PRIVACY BREACHES AND WORKING WITH THE IPC

AdvantAge Ontario Privacy Webinar Series

August 23, 2017

Manuela Di Re

Director of Legal Services and General Counsel

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Common Causes of Privacy Breaches

1. Insecure Disposal of Records

Common Examples

- Records of personal health information in paper format that are intended for shredding, are recycled
- Insecure disposal of records of personal health information in electronic format
- Abandoning records of personal health information when there is a change in practice

Order HO-001

- A medical clinic retained a company to shred records of personal health information dating between 1992 -1994
- Due to a misunderstanding, these records were transported to a recycling company instead of being shred
- The recycling company sold the records to a special effects company and were used in a film shoot

Film shoot uses real medical records

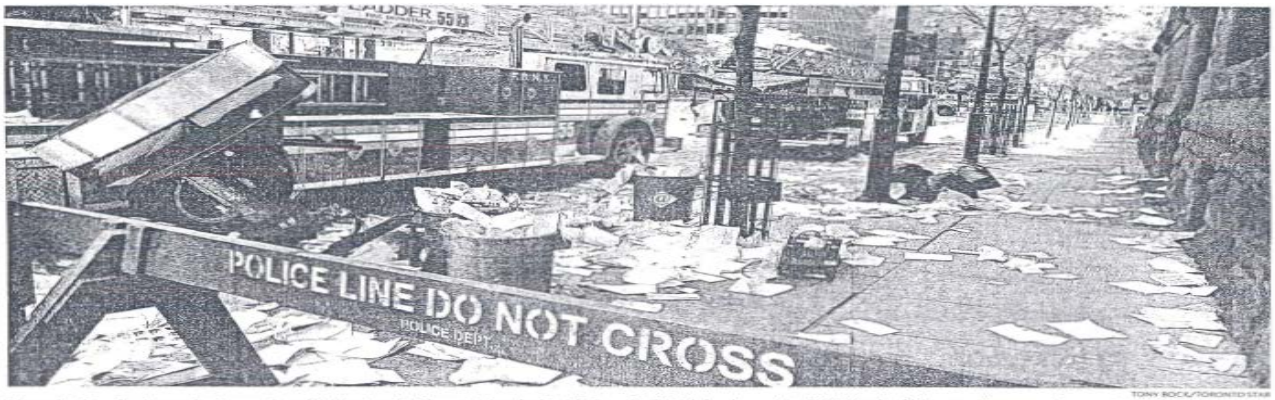
Privacy official has plans to investigate

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-



TONY ROCK/TORONTO STAR

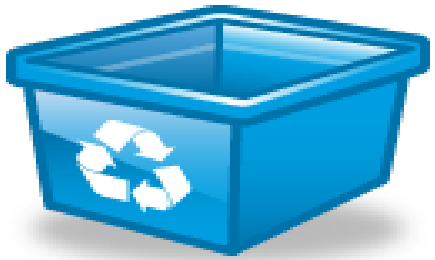
Mounds of medical records strewn along Wellington St. W. yesterday during filming of a TV miniseries on the 9/11 attacks. Below, an ultrasound report picked from the pile.

Order HO-003

- A Medical and Rehab Centre closed and left behind records of personal health information
- The landlord asked the Centre if it wanted to claim property on the premises, but received no response
- The landlord required the immediate removal of the records due to impending renovations
- The Centre said it “thought a notice may have been posted notifying patients of the closure, but it was not sure.”

Order HO-006

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



How to Reduce the Risk…
Ensure Full Life Cycle Protection

- Ensure records of personal health information are disposed of so that reconstruction is not reasonably foreseeable
- For paper records – use cross-cut shredding and if particularly sensitive, pulverization or incineration should be considered
- For electronic records – physically damage and discard the media or if re-use is preferred, use wiping utilities
- Plan for a change in practice:
  - Enter into an agreement identifying the obligations of practitioners in relation to the records
  - Arrange for secure retention of the records
  - Notify individuals of a change in practice

