Privacy in Health Care:
Barrier or Enabler?

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

The Emerging Leaders Forum

June 21, 2007

IPC

Presentation Outline

1. *Personal Health Information*
2. *Privacy as an Enabler*
3. *Privacy as a Barrier?*
4. *Privacy Breaches*
5. *Technology-Related Orders*
6. *Early Orders*
7. *Culture of Privacy*
8. *How is the IPC Helping?*
9. *Conclusion*

IPC

Personal Health Information

IPC

Unique Characteristics of Personal Health Information

- Highly sensitive and personal in nature;
- Must be shared immediately and accurately among a range of health care providers for the benefit of the individual;
- Widely used and disclosed for secondary purposes that are seen to be in the public interest (e.g., research, planning, fraud investigation, quality assurance);
- Dual nature of personal health information is reflected in *PHIPA*, and all other health privacy legislation.

Privacy in the Context of Health Care

- Privacy is not a new issue in the health care context – all medical staff are well aware of the privacy issues;
- *PHIPA* was drafted in a manner such that privacy would not impede the delivery of health care services;
- Health information custodians may imply consent for the collection, use and disclosure of personal health information for the delivery of health care services;
- Express consent is required when personal health information is disclosed to a person who is not a health information custodian, or for a purpose other than the delivery of health care services.

Privacy as an Enabler

IPC

Privacy as an Enabler

- A consistent set of privacy rules ensures that personal health information will be provided the same high degree of protection across the entire health sector;
- This allows the sharing of personal health information among providers and the integration of health care services;
- Health information technology (e.g., EHRs and health information networks) can be developed and implemented based on a consistent set of privacy standards;
- If patients do not have confidence that their personal health information will be protected, they may withhold information or withdraw consent.

Privacy as a Barrier?

IPC

Privacy as a Barrier?

- Privacy requirements pose some challenges to the use of most legacy systems and, to some extent, the development and implementation of new health information technology (e.g., consent management);
- If you build privacy into the design and implementation of health information technology, it should not pose a barrier;
- IPC Orders highlight some of the privacy challenges posed by technology;
- Privacy presents a barrier to the unauthorized collection, use and disclosure of personal health information.

Privacy Breaches

IPC

Status of *PHIPA* Complaints

— As of June 21, 2007

- Total number of *PHIPA* complaints = 624;
- 536 are closed (86%); 88 are open (14%);

PHIPA complaints by category (open and closed):

TOTAL PHIPA COMPLAINTS (OPEN+CLOSED)	No.	%
Access/Correction	231	37%
Collection/Use/Disclosure	138	22%
HIC Reported Breach	197	32%
IPC Initiated Complaint	58	9%
Total Complaints	624	100%

Technology-Related Orders

IPC

Health Order No. 5

Wireless Technology Results in Order

- **Health Order No. 5** (HO-05) resulted from a methadone clinic that installed a wireless video surveillance system in its washroom to monitor patients providing urine samples;
- Video images were intercepted by a wireless rear view backup camera in a car outside of the clinic;
- Clinic immediately agreed to shut down the cameras and replaced the wireless surveillance system with a more secure wired system.

