YOUR INFORMATION? WHAT ARE THE RIGHTS OF ACCESS TO YOUR INFORMATION?	Description of the Information you provide to the information technology services in our hospital. The information that you provide to the information technology services in our hospital is used to provide you with the services you need. This information is used to provide you with the services you need. This information is used to provide you with the services you need.



Information and Privacy Commissioner/Ontario
 2 Bloor Street East, Suite 1400
 Toronto, ON M4W 1A8
 1 416 326 3333 or 1 800 387 0073
 1 416 325 9195 www.ipc.on.ca

Your Health Information and Your Privacy in Our Hospital



Complaints and Investigations



Stages of Complaints

- **Intake:**
 - Matter may be resolved by informal resolution;
- **Mediation:**
 - Matter may be resolved by a mutually agreed upon resolution between a complainant and the custodian; or
 - Matter may be resolved when IPC is satisfied with the actions taken by the custodian;
- **Adjudication:**
 - Matter is fully investigated and a formal determination is made on the issues.



Outcomes of Complaints

Intake:

- The outcome of an informal resolution is a letter to both parties confirming the resolution;

Mediation:

- When a complaint is resolved between an individual and a custodian, a letter is sent to both parties confirming the resolution;
- When the IPC is satisfied with the actions taken to resolve a HIC–reported breach, or an IPC-Initiated Complaint, a Report is issued;

Adjudication:

- The outcome at adjudication can be a Report or an Order (only two Orders issued to date).



Status of *PHIPA* Complaints

As of October 1, 2006

- Total number of *PHIPA* complaints = 405;
- 335 are closed (83%); 70 are open (17%);

PHIPA complaints by category (open and closed):

TOTAL PHIPA COMPLAINTS (OPEN+CLOSED)	No.	%
Access/Correction	149	37%
Collection/Use/Disclosure	107	26%
HIC-Reported Breach	108	27%
IPC-Initiated Complaint	41	10%
Total Complaints	405	100%



The First Incident



“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.



“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)*.



“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

STAR REPORTS

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 Barhurst St. clinic.

The paper littered the sidewalk on Wellington St. W., near York St., yesterday for filming of *The Untold 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 Barhurst St. clinic. The material, noticed by someone on the movie set, included information about ultrasounds, chest X-rays and even diagnos-



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



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.



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.



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.



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.*



Ontario's *PHIPA*: *Requirement for Breach Notification*

Section 12 (2) – Notice of Loss:

A health information custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons.

www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm



Notifying Affected Parties of A Privacy Breach

- Common issue in HIC reported breaches is how to notify individuals who may have been affected by breach;
- Custodian sometimes unsure of what happened to patients' personal health information;
- Patients to be notified may have life threatening illnesses – don't want to inflict any additional stress;
- **IPC has taken a flexible approach to notification:**
 - in some cases, far preferable for the physician to notify in person at next visit rather than immediately, in writing.



Order #1
(H0-001)



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



The Second Incident



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.



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?



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.



Order #2
(HO-002)



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

“Despite having alerted the hospital to the possibility of harm, the harm nonetheless occurred. While the hospital had policies in place to safeguard health information, they were not followed completely, nor were they sufficient to prevent a breach of this nature from occurring. In addition, the fact that the nurse chose to disregard not only the hospital’s policies but her ethical obligations as a registered nurse, and continued to surreptitiously access a patient’s electronic health record, disregarding three warnings alerting her to the seriousness of her unauthorized access, is especially troubling. Protections against such blatant disregard for a patient’s privacy by an employee of a hospital must be built into the policies and practices of a health institution.”



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.



“Initiate” Privacy Investigation



The Complaint

- IPC was alerted to an article in “Government Health IT”;
- Privacy advocates expressed concerns about IN-Q-TEL (an investment arm of the CIA) investing in Initiate Systems – the software company that provided Ontario’s Enterprise Master Person Index (EMPI);
- EMPI is a directory of identifiers assigned to an individual by multiple HICs;
- EMPI will help to ensure that PHI can be consistently linked to the correct individual; will provide the foundation for an EHR.



Commissioner's Investigation

- Obtained background information from Canada Health Infoway;
- Contacted Initiate Systems to find out about its role in the EMPI and its relationship to IN-Q-TEL;
- Contacted Cancer Care Ontario (agent for the Ministry of Health in implementing the EMPI) to learn about the confidentiality and privacy provisions included in its agreement with Initiate Systems.



Commissioner's Findings

- EMPI contains individual identifiers but no clinical information;
- Initiate Systems is only provided with access to the EMPI **on-site** and under very restricted conditions;
- No remote access to the EMPI;
- No “backdoor” or “gated” access to the EMPI;
- Initiate’s relationship to IN-Q-TEL does not allow for any access to PHI.



Commissioner's Recommendations

- Commissioner should be consulted about amendments to current agreement between CCO and Initiate Systems;
- Commissioner should be advised about any breach of the confidentiality or privacy obligations of the agreement;
- Commissioner should be advised about any changes to the source code.



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.*).



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