2. Mobile and Portable Devices

Common Examples

- Records of personal health information transferred on unencrypted:
  - Laptops
  - USBs
  - Personal digital assistants (PDAs)
  - Other portable and mobile devices

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, THINK, PROTECT

- **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

3. Unauthorized Access

Meaning of Unauthorized Access

- Unauthorized access is when you view, handle or deal with personal health information without consent and for purposes not permitted by the custodian or the *Personal Health Information Protection Act* (*PHIPA*), for example:
  - When you are not providing or assisting in the provision of health care to the individual; and
  - When it is not necessary for the purposes of exercising your employment, contractual or other responsibilities
- The act of viewing personal health information on its own, without any further action, is an unauthorized access

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

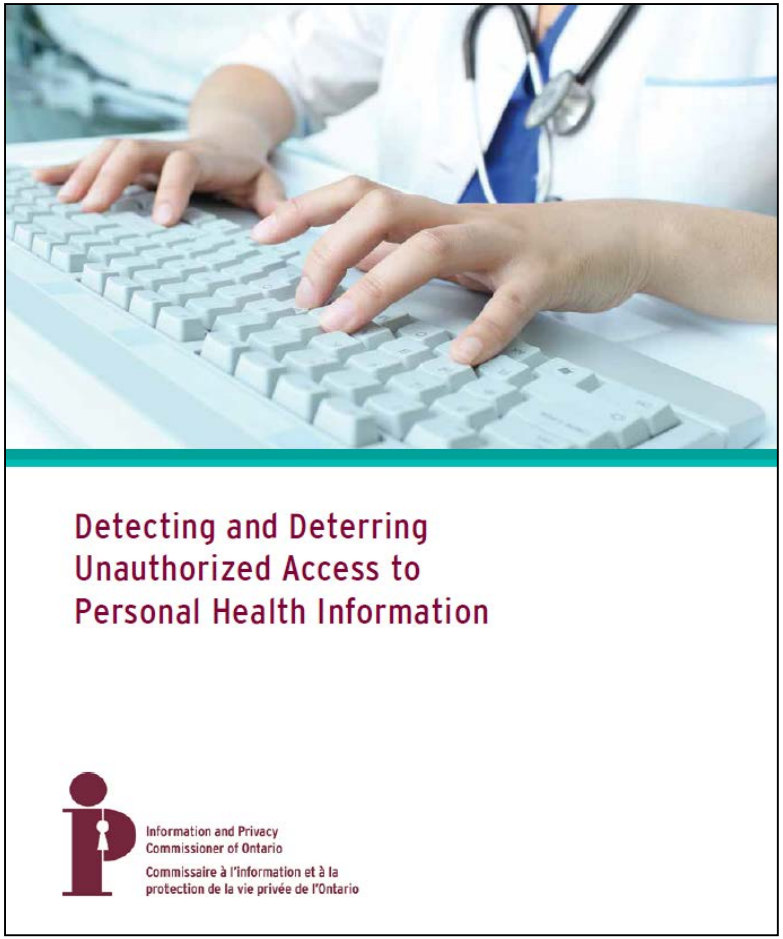
Our office has issued three orders involving unauthorized access:

- **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

Guidance Document:
Detecting and Deterring Unauthorized Access



Potential Consequences of Privacy Breaches

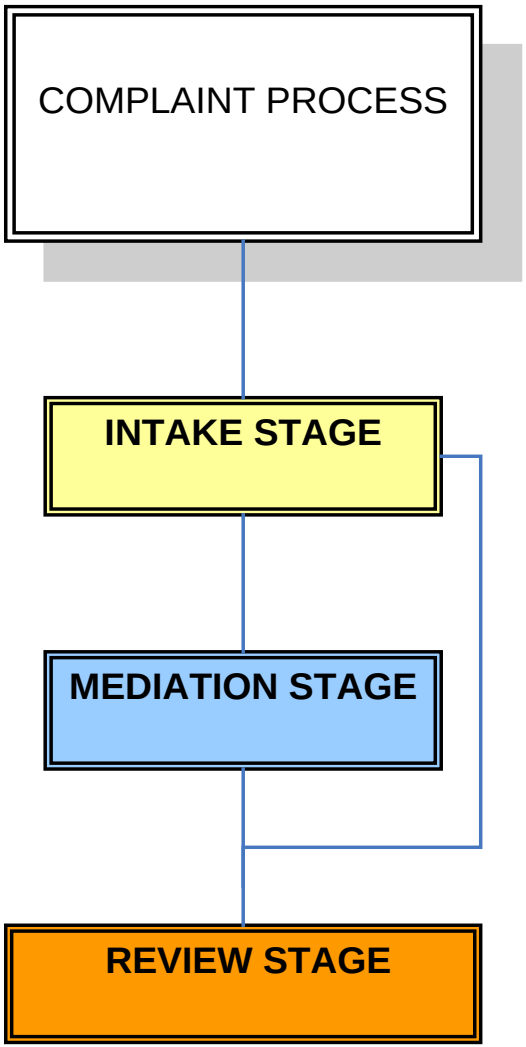
Potential Consequences to Health Care Providers

- Review by the Information and Privacy Commissioner (IPC)
- Prosecution for offences
- Statutory or common law actions
- Discipline by employers
- Discipline by regulatory bodies

1. Review by the IPC

Role of the IPC

- The IPC has oversight responsibility for *PHIPA*
- This includes receiving and responding to complaints, undertaking investigations and issuing orders
- May conduct an investigation where:
  - A written complaint has been received
  - In the absence of complaint, where there are reasonable grounds to believe *PHIPA* has or is about to be contravened


COMPLAINT PROCESS
INTAKE STAGE
MEDIATION STAGE
REVIEW STAGE

Stages of Process

Intake

- An analyst typically contacts the parties to obtain and clarify information, explain the process and ensure the matter falls within our jurisdiction
- At the end of intake, the matter may be resolved informally, may be closed, or may be sent to investigation/mediation or directly to adjudication
- If a matter is closed, a letter is sent to the parties explaining the reasons
- The letter closing the matter is not published

Investigation/Mediation

- A mediator is assigned to try to resolve or simplify the matters at issue
- At the end of mediation, the matter may be resolved with the agreement of the parties or may be sent to adjudication
- Where the matter is resolved, a letter is sent to the parties confirming the resolution. Where the matter is sent to adjudication, a report is sent to the parties outlining the facts gathered and the issues in dispute
- The letter and report are not published

Stages of Complaint Process

Adjudication

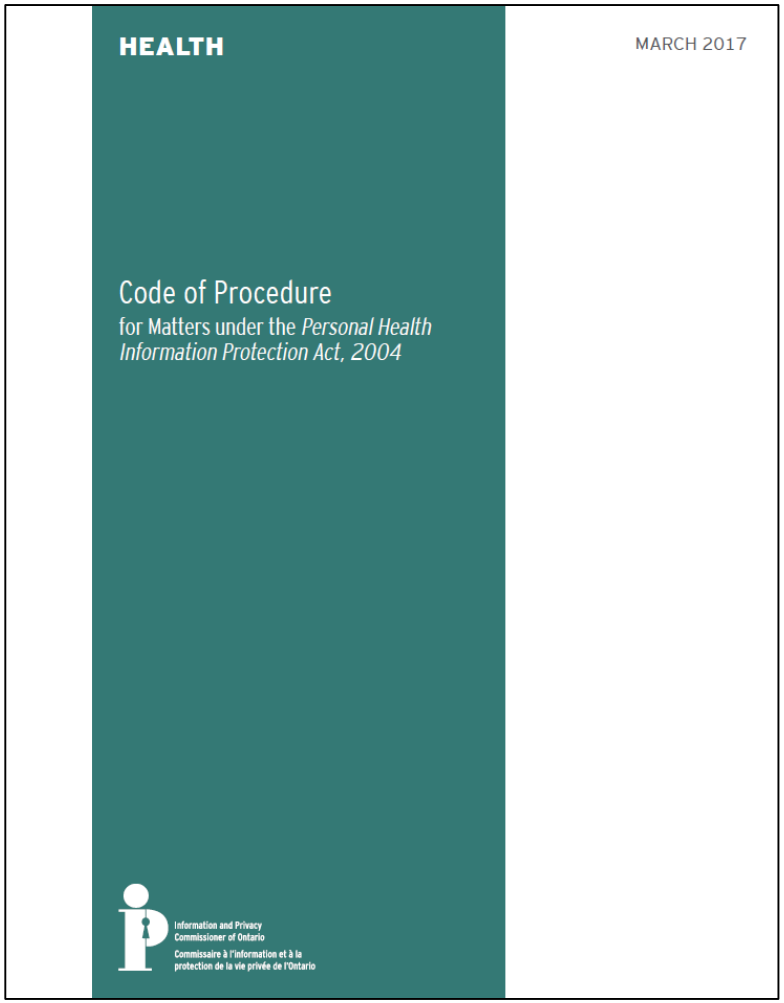
- An adjudicator determines whether there are reasonable grounds to commence a review under *PHIPA*
- If there are no reasonable grounds to commence a review, the matter is closed and a public decision is prepared
- If there are reasonable grounds to commence a review, the adjudicator:
  - Issues a Notice of Review
  - Seeks representations on the facts and issues in dispute
  - Decides whether or not to issue an order
  - Publishes a decision

