



*Avoiding Privacy Breaches ...  
Managing Them If They Occur*

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

**Primary Care eHealth Forum**  
*April 30, 2009*



# Presentation Outline

- 1. Personal Health Information*
- 2. Personal Health Information Protection Act (PHIPA)*
- 3. Costs of A Privacy Breach*
- 4. Preventing Privacy Breaches*
- 5. What to Do if A Privacy Breach Occurs*
- 6. Health Orders Under Ontario's PHIPA*
- 7. Conclusions*



# *Personal Health Information*



# 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.



*Personal Health  
Information Protection Act  
(PHIPA)*



# *Personal Health Information Protection Act (PHIPA)*

- Applies to organizations and individuals involved in the delivery of health care services (both public and private sector);
- The only health sector privacy legislation in Canada based on consent: implied consent within healthcare providers' "circle of care," otherwise, express consent;
- The only health sector privacy legislation that was declared to be substantially similar to Canada's federal private sector law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA).



# 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.





# *PHIPA – Section 12(1)*

## **Security**

A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information 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. 2004, c. 3, Sched. A, s. 12 (1).



# *PHIPA – Section 12(2)*

## **Notice of Loss**

Subject to subsection (3) and subject to the exceptions and additional requirements, if any, that are prescribed, 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. 2004, c. 3, Sched. A, s. 12 (2).



# *Costs of A Privacy Breach*



# Costs of A Privacy Breach

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



# Consequences of Inadequate Attention to Health Privacy

- Damage to a health provider's reputation, image, and business relationships (unwanted media, notification of patients);
- Psychological and economic harm to patients (identity theft, loss of insurance, employment, housing, etc.);
- Patients may withhold consent for the collection, use and disclosure of personal health information, making the effective delivery of care far more challenging;
- Unhappy patients can create an administrative burden for hospitals (e.g., placing additional lock box requests, filing complaints to the IPC, etc.);
- Dealing with a privacy breach, after the fact, can be time consuming and expensive (e.g., breach notification).



# Privacy Breaches

- One U.S. study found that from 2006/2007, over 1.5 million names were exposed during data breaches that occurred in hospitals.
  - 2008 HIMSS Analytics Report: Security of Patient Data, Kroll Fraud Solutions, April 2008.
- Another U.S. study found that the cost of a data breach was \$202 per record; the average cost per operating company was more than \$6.6 million per breach.
  - 2008 Annual Study: Cost of a Data Breach, Ponemon Institute, February 2009.



# Breach Management Costs

*“Our experience indicates that breach management costs between \$100 and \$200 per individual, but this does not consider the cost to our reputation and the erosion of trust.”*

— Jacqueline Malonda, et al,  
Health Care Quarterly, Vol.12, No. 1, 2009.



# Good Governance and Privacy: *Board of Directors*

## IPC Publication:

- Guidance to corporate directors faced with increasing responsibilities and expectation of openness and transparency;
- Privacy among the key issues that Boards of Directors must address;
- Potential risks if Directors ignore privacy;
- Great benefits to be reaped if privacy included in a company's business plan.