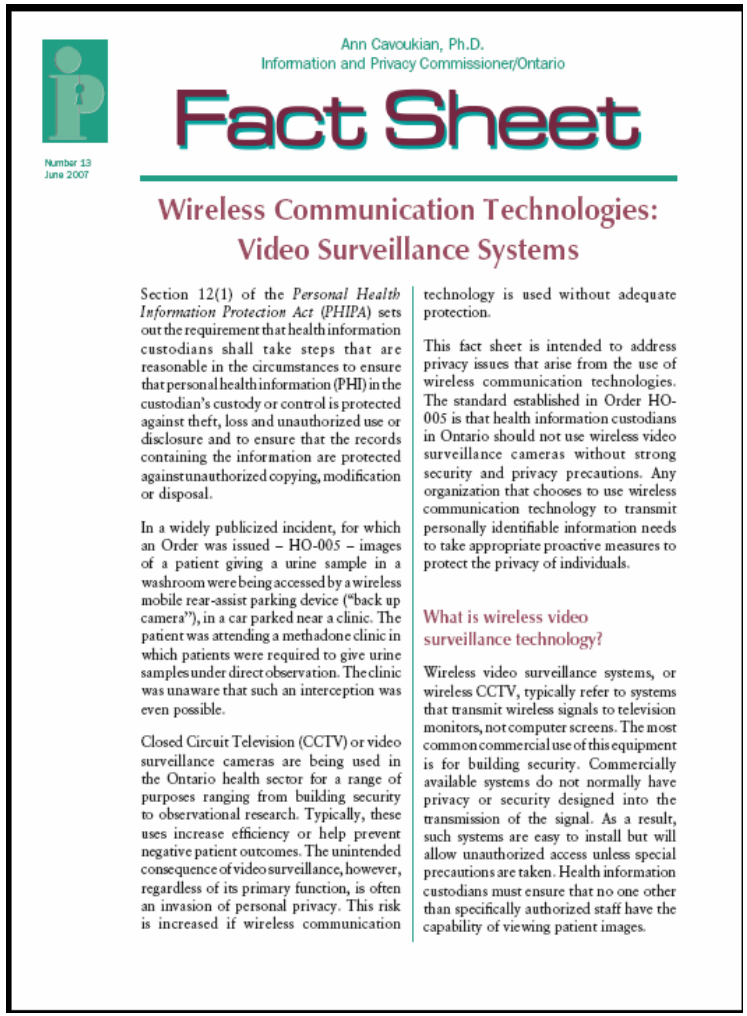
Commissioner's Message

- Although the clinic did not video tape the images captured by the surveillance system, since the system created digital data that were transmitted via air waves, the IPC determined that these digital images were, in fact, records of personal health information subject to *PHIPA*;
- Custodians should either use a wired system which inherently prevents unauthorized interception, or a wireless one with strong security measures such as encryption, to preclude unauthorized access;
- In response to this incidence, all health information custodians should assess the use of their wireless communication technology for the collection, use and/or disclosure of personal health information;
- In light of the evolving technological landscape, health information custodians should regularly and proactively review their privacy and security policies and procedures, and technologies employed;
- IPC has issued a new Fact Sheet: *Wireless Communications Technologies: Video Surveillance Systems.* A second Fact Sheet on Wireless Technology will follow.

Fact Sheet:

Wireless Communication Technologies

- Special precautions must be taken to protect the privacy of video images;
- No covert surveillance should be conducted;
- Clearly visible signs should be posted indicating the presence of cameras and the location of their use;
- Recording devices should not be used;
- Only minimum number of staff should have access to the video equipment;
- Staff should receive technical training on the privacy and security issues;
- Regular security and privacy audits should be conducted, on an annual basis.



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

Fact Sheet

Number 13
June 2007

Wireless Communication Technologies: Video Surveillance Systems

Section 12(1) of the *Personal Health Information Protection Act* (*PHIPA*) sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

In a widely publicized incident, for which an Order was issued – HO-005 – images of a patient giving a urine sample in a washroom were being accessed by a wireless mobile rear-assist parking device ("back up camera"), in a car parked near a clinic. The patient was attending a methadone clinic in which patients were required to give urine samples under direct observation. The clinic was unaware that such an interception was even possible.

Closed Circuit Television (CCTV) or video surveillance cameras are being used in the Ontario health sector for a range of purposes ranging from building security to observational research. Typically, these uses increase efficiency or help prevent negative patient outcomes. The unintended consequence of video surveillance, however, regardless of its primary function, is often an invasion of personal privacy. This risk is increased if wireless communication technology is used without adequate protection.

This fact sheet is intended to address privacy issues that arise from the use of wireless communication technologies. The standard established in Order HO-005 is that health information custodians in Ontario should not use wireless video surveillance cameras without strong security and privacy precautions. Any organization that chooses to use wireless communication technology to transmit personally identifiable information needs to take appropriate proactive measures to protect the privacy of individuals.

What is wireless video surveillance technology?

Wireless video surveillance systems, or wireless CCTV, typically refer to systems that transmit wireless signals to television monitors, not computer screens. The most common commercial use of this equipment is for building security. Commercially available systems do not normally have privacy or security designed into the transmission of the signal. As a result, such systems are easy to install but will allow unauthorized access unless special precautions are taken. Health information custodians must ensure that no one other than specifically authorized staff have the capability of viewing patient images.

www.ipc.on.ca/images/Resources/up-fact_13_e.pdf

IPC

Health Order No. 4
Stolen Laptop Results in Order

- **Health Order No. 4** (HO-04) resulted from a hospital not having adequate policies and procedures to permit compliance with *PHIPA*;
- In spite of the known high risk of loss or theft, extremely sensitive personal health information was transported on a portable device (laptop) without adequate safeguards;
- This is clearly unacceptable, more than two years after *PHIPA* came into force.

Commissioner's Findings

- The laptop contained highly sensitive information including HIV status;
- The researcher admitted that he did not need identifiable health information for the purposes of the research – it should not have been on the laptop in the first place;
- Although the hospital's research protocol required researchers to only use coded information, the hospital did not take steps to ensure that researchers followed this protocol.

