Complying with the Personal Health Information Protection Act

Debra Grant, Ph.D.

Office of the Information and Privacy Commissioner of Ontario

Annual Meeting and Education Day
Ontario College of Social Workers and Social Services Workers
June 19, 2014

Presentation Outline

1. *Importance of PHI*
2. *Application of PHIPA*
3. *Duties Imposed by PHIPA*
4. *Transparency of Information Practices*
5. *Collection, Use and Disclosure*
6. *Security of PHI*
7. *Privacy by Design*
8. *Hot Topics*

Personal Health Information
A Unique Type of Personal Information

The need to protect the privacy of individuals' personal health information has never been greater given the:

- Extreme sensitivity of personal health information
- Number of persons involved in health care
- Emphasis on information technology including electronic records of personal health information
- Need to use or disclose health information for secondary purposes seen to be in the public interest (i.e. research, planning, surveillance)

Why is the Protection of Privacy in Important?

If inadequate attention is paid to the protection of privacy of individuals, it may result in:

- Discrimination, stigmatization and economic or psychological harm to the individuals based on the information
- Loss of trust or confidence in the health system
- Individuals being deterred from seeking information, testing or treatment for certain disease
- Individuals withholding or falsifying information

APPLICATION OF THE ACT

Definition of Personal Health Information

Defined as identifying information that:

- Relates to an individual's physical or mental health
- Relates to the provision of health care to the individual
- Identifies an individual's health care provider
- Identifies an individual's substitute decision-maker
- Relates to payments or eligibility for health care
- Is the individual's health number
- Relates to the donation of body parts or bodily substances
- Is a plan of service under *Long-Term Care Act, 1994*

Definition of Health Information Custodian

Health information custodians include:

- A health care practitioner or a person who operates a group practice of health care practitioners
- A medical officer of health of a board of health within the meaning of the *Health Protection and Promotion Act*
- A person who operates a long-term care home within the meaning of the *Long-Term Care Homes Act, 2007*, a placement coordinator, or a care home within the meaning of the *Residential Tenancies Act, 2006*.
- A person who operates an ambulance service within the meaning of the *Ambulance Act*
- A community care access corporation
- A person who operates a hospital, psychiatric facility, independent health facility, pharmacy, laboratory or specimen collection centre
- Minister/Ministry of Health and Long-Term Care
- Minister/Ministry of Health Promotion

Definition of Agent

- An agent is a person that, with the authorization of a health information custodian, acts for or on behalf of the custodian in respect of personal health information
- It is irrelevant whether or not the agent:
  - is employed by the health information custodian
  - is remunerated by the health information custodian
  - has the authority to bind the health information custodian
- A health information custodian remains responsible for personal health information collected, used, disclosed, retained or disposed of by an agent

DUTIES IMPOSED BY THE ACT

Duties Imposed on Health Information Custodians and Their Agents

- A number of duties are imposed on health information custodians and their agents under the Act
- These duties generally fall into four categories:
  - Transparency of information practices
  - Collection, use and disclosure of personal health information
  - Security of personal health information
  - Requests for access and correction to records of personal health information
- This presentation will be limited to a discussion of the first three categories of duties

TRANSPARENCY OF INFORMATION PRACTICES

Designate a Contact Person

Designate or perform the functions of a contact person who is authorized to:

- Facilitate compliance with the Act
- Ensure all agents are appropriately informed of their duties
- Respond to inquiries in relation to information practices
- Respond to the requests of individuals for access to or correction of their records of personal health information
- Receive complaints about alleged contraventions of the Act

Information Practices

Have information practices that comply with the Act, including policies and procedures in relation to:

- When, how and the purposes for which personal health information is collected, used, disclosed, retained or disposed
- Administrative, technical and physical safeguards and practices implemented with respect to personal health information

Transparency of Information Practices

Have and make available a written public statement that describes:

- The information practices of the health information custodian
- How to contact the contact person
- How an individual may obtain access or request a correction of his or her records of personal health information
- How an individual may make a complaint to the custodian and to the Information and Privacy Commissioner/Ontario

COLLECTION, USE AND DISCLOSURE

General Provisions Related to Collection, Use and Disclosure

- Not permitted to collect, use or disclose personal health information if other information will serve the purpose of the collection, use or disclosure
- Not permitted to collect, use or disclose more personal health information than reasonably necessary to meet the purpose of the collection, use or disclosure
- Not permitted to collect, use or disclose personal health information UNLESS:
  - The individual consents, or
  - The collection, use or disclosure is permitted or required by the Act to be made without consent

CONSENT PROVISIONS

Overview of Consent Provisions

- There are three types of consent under the Act:
  - Express consent
  - Implied consent
  - Assumed implied consent

- The assumed implied consent provisions are referred to as the “circle of care” provisions although the term “circle of care” does not appear in the Act

Express Consent

- Consent may be express or implied, except when the Act specifies that consent must be express
- Express consent is not a defined term in the Act
- It is commonly understood as consent that has been clearly and unmistakably given orally or in writing
- Express consent is required to:
  - *Disclose* personal health information to a non-health information custodian (subject to certain exceptions)
  - *Disclose* personal health information to another health information custodian for a purpose other than the provision of health care (subject to certain exceptions)
  - *Collect*, *use* or *disclose* personal health information for marketing
  - *Collect*, *use* or *disclose* personal health information for fundraising (if it amounts to more than the name and address of the individual)

Implied Consent

- In all other circumstances, consent may be implied
- Implied consent is not a defined term in the Act
- Commonly understood as a consent that one concludes has been given based on an individual's action or inaction in particular factual circumstances
- For example, consent may be implied:
  - To *collect* or *use* personal health information for any purpose, subject to certain exceptions
  - To *disclose* personal health information to another health information custodian for the provision of health care

Elements for Valid Consent

Consent, whether express or implied, must:

1. Be the consent of the individual or his or her substitute decision-maker (where applicable),

2. Be knowledgeable, meaning, it must be reasonable to believe that the individual knows:
   - The purpose of the collection, use or disclosure; and
   - That the individual may give or withhold consent

3. Relate to the information, and

4. Not be obtained by deception or coercion.

Notice of Purposes

- A custodian may rely on a *Notice of Purposes* to support the reasonable belief that an individual knows the purpose of the collection, use or disclosure of personal health information unless it is not reasonable

- A *Notice of Purposes*:
  - Must be posted where it is likely to come to the attention of the individual or must be provided to the individual;
  - Must outline the purposes for which the custodian collects, uses or discloses personal health information; and
  - Should advise the individual that he or she has the right to give or withhold consent

- A *Notice of Purposes* is not required when consent may be assumed to be implied but it is a best practice

Notice of Purposes

Health Information Privacy in our Office

PERSONAL HEALTH INFORMATION AND PRIVACY

Ontario has a law that protects your personal health information.
You have the right to know how we may use and give out your personal health information and how you can get access to it.
Please ask to see our Brochure and Privacy Statement for more details on our privacy practices.