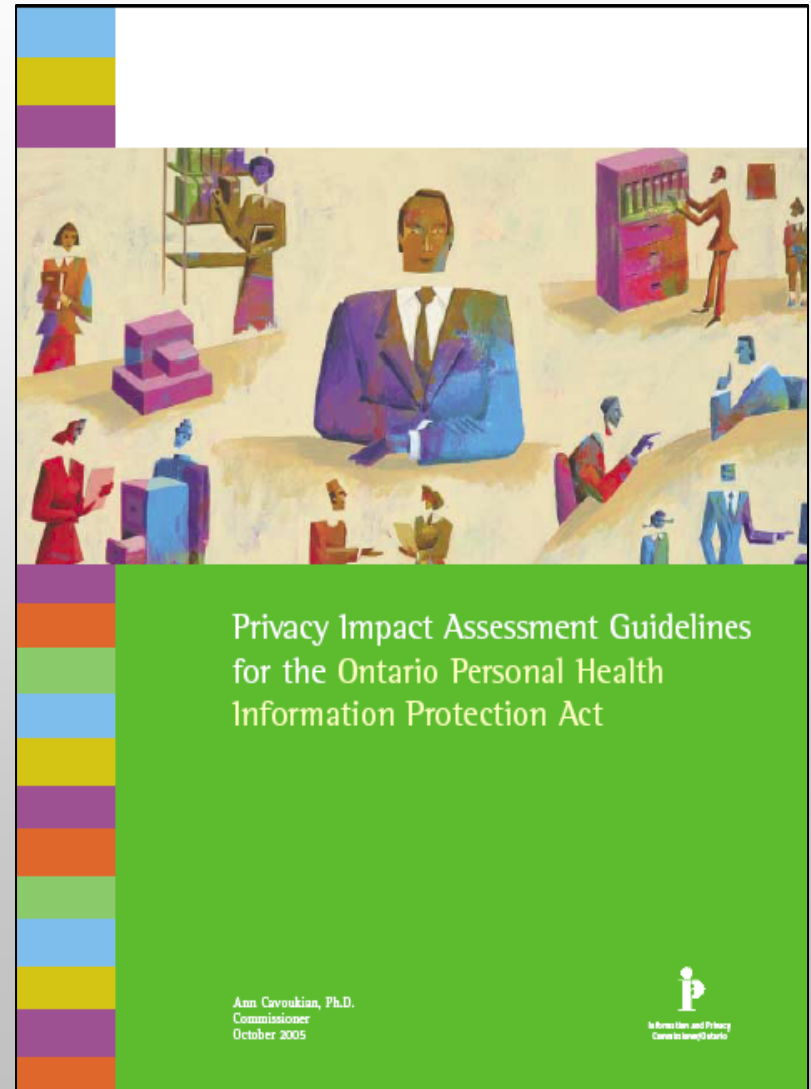


# *Preventing Privacy Breaches*



# Privacy Impact Assessment (PIA)

- A PIA is an assessment tool used to identify potential effects that a proposed or existing technology or program may have on individual privacy;
- The IPC developed this publication as a self-assessment tool to assist health information custodians in reviewing ways in which privacy risks can be mitigated.





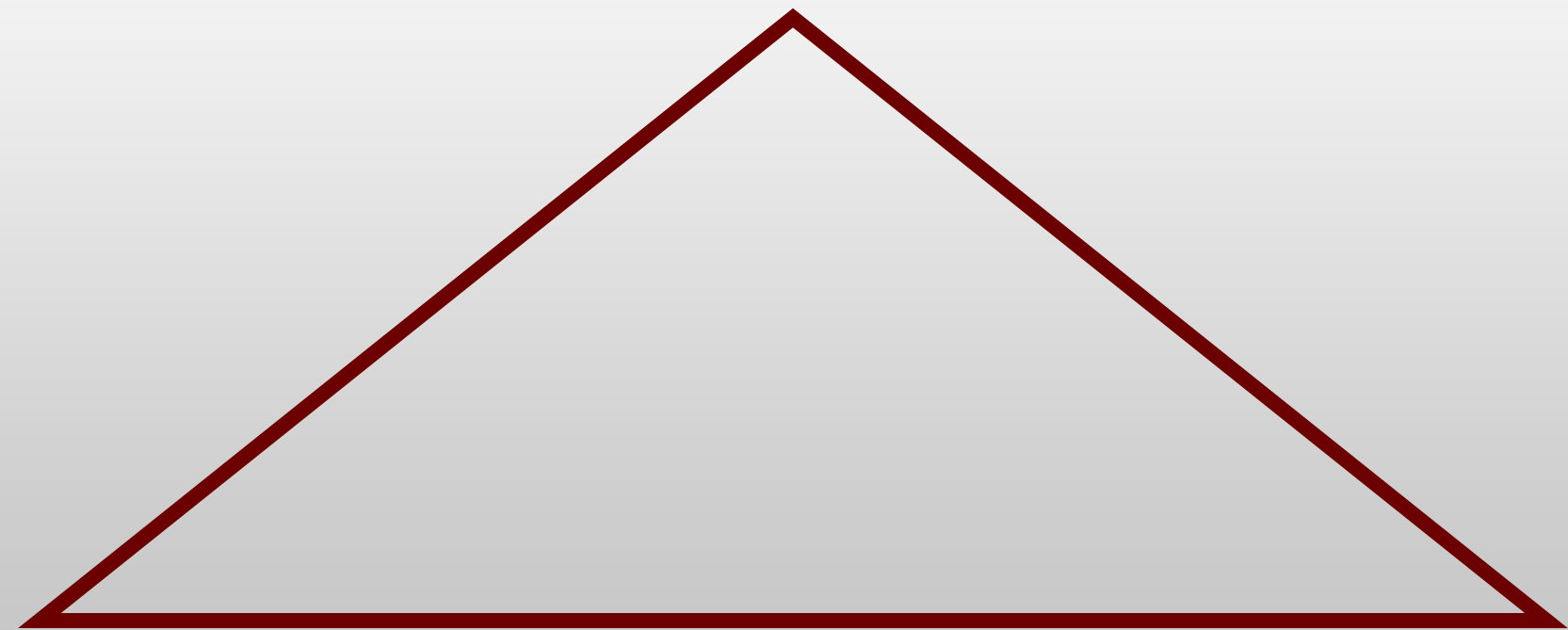
# Privacy by Design: “Build It In”