Commissioner's Message

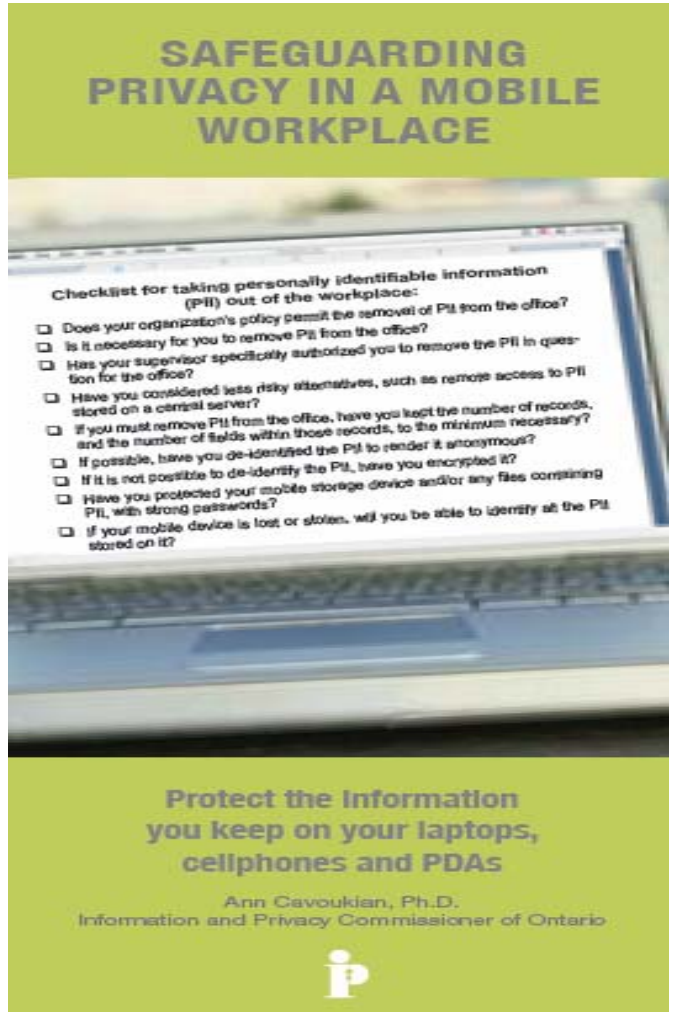
- Due to the known risk of theft, it is no longer reasonable to store personal health information on a mobile device, unless steps are taken to prevent unauthorized access in the event that the device is lost or stolen;
- A multi layered approach to security is needed;
- **Where personal health information is stored on a portable device, it must be encrypted;**
- If information is encrypted in a manner that would make the identification of individuals not reasonably possible, custodians need not notify individuals, in the event that the encrypted information is lost or stolen;
- IPC publication, *Fact Sheet: Encrypting Personal Health Information on Mobile Devices* available on our website to assist custodians.

www.ipc.on.ca/images/Resources/up-fact_12e.pdf

Brochure on Mobile Devices

Safeguarding Privacy In A Mobile Workplace

- Does your organization's policy permit the removal of PII from the office?
- Is it necessary for you to remove PII from the office?
- Has your supervisor specifically authorized you to remove the PII in question for the office?
- Have you considered less risky alternatives, such as remote access to PII stored on a central server?
- If possible, have you de-identified the PII to render it anonymous?
- If it is not possible to de-identify the PII, have you encrypted it?
- If your mobile device is lost or stolen, will you be able to identify the PII stored on it?



www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf

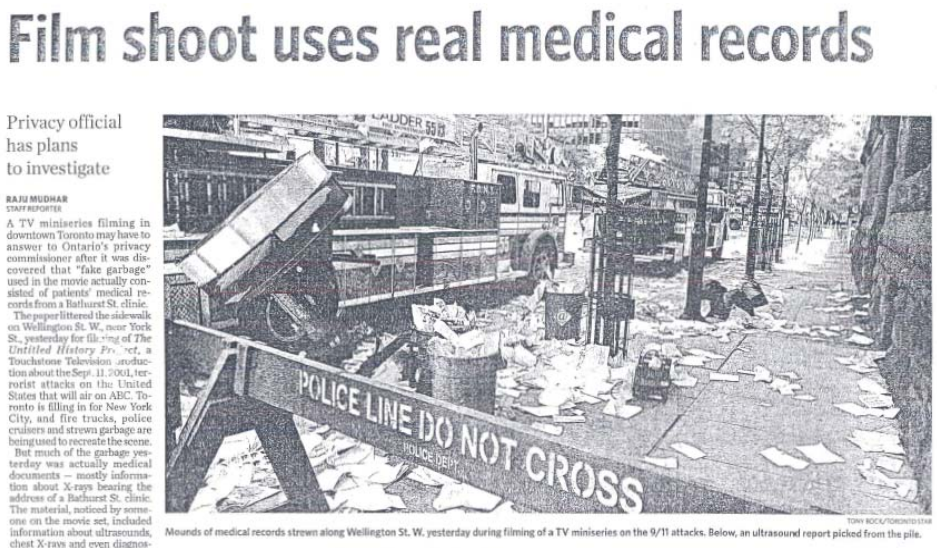
IPC

Early Orders

IPC

Health Order No. 1:
Improper Disposal Results in Order

- 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 at our request, from the photograph of the actual health record.