WHO CAN USE AND SEE YOUR PERSONAL HEALTH INFORMATION

Your personal health information must be kept private and secure.
You or a person who can legally make decisions for you about your personal health information can use and see it.
Your personal health information is shared among the people who provide you with health care. We may collect, use and give out your personal health information to others as reasonably necessary to:

- provide you with health care;
- communicate with or consult other health care providers or students in training for your health care;
- get payment for your health care, including from OHIP and private insurance; and
- report as required or permitted by law.

There are certain other circumstances where we may be required give out some of your personal health information. If you want to know more, please see our Brochure, or speak to us.

YOUR RIGHTS AND CHOICES

You or a person who can make decisions for you about your personal health information have the right:

- to see and get a copy of your personal health information;
- to ask us to make corrections to inaccurate or incomplete personal health information;
- to ask us not to give out your personal health information to other health care providers – we will not give out this information unless required or permitted by law to do so; and
- to be told if your personal health information is stolen, lost or improperly accessed.

There are certain exceptions to these rights – please see our Brochure for more information.

WHO YOU CAN TALK TO ABOUT YOUR DECISIONS

Where you give us permission to use or give out your information, you may change your mind at any time.
However, sometimes the law allows or requires us to give out your information without your permission.
For more information, please see our Brochure.
To make your choices, please speak to our Contact Person below.

OTHER IMPORTANT INFORMATION

We are required to keep your personal health information safe and secure. We will get your permission before we give out your personal health information to others

- who want to offer you their products or services, or
- for certain research projects where your consent is required.

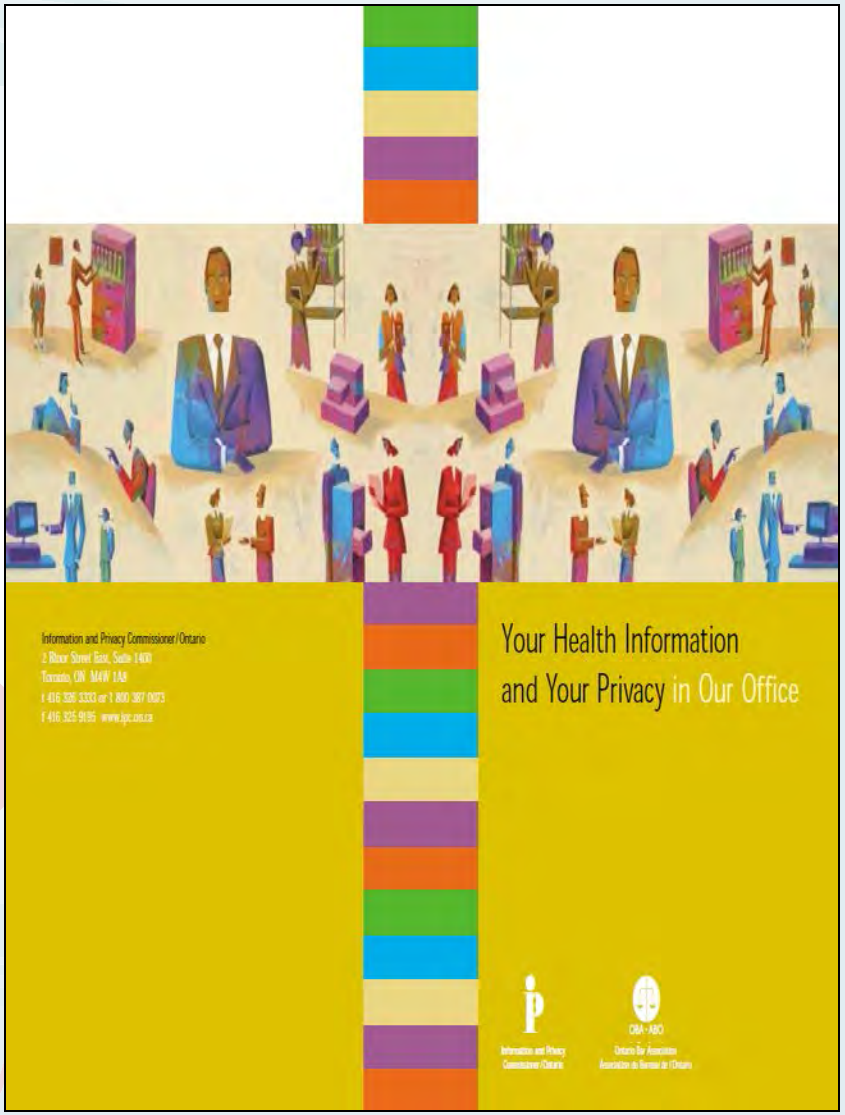
Please ask us or see our Brochure for more details.

HOW TO REACH US

If you have questions or concerns about our privacy practices, please speak to Our Contact Person:

Name: _____ Phone Number: _____

The Information and Privacy Commissioner of Ontario is responsible for making sure that privacy law is followed in Ontario. For more information about your privacy rights, or if you are not able to resolve a problem directly with us and wish to make a complaint, contact: Information and Privacy Commissioner of Ontario, 2 Bloor Street East, Suite 1400, Toronto, Ontario, M4W 1A8; Toll Free: 1-800-387-0073; www.ipc.on.ca



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

Your Health Information and Your Privacy in Our Office

Information and Privacy Commissioner / Ontario

OBA · ABO
Ontario Bar Association
Association du Barreau de l'Ontario

Assumed Implied Consent – Circle of Care

- Certain health information custodians *may* assume implied consent to collect, use or disclose personal health information in defined circumstances

- The assumed implied consent provisions have come to be referred to as the "circle of care" provisions although "circle of care" does not appear in the Act

- A health information custodian may only assume implied consent if six conditions are satisfied

Conditions to be Satisfied to Assume Implied Consent

A health information custodian may only assume implied consent if **all** six conditions are satisfied:

1. The health information custodian falls within a category of health information custodians that are entitled to rely on assumed implied consent

   - Some health information custodians are not entitled to rely on assumed implied consent, such as:
     - An evaluator as defined in the *Health Care Consent Act, 1996*
     - An assessor as defined in the *Substitute Decisions Act, 1992*
     - The Minister or Ministry of Health and Long-Term Care
     - The Minister or Ministry of Health Promotion

Conditions to be Satisfied to Assume Implied Consent (cont'd)

2. The personal health information must have been received from the individual, his or her substitute decision-maker or another custodian
   - It must not have been received from any other person such as an employer, insurer or educational institution

