PROTECTING PRIVACY IN THE DELIVERY OF HEALTH CARE

Manuela Di Re

Director of Legal Services and General Counsel
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

ALLIANCE FOR HEALTHIER COMMUNITIES

SEPTEMBER 27, 2019

Overview

- The *Connecting Care Act, 2019*
  - What the Act provides
  - Implications for the health sector
  - Implications for the *Personal Health Information Protection Act*
- Unauthorized access in the health sector
  - Meaning of unauthorized access
  - Legal and regulatory consequences of unauthorized access

CONNECTING CARE ACT

Connecting Care Act

- The *Connecting Care Act* was proclaimed into force on June 6, 2019
- It proposes to transform the health system through, among other things, the:
  - Establishment of Ontario Health
  - Creation of Ontario Health Teams
- The Minister may designate a person, entity or group as an Ontario Health Team
- Designation depends on whether they can deliver integrated and coordinated services in at least three areas identified in the Act (e.g. primary care services, mental health or addictions services, home care or community services)

Operation of Ontario Health Teams

- In the absence of amendments, Ontario Health Teams must comply with the current provisions of the *Personal Health Information Protection Act* (PHIPA)
- To assist in ensuring compliance, Ontario Health Teams should:
  - Identify all of the participants in the Ontario Health Team
  - Determine whether each participant is a health information custodian
  - Identify the purpose(s) of each collection, use and disclosure of personal health information
  - Determine whether there is authority for each collection, use and disclosure
  - If the authority is consent, determine the consent required (express/implied/assumed)
  - Be transparent with clients about the information practices
  - Develop a governance framework and harmonized policies and procedures
    - If all participants are health information custodians, are they acting as independent health information custodians or as a single health information custodian pursuant to an order of the Minister?

Collection, Use and 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 without consent
- There are three types of consent under PHIPA:
  - Express
  - Implied
  - Assumed implied

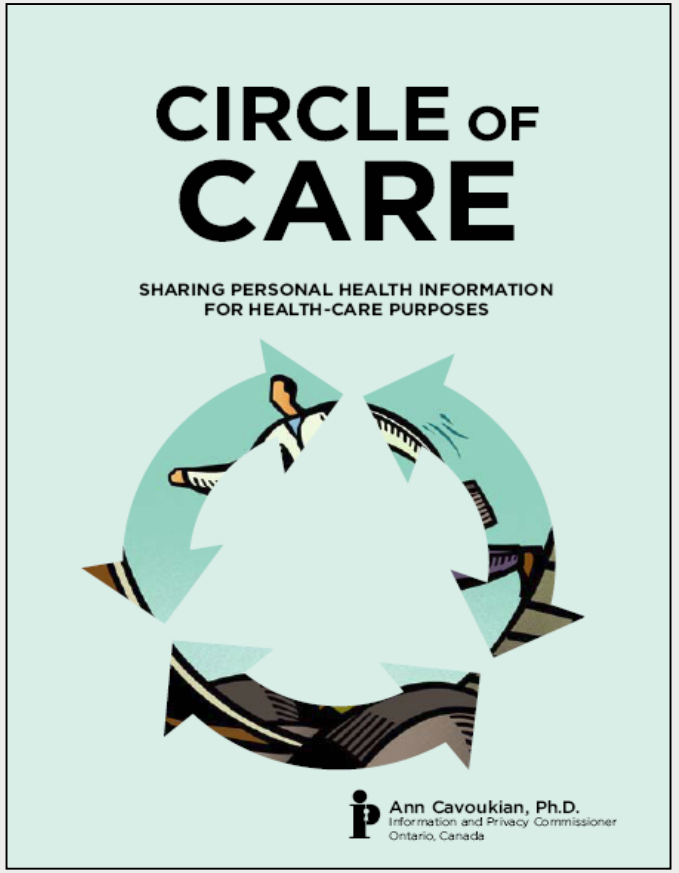
Express vs Implied Consent

- In general, express consent is required to:
  - Disclose health information to a non-health information custodian
  - Disclose health information to another custodian for a purpose other than health care
  - Collect, use or disclose health information for marketing or fundraising
- In all other circumstances, consent may be implied
- For example, consent may be implied:
  - To collect or use health information for any purpose, subject to certain exceptions
  - To disclose health information to another custodian for a health care purpose

Assumed Implied Consent

Custodians *may* assume implied consent provided all six conditions are satisfied:

1. The custodian falls within a category of custodians that are entitled to rely on assumed implied consent
2. The personal health information must have been received from the individual, his or her substitute decision-maker or another custodian
3. The personal health information must have been received for providing or assisting in providing health care to the individual
4. The purpose of the collection, use or disclosure must be for providing or assisting in providing health care to the individual
5. In the context of a disclosure, the disclosure must be to another custodian
6. The custodian must not be aware the individual expressly withheld or withdrew consent



Elements for Valid Consent

Consent must:

1. Be the consent of the individual or their substitute decision-maker (if 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

4. Not be obtained by deception or coercion.

Transparency Regarding Information Practices

Ensure that you have public facing documents that:

- Identify the Ontario Health Team (including all participating organizations)
- Describe its governance structure
- Describe the personal health information that will be collected
- Identify the purpose(s) for which the information will be collected and used
- Identify to whom and the purposes for which the information will be shared
- Describe how individuals may refuse or withdraw consent
- Describe how individuals may make requests for access or correction
- Identify the person to contact if they have questions or concerns

Harmonized Policies and Procedures

- Harmonized privacy policies and procedures should be developed to:
  - Set out the roles and responsibilities of each participating organization
  - Clarify what organization(s) are responsible for undertaking each duty and obligation under PHIPA
- Harmonized privacy policies and procedures should address such areas as:
  - Privacy training
  - Privacy assurance
  - Logging, auditing and monitoring
  - Consent management
  - Privacy breach management
  - Privacy complaints and inquiries management
  - Access and correction
  - Governance
- Content of privacy policies and procedures will depend on governance structure

UNAUTHORIZED ACCESS

Meaning of Unauthorized Access

- Unauthorized access is when you view, handle or otherwise deal with health information without consent and for purposes not permitted by PHIPA
- For example:
  - When you are not providing health care to the individual
  - When the individual has provided an express instruction
  - When it is not necessary for your employment, contractual or other responsibilities
- The act of viewing the personal health information on its own, without any further action, **is** an unauthorized access
- Unauthorized access is a serious matter, regardless of the motive

How to Address Challenges

- Implement policies that clearly set out the purposes for which access is and is not permitted
- Provide ongoing training and use multiple means of raising awareness such as:
  - Confidentiality and end-user agreements
  - Privacy notices and privacy warning flags
- Implement appropriate access controls and data minimization
- Log, audit and monitor access to health information
- Immediately terminate access pending an investigation
- Impose appropriate discipline for unauthorized access

Guidance Document

Reduce the risk through:

- ✓ Policies and procedures
- ✓ Training and awareness
- ✓ Privacy notices and warning flags
- ✓ Confidentiality and end-user agreements
- ✓ Access management
- ✓ Logging, auditing and monitoring
- ✓ Privacy breach management
- ✓ Discipline

Detecting and Deterring Unauthorized Access to Personal Health Information

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

Consequences of Unauthorized Access

- Duty to notify individuals
- Review or investigation by the Information and Privacy Commissioner (IPC)
- Prosecution
- Statutory or common law actions
- Discipline by employers
- Discipline by regulatory bodies

Duty to Notify

Notification of Individual

- A 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 it is collected without authority

Notification of the IPC

- A 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

Reviews and Investigations by the IPC

- A final order of the IPC may be filed with the court and on filing, is enforceable as an order of the court
- The IPC has issued orders involving unauthorized access, including:

HO-002

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

HO-010

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

HO-013

- Two employees accessed records to market and sell RESPs

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

Prosecutions

To date, five individuals have been successfully prosecuted:

- **2016** – two radiation therapists at a Toronto Hospital
- **2016** – a registration clerk at a regional hospital
- **2017** – a social worker at a family health team*
- **2017** – an administrative support clerk at a Toronto hospital

*The fine in this case is the highest fine to date for a health privacy breach in Canada - the social worker was ordered to pay a $20 000 fine plus a $5 000 victim surcharge

"The various victims have provided victim impact statements which are quite telling in terms of the sense of violation, the loss of trust, the loss of faith in their own health care community, and the utter disrespect [the accused] displayed towards these individuals."

"I have to take [the effect of deterrence on the accused] into consideration, but realistically, it's general deterrence, and that has to deal with every other heath care professional or someone who is governed by this piece of legislation. This is an important piece of legislation …"

- Justice of the Peace, Anna Hampson

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 called “intrusion upon seclusion”

Discipline by Regulatory Colleges

- The Masters of Social Work student prosecuted was also disciplined by the Ontario College of Social Workers and Social Service Workers in June 2017
- The member admitted and the panel found that the student committed professional misconduct, including by undermining the "trust the public has in social workers and other health care providers"
- The member was reprimanded, her certificate of registration was suspended for six months and she was required to complete an ethics course
- The member was also ordered to pay costs of $5 000 to the College

Discipline by Regulatory Colleges

- A member of the College of Physicians and Surgeons accessed health records of a colleague through the hospital electronic records system without authorization
- The relationship between the member and the colleague was deteriorating and the member questioned the well being and mental health of the colleague
- The member admitted that he engaged in professional misconduct
- The member's certificate of registration was suspended for three months and he was required to complete an individualized instruction in medical ethics
- The member was also ordered to pay costs of $5 000 to the College

Discipline by Regulatory Colleges

- A member of the College of Nurses accessed health records of a patient through the hospital electronic records system without authorization
- The patient's admission and general diagnosis were widely publicized and a privacy notice popped up when the patient's name was clicked in the system
- The member admitted her actions and claimed that she was curious about the patient's age
- The member's certificate of registration was suspended for one month and a number of terms, conditions and limitations were placed on her certificate of registration, including to notify employers of this decision for a 12 month period

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

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965