Commissioner's Findings

- A Toronto clinic had given the records to a Paper Disposal Company;
- The records were supposed to be shredded, but instead were sent for recycling;
- The clinic was found to have failed:
  - to take reasonable steps to ensure that personal health information was protected against theft, loss and unauthorized use or disclosure as required under section 12(1) of *PHIPA*;
  - to dispose of records in a secure manner as required by section 13(1) of *PHIPA*;
  - to comply with the requirements of section 17(1) which requires custodians to be responsible for the proper handling of personal health information by its agents
- The Paper Disposal Company was found to have failed to comply with section 17(2) which requires agents of custodians to collect, use, disclose, retain or dispose of personal health information only as permitted by the custodian

Commissioner's Message

- Custodian's responsibility for the proper of handling of personal health information by its agents requires a written contractual agreement setting out the agent's duty to securely shred the documents and requires the agent to provide an attestation confirming the fact that shredding has been completed;
- The incident led to the publication titled, *Fact Sheet on Secure Destruction of Personal Information*; — www.ipc.on.ca/images/Resources/up-fact_10_e.pdf
- Secure destruction requirements as set out in our Order have now been incorporated into the regulations under *PHIPA*.

Health Order No. 2:
Unauthorized Access Results in Order

- **Health Order No. 2** (HO-02) showed that the hospital's policies and procedures failed to prevent ongoing privacy breaches by an employee, even after the hospital became aware that such breaches had occurred repeatedly;
- Even when patient alerted the hospital to her concerns upon admission, the staff did not recognize the obvious threat to privacy posed by the estranged husband and his girlfriend;
- Staff only recognized the threat to the physical security of the patient, not the threat to her privacy;
- After learning about the breach, the hospital was more concerned about the employee's right to due process than the patient's right to privacy;
- Hospitals can have both –but HR cannot trump privacy.

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

Commissioner's Findings

- Hospital had not taken steps that were reasonable in the circumstances to ensure that the personal health information was protected against theft, loss and unauthorized use or disclosure;
- Hospital was ordered to review it practices and procedures to ensure that human resource issues did not trump privacy;
- Hospital was ordered to implement a protocol that would require immediate steps are taken, upon being notified of an actual or potential privacy breach.

Commissioner's Message

The fact that:

- the nurse/girlfriend disregarded the hospital's policies and her own professional obligations;
- human resources policies trumped the privacy policies;
- the patient alerting the hospital to the threat from her estranged spouse was interpreted solely as a security risk, not a privacy risk;

- All of the above speak to the absence of a culture of privacy within the hospital;
- Privacy policies must be interwoven into the day-to-day fabric and operations of an organization.

Culture of Privacy

IPC

Building A Culture of Privacy

- A culture of privacy enables sustained collective action by providing people with a similarity of approach, outlook, and priorities;
- Importance of privacy must be the message from the top;
- Adequate resources must be devoted to privacy program;
- Privacy must be woven into the fabric of the day-to-day operations of an organization.

Benefits of a Commitment to Privacy

- Strong organizational image and reputation as a leader;
- Enhanced data quality and integrity;
- Enhanced patient trust;
- Savings in terms of time and money (e.g., avoid lawsuits, avoid requirement to notify individuals following a privacy breach).

Weaving Privacy into Day-to-Day Operations

- On-going privacy training and awareness program (new staff training; refresher training for existing staff, new threats to privacy, new technology threats and solutions);
- Policies and procedures for maintaining privacy must be clearly articulated and individuals must know how to apply them in the day-to-day work;
- Privacy must form part of the performance standard for every individual working in the information-intensive health care sector.

How is the IPC Helping?

IPC

How Is the IPC Helping?

- Providing a wide range of resources on our website;
- Working cooperatively with health information custodians to address issues and to respond to privacy breaches when they occur;
- Providing staff dedicated to respond to *PHIPA* inquiries and to provide review and comment on hospitals' polices, technology and programs;
- The IPC is always here to help you – just a call away.

Conclusion

- Privacy is an enabler of integration in the delivery of health care services, as well as in the implementation of health information technology;
- Privacy must be built into the design and implementation of new technologies – we call this ***"Privacy by Design;"***
- Privacy is a barrier to the unauthorized collection, use and disclosure of personal health information;
- IPC Orders highlight the privacy issues posed by various new technologies and provide guidance on best practices.

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