3. The personal health information must have been received for providing or assisting in providing health care to the individual to whom it relates
   - It must not have been received for other purposes, such as providing health care to another individual

Conditions to be Satisfied to Assume Implied Consent (cont'd)

4. The purpose of the collection, use or disclosure must be for providing or assisting in providing health care to the individual to whom the information relates
   - It must not be collected, used or disclosed for any other purpose, such as research, fundraising or marketing

5. In the context of a disclosure, the disclosure must be to another health information custodian
   - Personal health information must not be disclosed to any other person regardless of the purpose of the disclosure

Conditions to be Satisfied to Assume Implied Consent (cont'd)

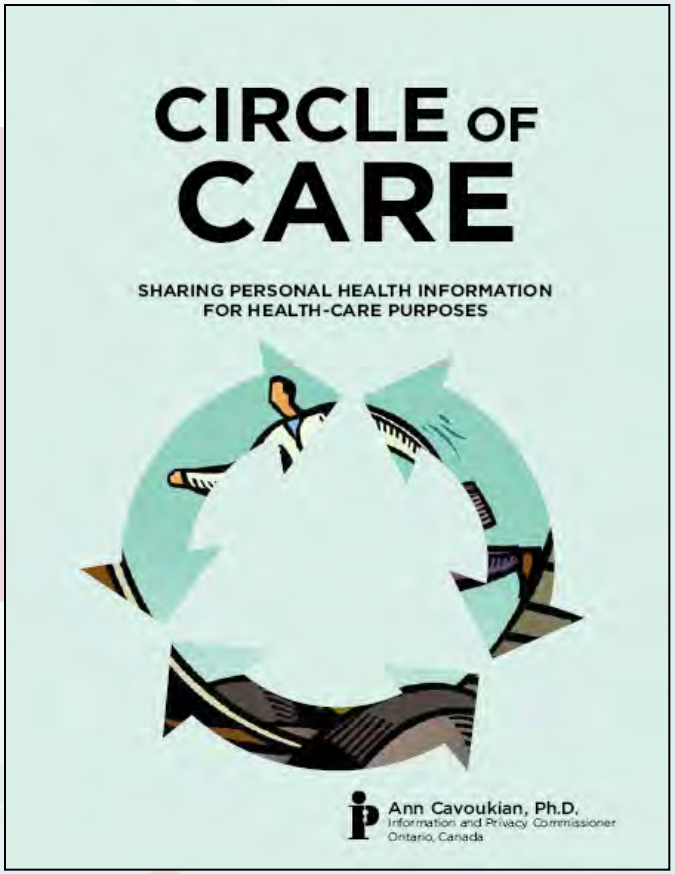
6. The health information custodian that receives the personal health information from the individual, his or her substitute decision-maker or the other health information must not be aware that the individual has expressly withheld or withdrawn consent

Circle of Care: Sharing Personal Health Information for Health Care Purposes

The guide was published to clarify the circumstances in which consent may be *assumed* to be implied by custodians

Members of the working group who participated in publishing the guide, included:

- Information and Privacy Commissioner/Ontario
- College of Physicians and Surgeons of Ontario
- Ontario Association of Community Care Access Centres
- Ontario Association of Non-Profit Homes and Services for Seniors
- Ontario Long Term Care Association
- Ontario Hospital Association
- Ontario Medical Association
- Ontario Ministry of Health and Long-Term Care



Available at www.ipc.on.ca

COLLECTION, USE AND DISCLOSURE WITHOUT CONSENT

Permitted Collections Without Consent

Permitted in certain circumstances, such as where:

- The health information custodian is an institution under FIPPA/MFIPPA or is acting as part of such an institution and the collection is for a purpose related to
  - Conducting a proceeding or possible proceeding;
  - Investigating a breach of agreement or contravention of the law; or
  - The statutory function of the health information custodian
- It is collected from a person permitted or required by law to disclose it to the health information custodian
- The health information custodian is permitted or required by law to collect the personal health information indirectly

Permitted Uses Without Consent

Permitted in certain circumstances, such as:

- For the purposes for which it was collected or created and all functions reasonably necessary to carry out that purpose
- Planning or delivering programs or services, error management, risk management and activities to improve or maintain the quality of programs or services
- Educating agents to provide health care
- For a proceeding or contemplated proceeding in which the health information custodian or an agent is a party or witness
- Uses permitted or required by law
- Research provided a written research plan is prepared, the research is approved by a research ethics board and the researcher agrees to comply with conditions in the Act

Permitted Disclosures Without Consent

Permitted in certain circumstances, such as:

- To the Ontario College of Social Workers and Social Service Worker for the purpose of the administration or enforcement of the *Social Work and Social Service Work Act, 1998*
- To the Chief Medical Officer of Health or a Medical Officer of Health for *Health Protection and Promotion Act* purposes
- To the Ontario Agency for Health Protection and Promotion for purposes of the *Ontario Agency for Health Protection and Promotion Act, 2007*
- Where the individual is deceased, for the purpose of identifying the individual and informing others that the individual is deceased, or to family members that require the information to make decisions about their own health care or that of their children
- If there are reasonable grounds to believe that the disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm to a person or group of persons

Permitted Disclosures Without Consent

- To comply with a summons, court order or similar requirement
- To a person carrying out an inspection, investigation or similar procedure authorized by warrant or by or under an Act
- Where permitted or required by law
- For a proceeding or contemplated proceeding in which the health information custodian or agent is a party or witness
- To a researcher for research purposes provided:
  - Receive a written application
  - Receive a written research plan that complies with the Act
  - The written research plan received research ethics board approval
  - Enter into an agreement with the researcher that satisfies the Act

SECURITY OF PERSONAL HEALTH INFORMATION

Security of Personal Health Information

- Must ensure records of personal health information are retained, transferred and disposed of securely
- Must take reasonable steps to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure and that records of personal health information are protected against unauthorized copying, modification or disposal.
- Must notify an individual at the first reasonable opportunity if personal health information is stolen, lost or accessed by unauthorized persons

Implementation of Administrative, Technical and Physical Safeguards

Administrative Safeguards Include:

- Requiring agents to execute confidentiality agreements
- Requiring agents to attend privacy and security training
- Limiting persons with access to personal health information
- Developing, monitoring and enforcing privacy and security policies
- Conducting privacy impact assessments on information systems, technologies or programs that involve personal health information

Technical Safeguards Include:

- Building privacy into the design of information systems, technologies or programs
- Implementing encryption, pseudonymization, anonymization
- Instituting strong authentication measures
- Implementing detailed audit monitoring systems

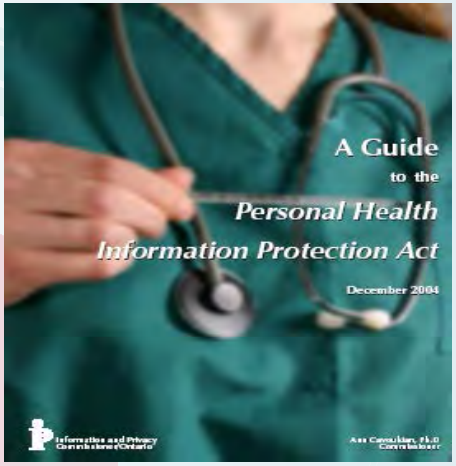
Physical Safeguards Include:

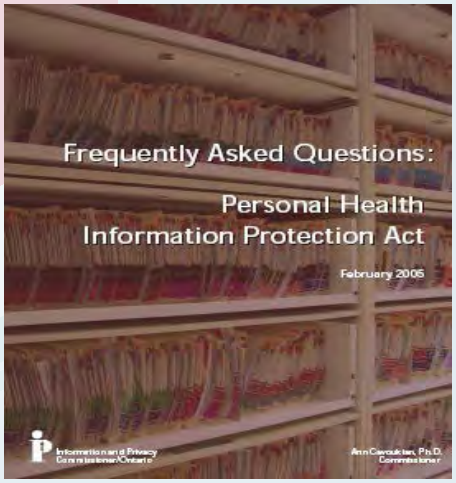
- Access control for areas where records of personal health information are retained
- Retaining records of personal health information in a secure area
- Deploying routine surveillance

Available Tools and Resources

Tools and resources are available on our website, www.ipc.on.ca, including:

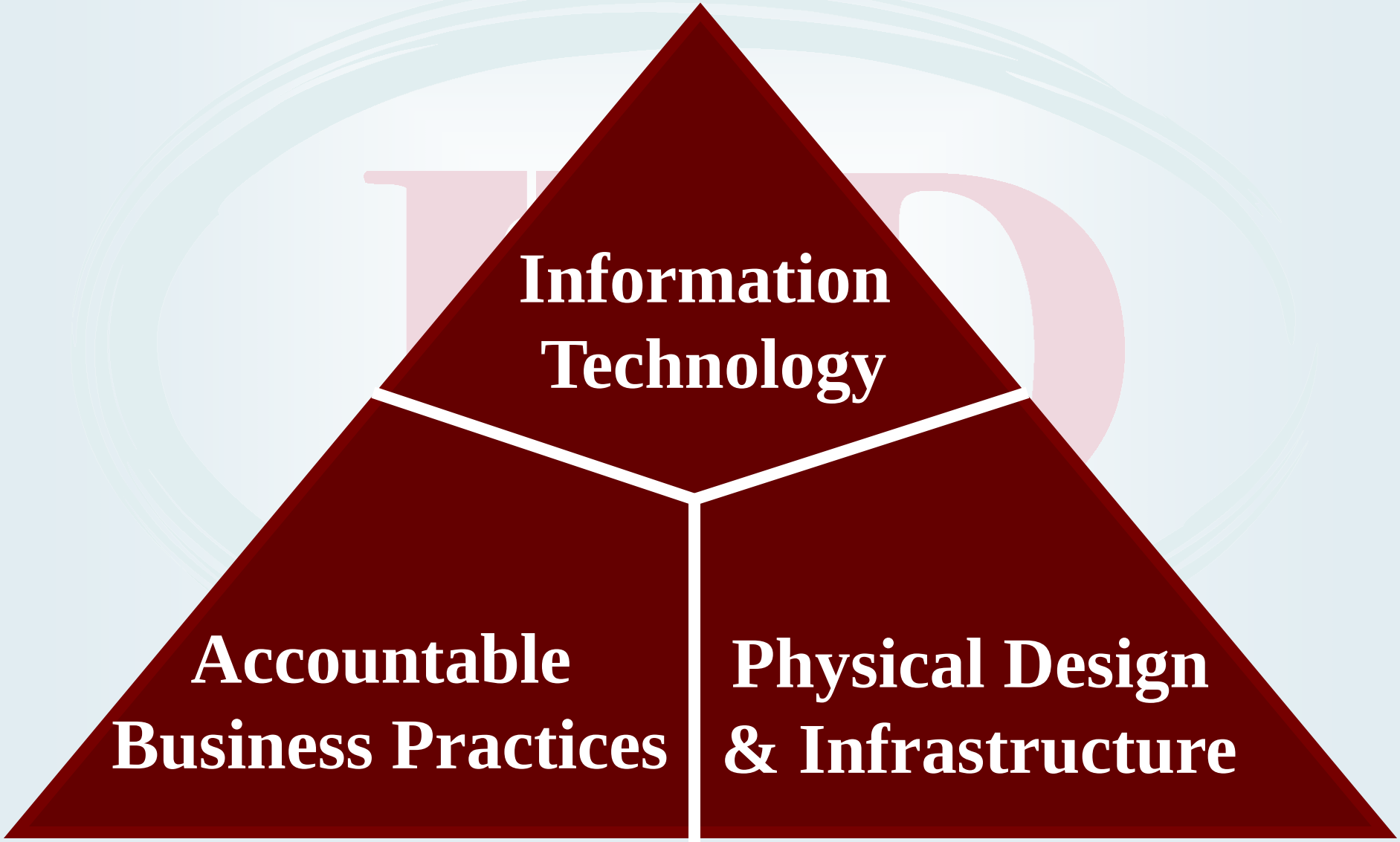
- Guide to the *Personal Health Information Protection Act*
- Frequently Asked Questions: *Personal Health Information Protection Act*
- Safeguarding Personal Health Information Fact Sheet
- Secure Destruction of Personal Information Fact Sheet
- Disclosure of Information in Emergency or Urgent Circumstances Fact Sheet
- Wireless Communication Technologies: Safeguarding Privacy and Security Fact Sheet
- Encrypting Personal Health Information on Mobile Devices Fact Sheet
- Safeguarding Privacy in a Mobile Workplace
- Privacy Impact Assessment Guidelines for the Ontario *Personal Health Information Protection Act*
- What to do When Faced With a Privacy Breach: Guidelines for the Health Sector





Privacy by Design

Privacy by Design:
The Trilogy of Applications



Privacy by Design: “Build It In”

- The term “Privacy by Design” was introduced 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 Will Help You Avoid

- Potential harm to individuals, including discrimination, stigmatization and economic or psychological harm
- Loss of trust or confidence in e-health by individuals and the health sector
- Damage to your reputation
- The time, expenses and resources necessary to contain, investigate and remediate privacy breaches
- The costs associated with legal liabilities and proceedings
- Potentially detrimental privacy protective behaviors, such as individuals not seeking treatment; withholding or providing false information and using multiple providers

High Cost of Taking a Reactive Approach to Privacy Breaches

Proactive

Lawsuits

Damage to Relationships and Reputation

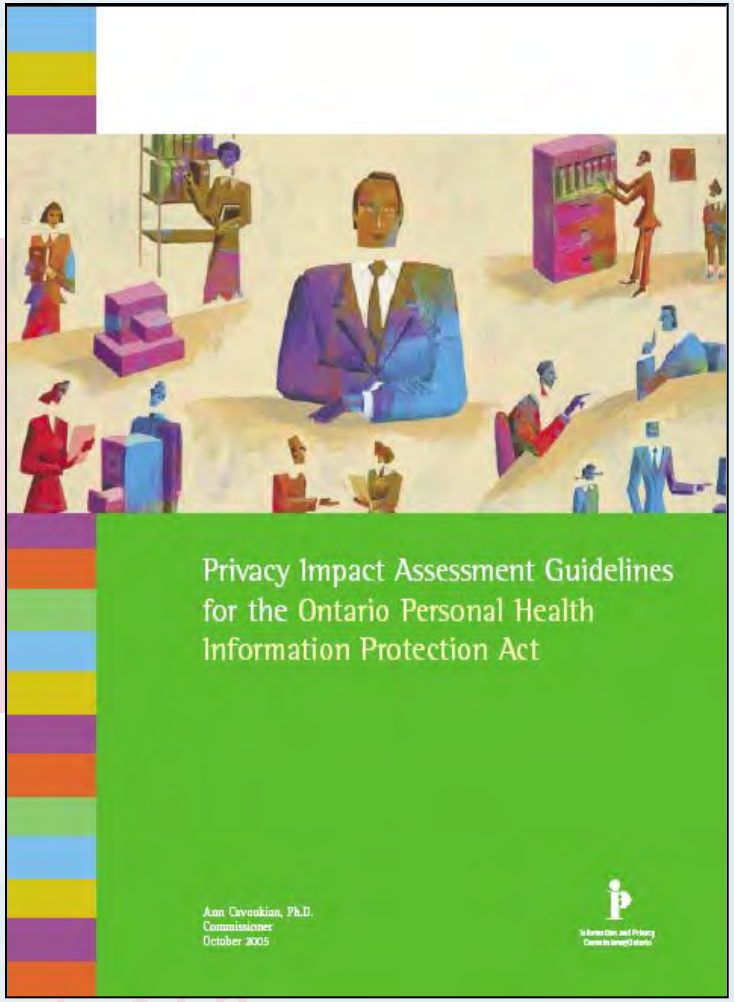
Reactive

Loss of Patient Confidence and Trust

Privacy Impact Assessments

The purpose of a privacy impact assessment is to:

- Review the impact an information system, technology or program has on privacy
- Identify, address and mitigate actual or potential risks to the privacy of individuals
- Ensure the contemplated retention, collection, use, disclosure and disposal of personal health information complies with the *Act*
- Ensure reasonable steps are taken to ensure personal health information is protected against theft, loss and unauthorized use or disclosure and that records of personal health information are protected against authorized copying, modification and disposal
- Ensure personal health information is retained, transferred and disposed securely



Privacy by Design: The 7 Foundational Principles

1. ***Proactive*** not ***Reactive***: Preventative, not Remedial;
2. Privacy as the ***Default*** setting;
3. Privacy ***Embedded*** into Design;
4. ***Full*** Functionality: Positive-Sum, not Zero-Sum;
5. End-to-End **Security**: Full Lifecycle Protection;
6. Visibility **and** Transparency: Keep it **Open**;
7. Respect for User Privacy: Keep it **User-Centric**.

PbD

www.privacybydesign.ca

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

HOT ISSUES….

SECURITY OF PERSONAL HEALTH INFORMATION

Provisions in the Act Relating to the Security of Personal Health Information

- Must ensure records of personal health information are retained, transferred and disposed of securely
- Must take reasonable steps to ensure personal health information is protected against:
  - Theft, loss and unauthorized use or disclosure
  - Unauthorized copying, modification or disposal
- Must notify individuals at the first reasonable opportunity if personal health information is stolen, lost or accessed by unauthorized person

1. Secure Disposal of Records

Order HO-001
Nature of the Incident

- A medical clinic hired a company to shred records of personal health information
- Due to a misunderstanding, the records were sent for recycling instead of being shredded
- The recycling company sold the records to a special effects company and were used in a film shoot

Film shoot uses real medical records

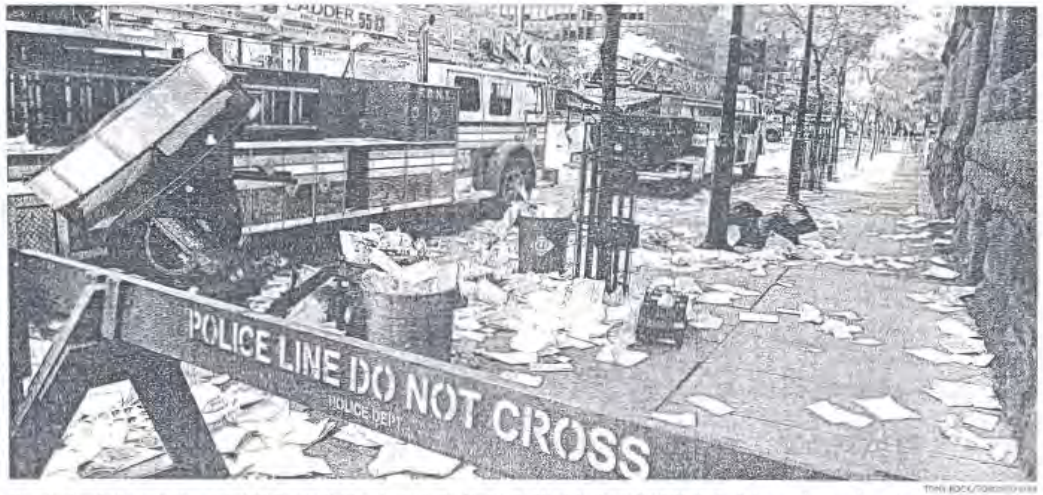
Privacy official has plans to investigate

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-



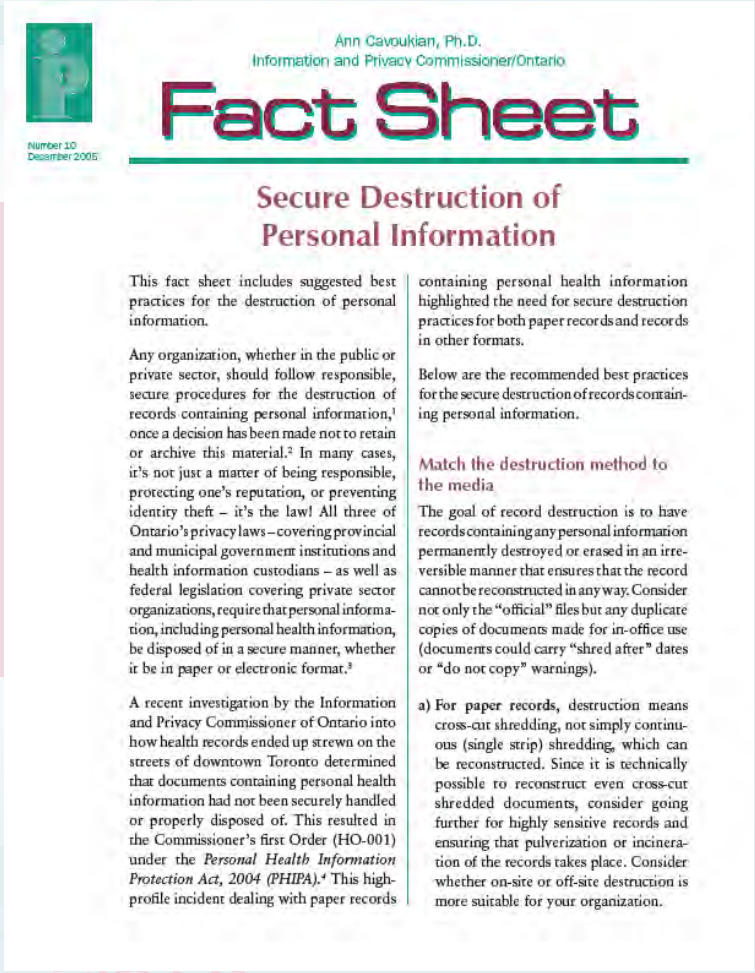
Mounds of medical records strewn along Wellington St. W. yesterday during filming of a TV miniseries on the 9/11 attacks. Below, an ultrasound report picked from the pile.

Order HO-006
Nature of the Incident

- Employees of a laboratory placed records of personal health information in boxes designated for recycling as opposed to that designated for shredding
- The boxes designated for recycling were located immediately beside boxes designated for shredding
- The records of personal health information were found scattered on the street outside the laboratory

Lessons Learned From Orders HO-001 and HO-006

- Ensure records of personal health information are disposed in a secure manner such that reconstruction is not reasonably foreseeable in the circumstances
- For paper records this means cross-cut shredding and, if the records are particularly sensitive, pulverization or incineration should be considered
- For electronic records this means physically damaging and discarding the media rendering it unusable or if re-use is preferred, using wiping utilities



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

Fact Sheet

Number 10
December 2005

Secure Destruction of Personal Information

This fact sheet includes suggested best practices for the destruction of personal information.

Any organization, whether in the public or private sector, should follow responsible, secure procedures for the destruction of records containing personal information,[1] once a decision has been made not to retain or archive this material.[2] In many cases, it's not just a matter of being responsible, protecting one's reputation, or preventing identity theft – it's the law! All three of Ontario's privacy laws – covering provincial and municipal government institutions and health information custodians – as well as federal legislation covering private sector organizations, require that personal information, including personal health information, be disposed of in a secure manner, whether it be in paper or electronic format.[3]

A recent investigation by the Information and Privacy Commissioner of Ontario into how health records ended up strewn on the streets of downtown Toronto determined that documents containing personal health information had not been securely handled or properly disposed of. This resulted in the Commissioner's first Order (HO-001) under the *Personal Health Information Protection Act, 2004 (PHIPA)*.[4] This high-profile incident dealing with paper records containing personal health information highlighted the need for secure destruction practices for both paper records and records in other formats.

Below are the recommended best practices for the secure destruction of records containing personal information.

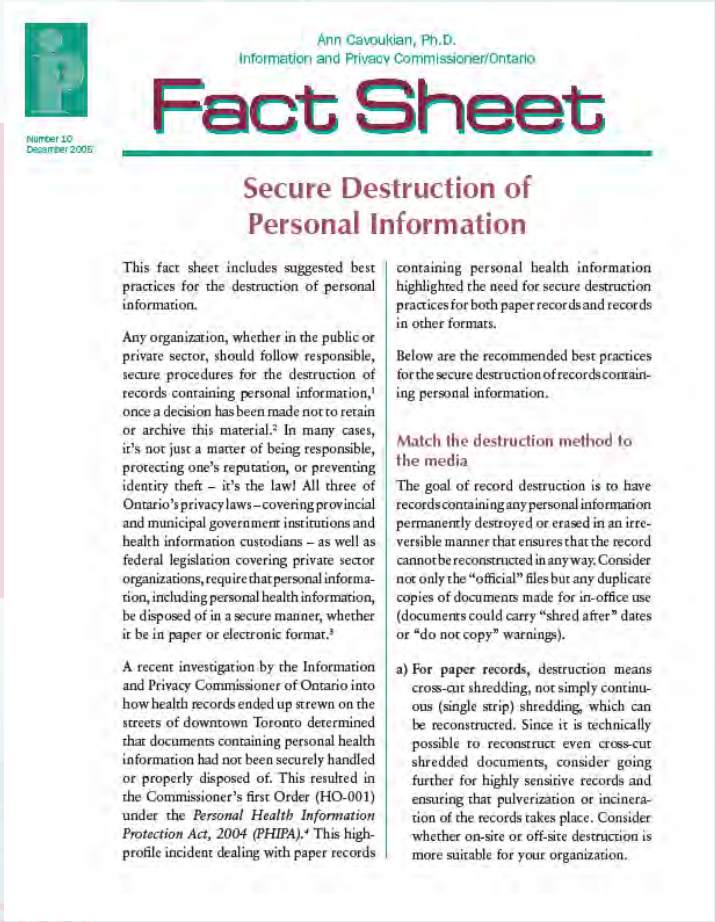
Match the destruction method to the media

The goal of record destruction is to have records containing any personal information permanently destroyed or erased in an irreversible manner that ensures that the record cannot be reconstructed in any way. Consider not only the "official" files but any duplicate copies of documents made for in-office use (documents could carry "shred after" dates or "do not copy" warnings).

a) **For paper records,** destruction means cross-cut shredding, not simply continuous (single strip) shredding, which can be reconstructed. Since it is technically possible to reconstruct even cross-cut shredded documents, consider going further for highly sensitive records and ensuring that pulverization or incineration of the records takes place. Consider whether on-site or off-site destruction is more suitable for your organization.

Lessons Learned From Orders HO-001 and HO-006

- If a third party is retained to dispose of records, check references, ensure the third party is accredited or is willing to undergo independent audits and enter an agreement that:
  - Sets out the third party's responsibilities in securely disposing of the records
  - Sets out who, how and under what conditions records will be securely disposed
  - Requires the third party to provide a signed written attestation setting out the date, time and location of the secure disposal
  - Requires the secure storage of the records pending their secure disposal
  - Specifies the time frame within which the records will be securely disposed



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

Fact Sheet

Number 10
December 2005

Secure Destruction of Personal Information

This fact sheet includes suggested best practices for the destruction of personal information.

Any organization, whether in the public or private sector, should follow responsible, secure procedures for the destruction of records containing personal information,[1] once a decision has been made not to retain or archive this material.[2] In many cases, it's not just a matter of being responsible, protecting one's reputation, or preventing identity theft – it's the law! All three of Ontario's privacy laws – covering provincial and municipal government institutions and health information custodians – as well as federal legislation covering private sector organizations, require that personal information, including personal health information, be disposed of in a secure manner, whether it be in paper or electronic format.[3]

A recent investigation by the Information and Privacy Commissioner of Ontario into how health records ended up strewn on the streets of downtown Toronto determined that documents containing personal health information had not been securely handled or properly disposed of. This resulted in the Commissioner's first Order (HO-001) under the *Personal Health Information Protection Act, 2004 (PHIPA).*[4] This high-profile incident dealing with paper records containing personal health information highlighted the need for secure destruction practices for both paper records and records in other formats.

Below are the recommended best practices for the secure destruction of records containing personal information.

Match the destruction method to the media

The goal of record destruction is to have records containing any personal information permanently destroyed or erased in an irreversible manner that ensures that the record cannot be reconstructed in any way. Consider not only the "official" files but any duplicate copies of documents made for in-office use (documents could carry "shred after" dates or "do not copy" warnings).

a) **For paper records,** destruction means cross-cut shredding, not simply continuous (single strip) shredding, which can be reconstructed. Since it is technically possible to reconstruct even cross-cut shredded documents, consider going further for highly sensitive records and ensuring that pulverization or incineration of the records takes place. Consider whether on-site or off-site destruction is more suitable for your organization.

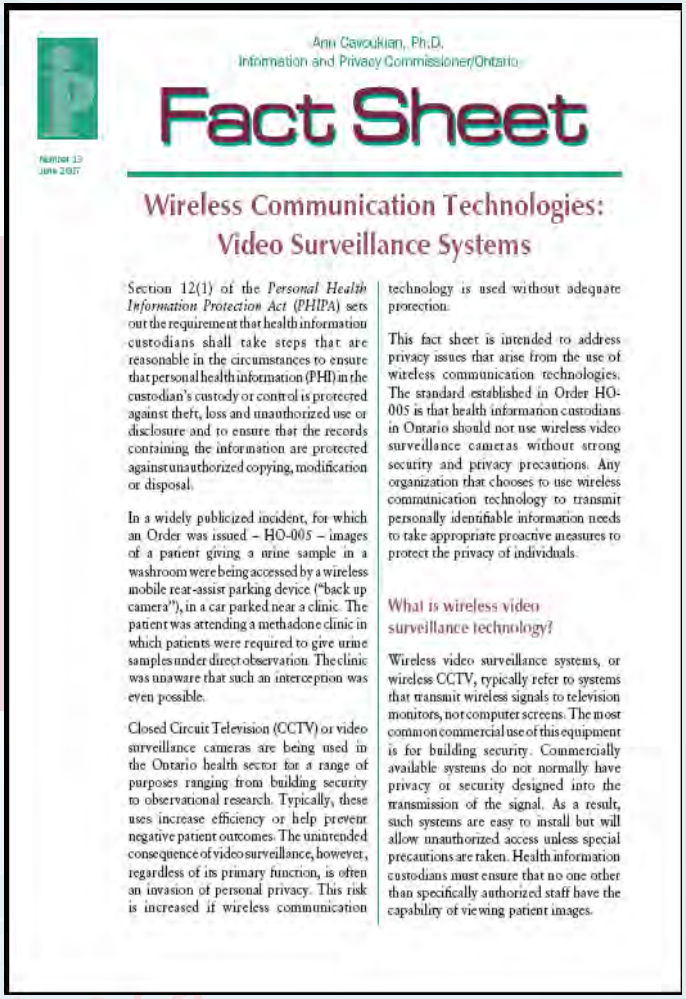
2. Wireless Communication Technology

Order HO-005
Nature of the Incident

- Received a report that a wireless mobile rear-assist parking device captured the image of an individual providing a urine sample at a methadone clinic
- The methadone clinic installed a wireless surveillance camera to monitor individuals providing urine samples
- Images are not recorded, images are only monitored in real time by a nurse working at the methadone clinic
- Consent is obtained for use of surveillance cameras

Lessons Learned From Order HO-005

- Wireless surveillance cameras should not be used to transmit personally identifiable information without strong security and privacy precautions
- Should not conduct covert surveillance
- Health information custodians should:
  - Conduct privacy impact assessments and annual security and privacy audits
  - Ensure privacy and security requirements are explicit in the procurement process
  - Ensure the vendor selection process requires signal protection
  - Ensure the surveillance camera is off except when used for designated purposes
  - Post visible signs to advise patients of the existence of the surveillance cameras



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.

3. Mobile and Portable Devices

Mobile Devices in Health Care

- Mobile applications are revolutionizing health care;
- Server-based applications designed to run on smartphones and tablets are allowing providers to access PHI at little cost, at any time, and from any location, and to share this information with others around the world;
- Mobile applications will bring health care to remote locations, avert medical emergencies, reduce hospitalization, and save lives.

Examples of Smart Phone Applications

- A smartphone radiology product, developed by a Calgary-based company, has been approved for primary diagnostic use in Canada;
- In a UHN trial, at-home heart failure patients received handheld electrocardiogram devices that fed data to a smartphone which sent it to the hospital, where it was monitored by an algorithm that alerted a cardiologist if necessary;
- A smartphone application is being used in the U.S. to provide patients with direct access to laboratory test results;
- A smartphone application is being used in California to recruit citizens trained in CPR to provide emergency care to cardiac arrest victims nearby.

Mobile and Portable Devices

The IPC has issued three orders in the context of mobile and portable devices:

Order HO-004

- Theft of a laptop containing the unencrypted personal health information of 2,900 individuals

Order HO-007

- Loss of a USB memory stick containing the unencrypted personal health information of 83,524 individuals

Order HO-008

- Theft of a laptop containing the unencrypted personal health information of 20,000 individuals

Lessons Learned From Orders HO-004, HO-007 and HO-008

- Do not retain personal health information on such devices unless necessary for the purpose
- Consider alternatives to retaining personal health information on a mobile or portable device like:
  - •Retaining de-identified information on the device,
  - •Retaining encoded information on the device and storing the code to unlock the identifying information separately on a secure computing device, or
  - •Retaining personal health information on a secure server and accessing the information remotely through a secure connection or virtual private network

STOP. THINK. PROTECT.

Patient Privacy is in Your Hands.

As health care practitioners, many of you are accustomed to dealing with loss. You interact with people every day who have lost their health, lost a loved one, or perhaps simply lost hope. And you are experts at helping people work through and manage that sense of loss.

But what if you, yourself, were responsible for the loss of something that a patient may never get back: their privacy?

Earlier this year, a health care professional did something seemingly well-intentioned: she placed a USB key into her purse as she left the office, planning to do some work at home. As it happened, the files in question were the records of personal health information of 763 patients.

Her purse was stolen. And all the records – unencrypted and easily read by anyone – were lost. Lost, too, was the sense of privacy of those 763 patients.

Scenarios such as this have been played out countless times all across Ontario. Indeed, in recent years, the unencrypted health information of over 100,000 patients on laptops, USB keys and other mobile computing and storage devices has been lost or stolen. It's a privacy problem of epic proportions, compromising some of the most sensitive and personal types of information possible. And it must stop.

The *Personal Health Information Protection Act* requires that you take reasonable steps to ensure that personal health information is protected against theft, loss, and unauthorized use and disclosure.

Mobile devices, such as laptops, PDAs, and USB keys, add a new layer of complexity to this task. The great advantage of these devices – portability – is also their greatest vulnerability, making them easily susceptible to loss and theft.

For that reason, personally identifiable health information should not be stored on any mobile devices unless it is absolutely necessary. And when it is, you can – and **must** – take steps to minimize the risks to privacy.

HOT ISSUES….

ELECTRONIC MEDICAL RECORDS
ELECTRONIC HEALTH RECORDS

The Promise

- Can be used in order to facilitate the provision of more efficient and effective health care thereby improving the quality of the health care provided
- Paper-based records may be incomplete because records are spread over a range of health care providers and may be difficult to read and locate
- Electronic health records can be readily accessed by all health care providers regardless of where they are located, are more complete and require less space and administrative resources to maintain.
- Can be designed to enhance privacy i.e. access controls, audit logs and user authentication

The Peril

- If privacy is not built into the design, these systems pose unique risks to the privacy of individuals and to the security of personal health information
- These systems allow for the collection, use and disclosure of massive amounts of personal health information from diverse sources at the press of a key
- May attract hackers and others with malicious intent, including health care providers who would otherwise be permitted to access these systems but who access the information for other than health care purposes
- Many high profile privacy and security breaches have arisen from improper implementation

Order HO-002
Nature of the Incident

- A patient told a hospital that her estranged husband and his girlfriend were employees and that she did not want them to know she was a patient
- Following discharge the patient became concerned, following a conversation with her estranged husband, that he was aware of her personal health information
- The complainant filed a complaint and the hospital placed a “VIP flag” on her electronic record of personal health information and ordered an audit
- The girlfriend, a nurse who was not involved in the health care of the patient, viewed the electronic record of personal health information on numerous occasions

Order HO-010
Nature of the Incident

- A patient complained to a hospital that an employee of the hospital inappropriately accessed the patient's records of personal health information
- The employee of the hospital was the former spouse of the patient's current spouse
- An audit revealed that the records of the patient were accessed by the employee on six separate occasions
- The employee was not involved in providing or assisting in providing health care to the patient

Personal Health Records

- Telus Health Space, smartphone applications
- Allows patients to integrate their own personal health information
- Can help patients to manage their own health care
- Allow patients to provide health care providers with access
- Unless these are directly link to EMRs, lack of interoperability results in information having to be inputted manually

Patient Portals

- Can provide educational resources about diseases and conditions
- Can provide information about health care services provided
- Can provide individual with access to their own personal health information
- Can provide tools to help patients track and manage their own health and wellbeing
- Can allow patients to interact with their health care providers directly (e.g., appointment scheduling)

Privacy Risks PHRs and Portals

- PHR users must ensure the privacy and security of their own information (e.g., strong passwords, firewalls, antivirus protection)
- User agreements may be complex and may lack transparency
- Patients can provide access to third parties
- Third party service providers could access the information for unintended purposes
- Third party service providers may not be bound by standards equivalent to health professional standards and may fall outside the scope of health privacy legislation

HOT ISSUES….

SOCIAL MEDIA

E-mail Risks

Disclosures of personal health information:

- Sending the document to the wrong email address (e.g., email address is automatically filled in).
- Email sent to multiple individuals instead of blind copying to protect email addresses and individual identities.
- Document sent to the correct email address but viewed by an unintended recipient.
- The emailed document is forwarded to other individuals who do not need to know the information.
- The email address of the intended recipient has changed or the intended recipient is no longer using the email address.

E-mail Benefits

- E-mail can also be helpful!
  - Scheduling
  - Patient reporting
  - Follow-up advice
  - Informative links
- Must ensure proper safeguards are in place, including secure e-mail and encryption.

E-mail Considerations

- Regular email is not a secure means of communication and may be vulnerable to interception by unauthorized third parties.
- Unless physicians have access to a secure e-mail service offering strong encryption, they should avoid using e-mail to communicate personal health information.
- The e-mail service must meet *PHIPA* requirements, including security requirements and patients should have knowledge, consent and control over e-mail use.
- Even if patients may be willing to accept the risks associated with communicating with their physician via e-mail, this does not alleviate physicians of their duty to take steps that are reasonable in the circumstances to safeguard personal health information in their custody and control.

Social Media (Facebook, Twitter, etc.)

- Health care providers may breach their duty to protect patient confidentiality and privacy
- Password protected sites may give users a false sense of security that they're in an exclusive environment.
- Loss of control over the information you share online.
  - Who's operating the platform and what are they able to see?
  - Do Facebook, Google or Twitter view, analyze or archive your communications on their platform?
- Even where information posted about patients may appear to be de-identified, others may be able to identify the patient through other information

Workplace Blogging

- Blogs may be a great tool for education and collaboration in the workplace, but may pose a threat to patient privacy in health care settings.
- Online discussions pertaining to unusual medical conditions or patients with unique characteristics (e.g., an unusual occupation) may result in identifying patients and/or inadvertent disclosure of personal health information.

Telemedicine

- Has the potential to bring care to individuals in remote locations
- Any communication of personal health information must occur over secure means (Skype does not provide a secure means of communicating – refer to user agreement and privacy policy)
- The Ontario Telemedicine Network provides a secure means of communication between patients and their health care providers – the patient has to go to one of their locations for an appointment.

How to Contact Us

Debra Grant, Ph.D.

Senior Health Privacy Specialist

Office of the Information & 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

E-mail: debra.grant@ipc.on.ca