Order- Making Power

- The IPC has broad order-making powers under *PHIPA*
- An order may include comments or recommendations
- On making an order, the IPC is required to provide a copy to the body legally entitled to review the activities of the health information custodian
- A final order may be filed with the court and on filing is enforceable as an order of the court

New Code of Procedure

- The new code is the result of an internal review of the IPC's processes under *PHIPA*
- Came into force on March 15, 2017, and applies immediately to all files under *PHIPA*
- Replaces the previous code of procedure for access/correction complaints
- There is now a single code applicable to all matters arising under *PHIPA*
- New practice directions will provide guidance to parties exercising their rights and complying with their obligations under this new code and *PHIPA*



2. Prosecution

Offences

- It is an offence to wilfully collect, use or disclose personal health information in contravention of *PHIPA*
- Consent of the Attorney General is required to commence a prosecution for offences under *PHIPA*
- On conviction, an individual may be liable to a fine of up to $100,000 and a corporation of up to $500,000

Referrals for Prosecution

- To date, six individuals have been referred for prosecution:
  - **2011**– A nurse at the North Bay Health Centre
  - **2015**– Two radiation therapists at the University Health Network
  - **2015** – A social worker at a family health team
  - **2016** – A registration clerk at a regional hospital
  - **2016**– A regulated professional at a Toronto hospital

Successful Prosecutions – Two Radiation Therapists

- The two radiation therapists charged with wilfully collecting, using or disclosing personal health information in contravention of *PHIPA* pled guilty
- Each radiation therapist was ordered to pay a $2,000 fine and to pay a $500 victim surcharge
- These were the first successful prosecutions under *PHIPA*

Successful Prosecutions – Registration Clerk

- The registration clerk charged with one count of willfully collecting, using or disclosing personal health information in contravention of *PHIPA* pled guilty
- The registration clerk was ordered to pay a $10,000 fine and to pay a $2,500 victim surcharge

Most Recent Prosecution

- The Masters of Social Work student on an educational placement with a family health team pled guilty to willfully accessing the personal health information of five individuals
- As part of her plea, she agreed she accessed the information of 139 individuals without authorization between September 2014 and March 2015
- She was ordered to pay a $20,000 fine and to pay a $5,000 victim surcharge
- This is the highest fine to date for a health privacy breach in Canada