- I first developed the term “Privacy by Design” in the ‘90s, as a response to the growing threats to online privacy that were beginning to emerge;
- “Privacy by Design” seeks to build in privacy – up front, right into the design specifications; into the architecture; embed privacy into the technology used – *bake it in*;
- Data minimization is key: minimize the routine collection and use of personally identifiable information – use encrypted or coded information whenever possible;
- Use privacy-enhancing technologies (PETs) where possible: give people maximum control over their own data.



# Privacy by Design: The Trinity of Applications

**Information Technology**



**Business Practices**

**Physical Design**



# Privacy by Design: *Focus for 2009*

- **Technology** – Building privacy directly into technology, at the developmental stage;
- **Business Practices** – Incorporating privacy into competitive business strategies;
- **Physical Design** – Ensuring privacy and security in organizational and health care settings.

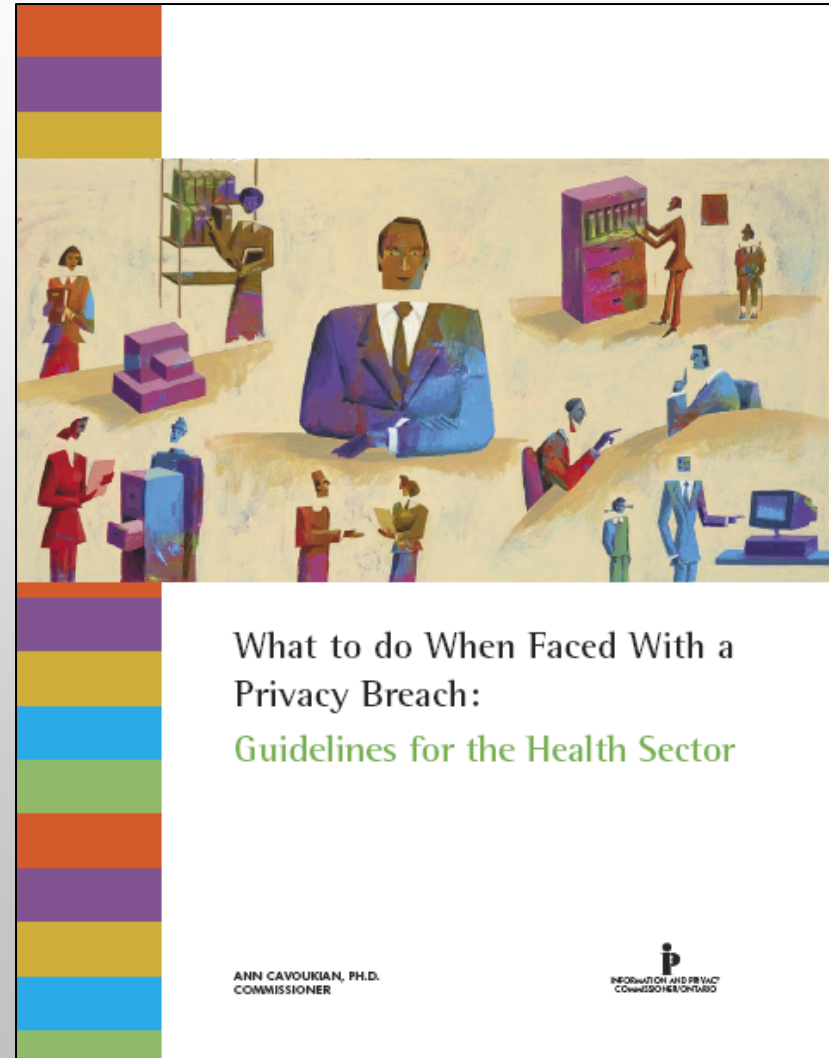


# *What to Do if A Privacy Breach Occurs*



# Implement A Privacy Breach Protocol

- Explains why you need a Privacy Breach Protocol;
- Covers steps including:
  - Respond immediately;
  - Contain the harm;
  - Notify patients;
  - Investigation and remediation.
- Tips to avoid breaches.





