Privacy Best Practices: Lessons from the world of *PHIPA* and *FIPPA/MFIPPA*

April 5, 2017

Brendan Gray, Health Law Counsel

Office of the Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

DISCLAIMER

THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES AND IS NOT LEGAL ADVICE

The Three *Acts*

IPC oversees compliance with:

- *Freedom of Information and Protection of Privacy Act* (***FIPPA***)
- *Municipal Freedom of Information and Protection of Privacy Act* (***MFIPPA***)
- *Personal Health Information Protection Act* (***PHIPA***)

First PHIPA

- *PHIPA* came into force on November 1, 2004
- The majority of *PHIPA* governs "personal health information" in the custody or control of:
  - "Health Information Custodians," or
  - "Agents" of health information custodians
- However, the *Act* also has broader application
- For example it contains restrictions on the use and disclosure of personal health information by non-health information custodians that receive personal health information from health information custodians

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.*

- PHIPA is a consent based statute.

- These duties generally fall into four categories:
  - Collection, use and disclosure of personal health information
  - Security of personal health information
  - Responding to requests for access to and correction of records of personal health information
  - Transparency of information practices

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

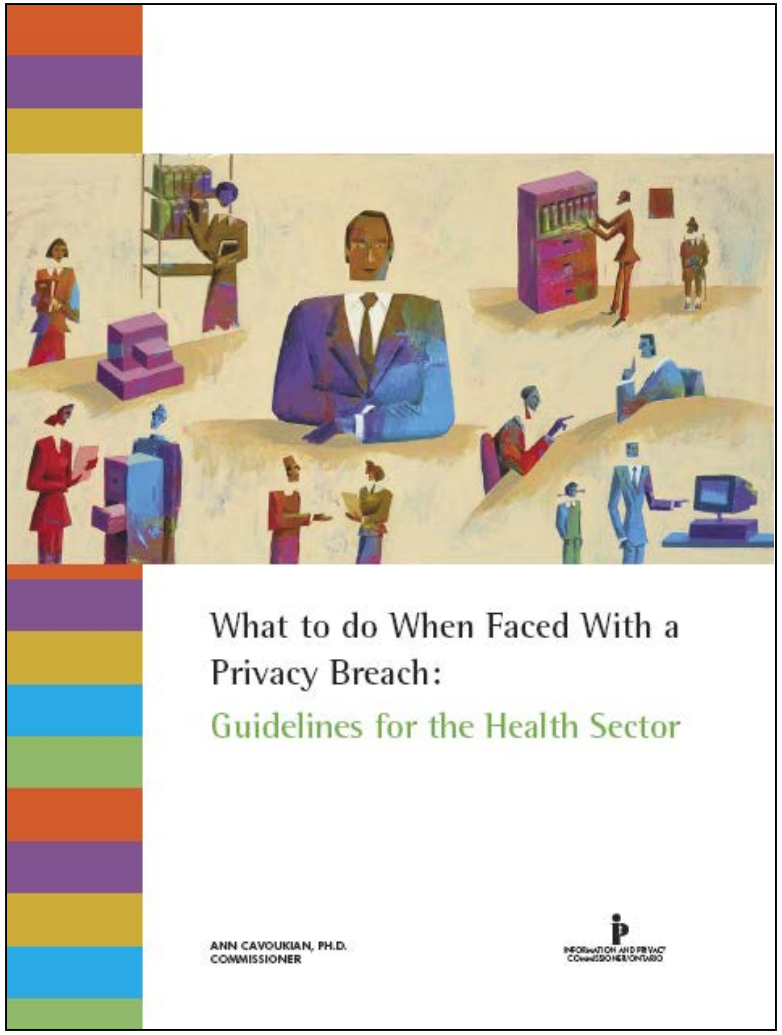
- Not permitted to collect, use or disclose more personal health information than reasonably necessary

- 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

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 used or disclosed without authority

Develop and Implement a Privacy Breach Management Protocol



Responding to a Privacy Breach

STEP 1: IMMEDIATELY IMPLEMENT PRIVACY BREACH PROTOCOL

- Notify all relevant staff of the breach
- Develop and execute a plan designed to contain the breach and notify those affected
- Recommended that you contact the IPC and provide our office with details of what happened

Responding to a Privacy Breach

STEP 2: STOP AND CONTAIN THE BREACH

- Identify the scope of the breach and take the necessary steps to contain it, including:
  - Retrieve and secure any personal health information that has been disclosed
  - Ensure that no copies of the personal health information have been made or retained by the individual who was not authorized to receive the information
  - Determine whether the privacy breach would allow unauthorized access to any other personal health information and take the necessary steps, such as changing passwords, identification numbers and/or temporarily shutting your system down

Responding to a Privacy Breach

STEP 3: NOTIFY THOSE AFFECTED BY THE BREACH

- You must take the necessary steps to notify those individuals whose privacy was breached at the first reasonable opportunity
- *PHIPA* does not specify the manner in which notification must be carried out. There are numerous factors that may need to be taken into consideration when deciding on the best form of notification
- When notifying individuals affected by a breach:
  - Provide details of the breach to affected individuals, including the extent of the breach and what personal health information was involved
  - Advise of the steps you are taking to address the breach and that they are entitled to make a complaint to the IPC. If you have reported the breach to the IPC, advise them of this fact
  - Provide contact information for someone within your organization who can provide additional information and assistance

Responding to a Privacy Breach

- STEP 4: INVESTIGATION AND REMEDIATION
  - You will be expected to conduct an internal investigation, including:
    - Ensuring that the immediate requirements of containment and notification have been met.
    - Reviewing the circumstances surrounding the breach.
    - Reviewing the adequacy of your existing policies and procedures in protecting personal health information.
    - Ensuring all staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of *PHIPA*.

Potential Causes of Privacy Breaches

Increased Portability of Personal Health Information Orders HO-004, HO-007 and HO-008

Our office has issued three orders involving personal health information on 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 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

How to Reduce the Risk….

- **STOP** and ask "Do I really need to store personal health information on this device?"
- **THINK** about the alternatives:
  - Would de-identified or coded information serve the purpose?
  - Could the information instead be accessed remotely through a secure connection or virtual private network?
- If you need to retain it on such a device, **PROTECT** it by:
  - Ensuring it is encrypted and protected with strong passwords
  - Retaining the least amount of personal health information
  - Developing policies and procedures, train and audit compliance

Unauthorized Access
Orders HO-002, HO-010 and HO-013

Our office has issued three orders involving unauthorized access:

Order HO-002

- A registered nurse accessed records of the estranged spouse of her boyfriend to whom she was not providing care
- They were accessed over six-weeks during divorce proceedings

Order HO-010

- A diagnostic imaging technologist accessed records of the current spouse of her former spouse to whom she was not providing care
- They were accessed on six occasions over nine months

Order HO-013

- Two employees accessed records to market and sell RESPs

How to Reduce the Risk…

- Clearly articulate the purposes for which employees, staff and other agents may access personal health information
- Provide ongoing training and use multiple means of raising awareness such as:
  - Confidentiality and end-user agreements
  - Privacy notices and privacy warning flags
- Immediately terminate access pending an investigation
- Implement appropriate access controls and data minimization
- Log, audit and monitor access to personal health information
- Impose appropriate discipline for unauthorized access

Secure Disposal of Records - 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