3. Statutory or Common Law Actions

Statutory or Common Law Actions

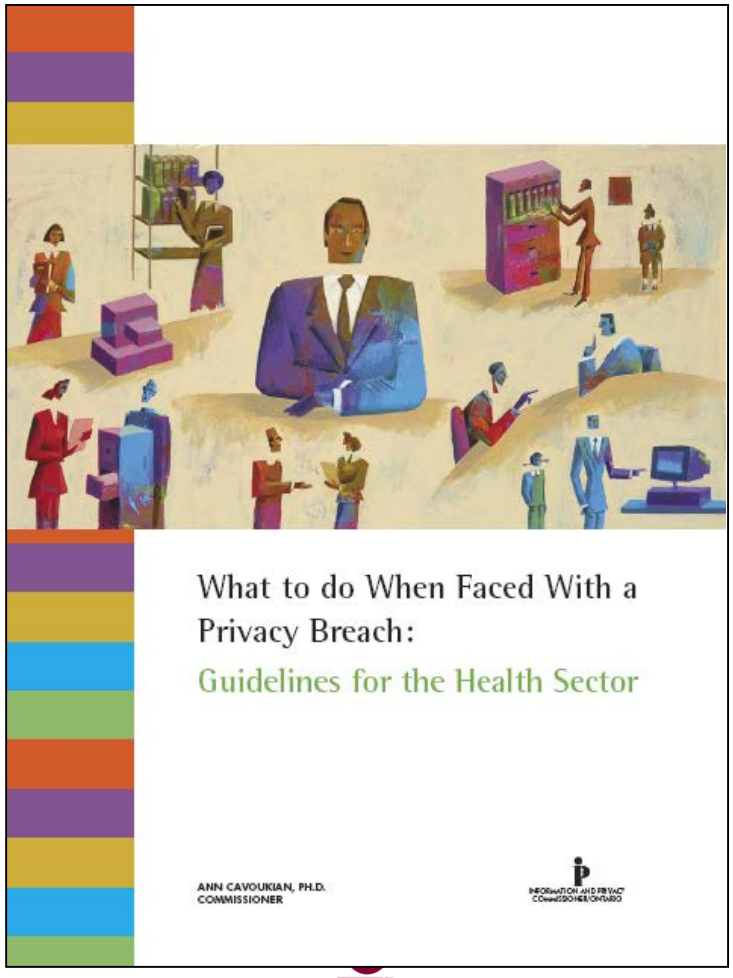
- A person affected by a final order of the IPC or by conduct that gave rise to a final conviction for an offence may start a proceeding for damages for actual harm suffered
- Where the harm was caused wilfully or recklessly, the court may award an amount not exceeding $10 000 for mental anguish
- In 2012, the Ontario Court of Appeal recognized a common law cause of action in tort for invasion of privacy

Planning for a Privacy Breach

Develop and Implement A Privacy Breach Management Policy and Procedure

The policy and procedure should:

- Require agents to notify the health information custodian of a privacy breach or suspected privacy breach
- Identify the person responsible and the procedure to be followed in notifying individuals and managing a breach
- Clarify responsibilities for containing, investigating and remediating a breach
- Outline the procedure to be followed in containing, investigating and remediating a breach



What to do in the Event of a Privacy Breach

Implementation, Identification and Containment

- Implement the privacy breach management policy
- Determine whether a privacy breach has occurred
- Identify the personal health information compromised
- Notify senior management of the privacy breach
- Implement containment measures to ensure personal health information is protected from further theft, loss or unauthorized use or disclosure, for example:
  - Ensure no copies of the records have been made
  - Ensure the records are either retrieved or disposed of securely
  - Obtain confirmation that the records were securely disposed of

Notification of Individuals

- A health information custodian must notify the individual at the first reasonable opportunity if personal health information is stolen, lost or used or disclosed without authority

- In the provincial electronic health record, the custodian must also notify the individual at the first reasonable opportunity if personal health information is collected without authority

- The notification should at minimum advise individuals of:
  - The nature and extent of the privacy breach
  - The nature and extent of the personal health information in issue
  - The measures taken to contain the privacy breach
  - Any further actions that will be undertaken to contain, investigate and remediate the privacy breach

Notification of the IPC

- A health information custodian must also notify the IPC of a theft, loss or unauthorized collection, use or disclosure in the circumstances set out in section 6.3 of the Regulation to *PHIPA*

- These circumstances include where:
  - The custodian has reasonable grounds to believe that:
    - The person knew or ought to have known they were using or disclosing personal health information without authority;
    - The personal health information was stolen;
    - After the initial loss or unauthorized use or disclosure, the personal health information was or will be further used or disclosed without authority;
  - The loss or unauthorized use or disclosure is part of a pattern of similar losses or unauthorized uses or disclosures;