# Status of *PHIPA* Complaints

— *As of April 30, 2009*

- Total number of *PHIPA* complaints = 1,174;
- 1,113 are closed (95%); 61 are open (5%);

## **PHIPA complaints by category (open and closed):**

<b>TOTAL PHIPA COMPLAINTS (OPEN+CLOSED)</b>	<b>No.</b>	<b>%</b>
<b>Access/Correction</b>	<b>382</b>	<b>32%</b>
<b>Collection/Use/Disclosure</b>	<b>266</b>	<b>23%</b>
<b>HIC Reported Breach</b>	<b>423</b>	<b>36%</b>
<b>IPC Initiated Complaint</b>	<b>103</b>	<b>9%</b>
<b>Total Complaints</b>	<b>1,174</b>	<b>100%</b>





# *Health Orders Under PHIPA*



# 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

STAR 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 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 filming 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 diagnoses.



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](http://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 the 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- both employees of the hospital;
- 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 (Human Resources Policy) than the patient's right to privacy;
- Hospitals can have both – but HR cannot trump privacy.



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?



# Commissioner's Findings

- After receiving the privacy complaint, the hospital put a privacy/VIP flag on the patient's electronic medical record – but the nurse continued to access the patient's record;
- Found that the 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 its 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 to be taken upon being notified of an actual or potential privacy breach.



# Health Order No. 3: *Abandoned Records*

- College of Physicians and Surgeons of Ontario notified 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 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

- The landlord wrote to the owner of the Clinic three times regarding abandonment of PHI records and requested that the Clinic notify him if it wished to claim any property on the premises – the lease had no provision for the storage or retention of records;
- A representative of the Clinic claimed that he had arranged for the transfer of medical files to a professional storage company. Further, he also claimed that he had contacted the College of Physiotherapists of Ontario (CPO), for advice respecting “non-active files,” which the CPO denied;
- In the course of our investigation, we determined that the operator of the Clinic had no knowledge of *PHIPA* or the Clinic's obligations under the *Act*.



# 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*;
- 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.



# 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.



# Encrypting Personal Health Information on Mobile Devices

- Why are login passwords not enough?
- What is encryption?
- What are the options?
  - Whole disk (drive) encryption
  - Virtual disk encryption
  - Folder or Directory encryption
  - Device encryption
  - Enterprise encryption



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

## Fact Sheet

Number 12  
May 2007

### Encrypting Personal Health Information on Mobile Devices

Section 12 (1) of the *Personal Health Information Protection Act, 2004 (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.

The Office of the Information and Privacy Commissioner/Ontario recognizes that the delivery of health care may require the use of PHI outside of the workplace, and that such PHI may most effectively be transported and used in electronic form. Notwithstanding the ease of use and portability of electronic documents, it is still important that only the minimum necessary data be transported in this manner.

Because of the high incidence of loss or theft of mobile devices such as laptop computers, personal digital assistants (PDAs), or flash drives, custodians need to ensure that personal health information that is stored on mobile devices is encrypted. When encryption is implemented properly, it renders PHI safe from disclosure. The availability of encryption means that it is easier to safeguard electronic records of PHI than it is to safeguard paper-based records when being transported.

This fact sheet is intended for health information custodians who store PHI on mobile devices. However, it is also relevant to anyone who stores personal information on a mobile device. If you are unsure of the meaning of these guidelines, please consult a computer systems security expert to determine how to apply this fact sheet to the information in your care. In many cases, encryption can be as easy as installing a simple program and implementing proper key management for the system.

#### Why are login passwords not enough?

It is not acceptable to rely solely on login passwords to protect PHI on devices that are easily stolen or lost. "Strong" login passwords will prevent casual access to data on a device, but may not prevent access by knowledgeable thieves. Strong login passwords are usually characterized by:

- No dictionary words;
- A combination of letters, numbers and symbols;
- Eight or more characters, with 14 or more being ideal.

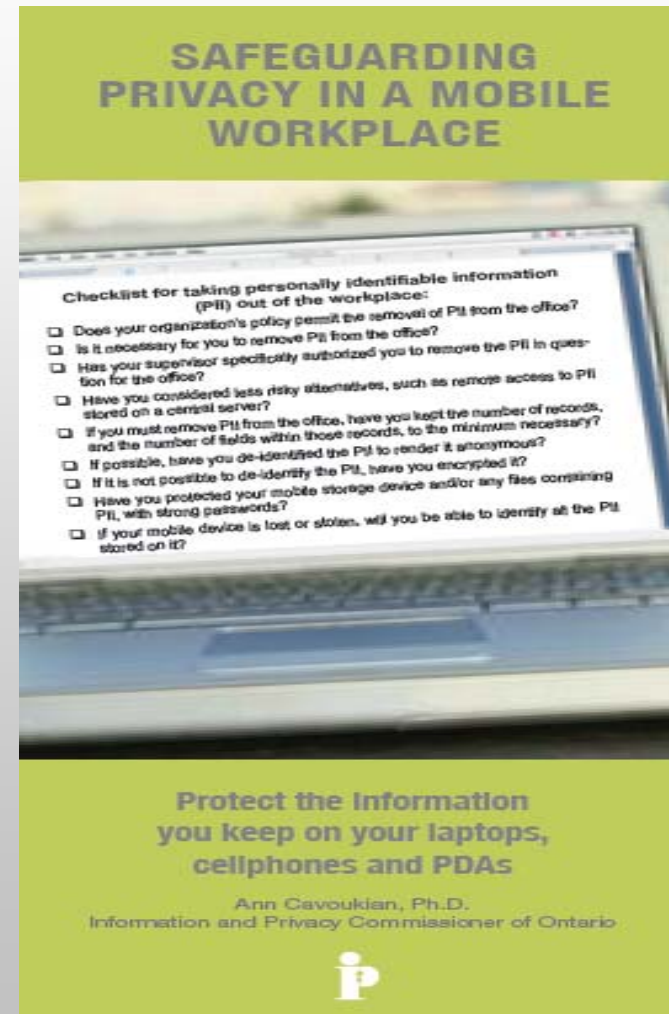
For example, "LetMeIn" is a weak password because it uses dictionary words. On the other hand, you could remember the phrase, "My birthday is October 21 and I'm 25"



# 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?





# Commissioner's Findings

- The laptop contained highly sensitive health 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 actually followed this protocol;
- The Hospital was ordered to either de-identify or encrypt all personal health information before allowing it to be removed from the workplace;
- Where personal health information is stored on a mobile, portable device, it must be encrypted.



# 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: Video Surveillance Systems*

- 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.



# Fact Sheet

## *Wireless Communication Technologies: Safeguarding Privacy & Security*

- A good starting point for understanding the impact of technological change is to regularly re-examine past assumptions and decisions;
- Any time wireless technology is used to transmit personal information, that information must be strongly protected to guard against unauthorized access to the contents of the signal.



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

### Fact Sheet

Number 14  
August 2007

#### Wireless Communication Technologies: Safeguarding Privacy & Security

**Taking Care**

We are fast approaching the point where it is reasonable to assume that any device that creates or stores data either has, or is connected to, some form of embedded wireless capability. Cellphones and personal digital assistants (PDAs) are increasingly sophisticated, often combining multiple wireless technologies in a single device.

Wireless technologies can reduce costs, increase efficiencies, and make important information more readily and widely available. In the health care sector, for example, wireless data communications now make it possible for paramedics to send cardiac images and data directly to cardiologists, significantly reducing wait time to treatment.

Clearly, the benefits of wireless communications are many. But, there are also risks. Without appropriate safeguards, transmitting data wirelessly can be like using an open filing cabinet in a waiting room. In fact, this Office just recently issued an Order about a case where unauthorized viewers had inadvertently intercepted wireless video images of patients in a washroom providing urine samples.

This Fact Sheet addresses privacy issues arising from the use of wireless technologies, expanding on Fact Sheet #13, *Wireless Communication Technologies: Video Surveillance Systems*.

The *Personal Health Information Protection Act* (PHIPA), the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) set out requirements for the protection of personal information, including information in electronic form.

In general, compliance with these Acts requires that those responsible take reasonable measures to protect personal information, which may include physical safeguards, using role-based access to personal information, or technological measures such as encryption.

The transmission of personal information in electronic form, particularly through the use of wireless technologies, means adding "data-in-motion" to "data-at-rest" as a category of data to protect, and adds another layer of complexity to compliance with these Acts.

A good starting point for understanding the impact of technological change or new developments is to regularly re-examine past assumptions and decisions. A reasonable precaution is one that any prudent and privacy conscious individual or institution would take. For example, there was a time when it was reasonable to browse the web and download files without



# Conclusions

- Privacy breaches can be costly, both financially and to your reputation;
- Custodians should take proactive steps to *prevent* privacy breaches – don't wait for one to occur;
- Custodians should have a Privacy Breach Protocol in place to respond immediately to breaches;
- IPC Health Orders have important messages for all custodians wishing to avoid breaches;
- For each Order, the IPC issues an educational document (often a Fact Sheet or brochure) to assist custodians in complying with the Order.



# 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) 326-3948 / 1-800-387-0073**

**Web: [www.ipc.on.ca](http://www.ipc.on.ca)**

**E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)**