Number 10
December 2005

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

Fact Sheet

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

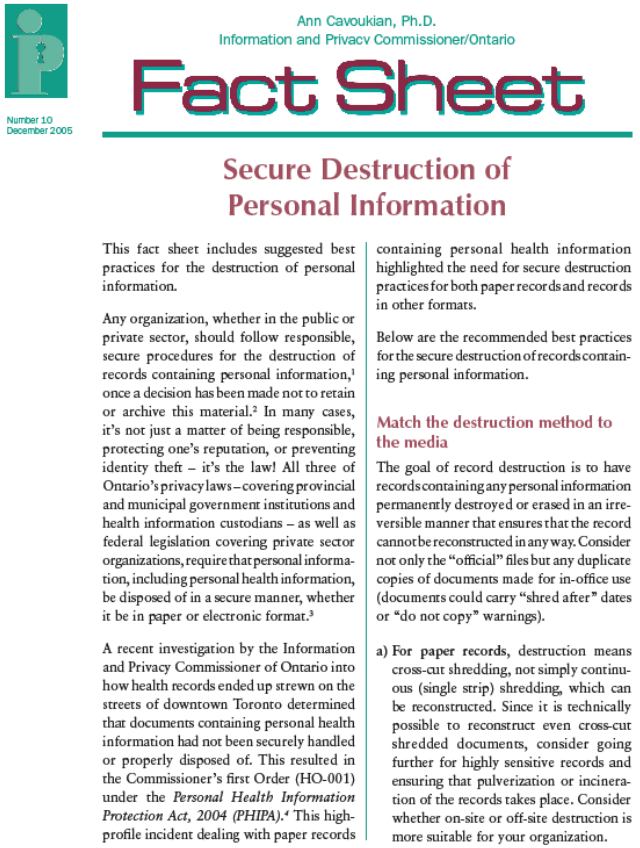
The goal of record destruction is to have records containing any personal information permanently destroyed or erased in an irreversible manner that ensures that the record cannot be reconstructed in any way. Consider not only the "official" files but any duplicate copies of documents made for in-office 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



Number 10
December 2005

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

Fact Sheet

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.

FIPPA/MFIPPA

- FIPPA/MFIPPA provide a right of access to records in the custody or control of an institution, subject to exemptions/exclusions.

- FIPPA/MFIPPA also
  - Address issues related to the collection, use and disclosure of personal information
  - Provide a mechanism for people to access copies of their own person information held by the government

What is “personal information”

- These restrictions only apply to “personal information”
- Definition of “personal information” “means recorded information about an identifiable individual including”
  - *FIPPA/MFIPPA* provide a non-exhaustive list of examples from
    - (a) race, religion, age, sex, sexual orientation or family status
    - (b) education, medical, criminal or employment history or information relating to financial transactions in which the individual has been involved
    - (c) any identifying number or symbol assigned to individual
    - (d) address, telephone number, fingerprints or blood type
    - (e) the personal opinions or views of the individual

What is NOT personal information

- Business information is not personal information
- Section 2(2.1) of *FIPPA*(*MFIPPA)*

  "Personal information does not include the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity"
- Section 2(2.2) of *FIPPA*/*MFIPPA*

  "For greater certainty, subsection (2.1) applies even if an individual carries out business, professional or official responsibilities from their dwelling and the contact information for the individual relates to that dwelling."

Collecting Personal Information

- *FIPPA/MFIPPA* prohibit the collection of personal information unless the collection is:
  - expressly authorized by statute;
  - used for the purposes of law enforcement; or
  - necessary to the proper administration of a lawfully authorized activity
- Consent does not matter
  - cannot collect personal information that does not meet one of the above criteria
- Sensitivity of the personal information is irrelevant

Collecting Personal Information – Direct

- The general rule is that personal information should be collected directly from individual
- There are exceptions to this rule including
  - consent
  - the Commissioner has authorized the manner of collection
  - report from a reporting agency in accordance with the *Consumer Reporting Act*
  - possible court or quasi-judicial proceedings
  - for purpose of law enforcement
- See IPC Practices No. 14: The Indirect Collection of Personal Information

Collecting Personal Information - Notice

- *FIPPA/MFIPPA* require that individuals be notified when their personal information is collected
  - This applies whether the institution is collecting information directly or by indirect means
- *FIPPA/MFIPPA* require that a notice contain the following elements
  - the legal authority for the collection;
  - the principal purpose(s) for which the personal information is intended to be used; and
  - the title, business address and business telephone number of a public official who can answer the individual's questions about the collection
- There are limited exceptions to the notification requirement.

Using Personal Information

- *FIPPA/MFIPPA* impose limits on the use of personal information once collected
- Can only use personal information:
  - for the purpose for which it was obtained
  - on consent
  - for the purpose for which the information may be disclosed to the institution under section 32 of *MFIPPA* or section 42 of *FIPPA*

Disclosing Personal Information

- *FIPPA/MFIPPA* prohibit disclosure of personal information except in certain circumstances
  - consent
  - consistent purpose
  - disclosure to other employees, officers or agents of institution
  - compliance with other Acts
  - to a law enforcement agency in aid of an investigation