Notification of the IPC

- The custodian is required to give notice to a health regulatory college of an event described in section 17.1 of *PHIPA;*
- The custodian would be required to give notice to a health regulatory college of an event described in section 17.1 of *PHIPA* if the agent of custodian were a member of the college;
- The custodian determines the loss or unauthorized use or disclosure is significant after considering relevant circumstances, like:
  - The sensitivity of the personal health information;
  - Whether the loss or unauthorized use or disclosure involved a large volume of personal health information;
  - Whether the loss or unauthorized use or disclosure involved many individuals' personal health information;
  - Whether more than one custodian or agent was responsible.

Investigation and Remediation

- Conduct an investigation in order to:
  - Review the containment measures implemented
  - Determine whether the breach has been effectively contained
  - Ensure notification has been provided to affected individuals
  - Ensure notification has been provided to the IPC, if applicable
  - Review the circumstances surrounding the privacy breach
  - Review the adequacy of existing policies and procedures
  - Develop recommendations to prevent similar future breaches
- Document the investigation, any recommendations and the persons responsible for implementation
- Implement the recommendations to prevent similar breaches in the future

Recent Amendments to PHIPA

Bill 119

- Bill 119, the *Health Information Protection Act, 2016,* was introduced on September 16, 2015
- It amends *PHIPA*, including by introducing Part V.1 related to the provincial electronic health record (provincial EHR)
- All provisions were proclaimed into force on June 3, 2016, with the exception of those related to the provincial EHR

Governance Model

- No custodian will have sole custody or control of PHI in the provincial EHR – it will be shared
- A custodian will only have custody or control of PHI if it:
  - creates and contributes to the provincial EHR, and
  - collects from the provincial EHR
- An advisory committee will be established to make recommendations to the Minister
- The Minister will establish membership of the committee, its terms of reference, organization and governance

Responsibility for Developing and Maintaining the Electronic Health Record

- The provincial EHR will be developed and maintained by one or more prescribed organizations
- The prescribed organization(s) will be required to comply with certain requirements, including:
  - Logging, auditing and monitoring instances where PHI is viewed, handled or otherwise dealt with
  - Logging, auditing and monitoring instances where consent directives are made, withdrawn, modified and overridden
  - Having and complying with practices and procedures that are approved by the IPC every three years

Collection, Use and Disclosure

- In general, custodians will only be permitted to collect PHI from the provincial EHR:
  - To provide or assist in the provision of health care to the individual to whom the PHI relates, or
  - If a custodian has reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm
- If PHI is collected to provide health care, it may subsequently be used or disclosed for any purpose permitted by *PHIPA*
- If collected to prevent a significant risk of serious bodily harm, it may only be used and disclosed for this purpose
- Special definitions of collection, use and disclosure will apply

Consent Directives

- Individuals cannot opt out of having their PHI included in the provincial EHR
- Once included, however, individuals will have the right to implement consent directives
- A consent directive withholds or withdraws the consent of an individual to the collection, use or disclosure of his or her PHI for health care purposes
- Authority is provided to make regulations specifying the data elements that may not be subject to a directive

Consent Overrides

- A custodian will be permitted to override a directive:
  - With the express consent of the individual; and
  - Where there are reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm to the individual or another person but, if the risk is to the individual, it must not be reasonably possible to get timely consent
- A custodian that collects PHI subject to a directive may only use it for the purpose for which it was collected
- For example, where collected with express consent, it may only be used in accordance with the individual's consent

Notice of Consent Overrides

- Where a directive is overridden, the prescribed organization will be immediately required to provide written notice to the custodian that collected the PHI
- Upon receipt of the notice, the custodian is required to:
  - Notify the individual to whom the PHI relates at the first reasonable opportunity; and
  - Where the PHI is collected to eliminate or reduce a significant risk of serious bodily harm to a third person, provide additional written notice to the IPC

How to Contact Us

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca