Introduction to PHIPA

Andrew Drummond

Director, Health Policy

Information and Privacy Commissioner of Ontario

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

College of Naturopaths

November 29, 2024

PHIPA – Purpose and Background

Disclaimer

Legislative Intent and Purposes

PHIPA within the broader IM legislative framework

Key concepts

Consent

Disclaimer

- IPC guidance and presentations are for informational purposes ONLY.
- We do not endorse, approve, or certify any proposal, program, service, device, or technology, and we do not confirm or provide legal advice. (Also: I'm not a lawyer!)
- What I say here today does not bind the IPC's Tribunal, which may be called upon to adjudicate the authorities under which a person or organization completes its roles and responsibilities, and whether it has complied with the obligations applicable to those roles.
- In addition, my views do not necessarily represent the views of the organization as a whole.

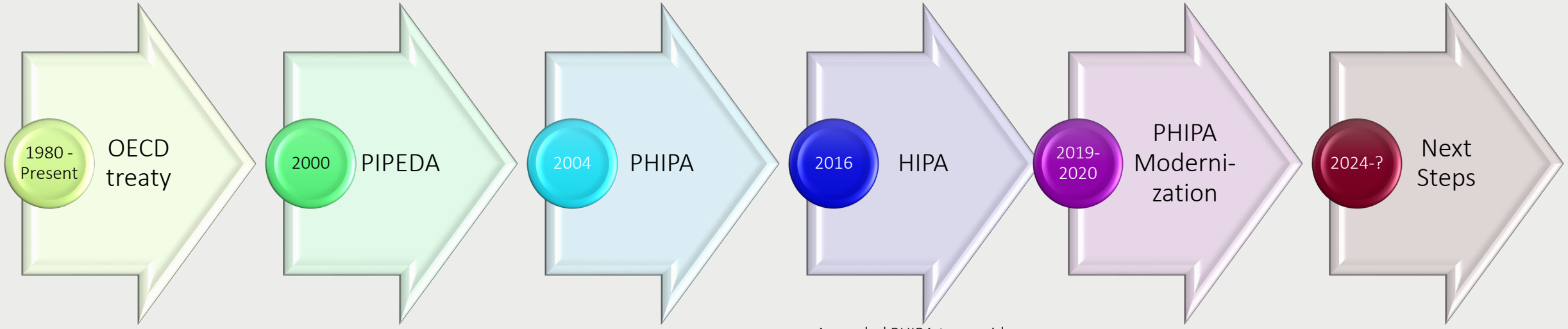
PHIPA - Purposes

- PHIPA has five stated purposes
  - I – to establish rules for collection, use and disclosure ("c/u/d") of personal health information (PHI) that protect confidentiality of the information and privacy of individuals, while facilitating the effective provision of health care;
  - II – to provide a right of access to individuals to their PHI (subject to limited exceptions)
  - III – to provide a right of correction or amendment of PHI (subject to limited exceptions)
  - IV – to provide for independent review and resolution of complaints about PHI
  - V – to provide for effective remedies for contravention of the Act.

- One of the key points of PHIPA is #1 – **which is a dual, co-equal purpose:**
  - **Protection of privacy**
  - **Facilitation of provision of care**

Ontario Benefits from a Well Established & Robust Legislative Framework for Health Information Management

Introduced in 2004, PHIPA built on best practices and leading principles for privacy protection in a health system context and it continues to be a key standard globally.



- Serves as the basis for the creation of leading practice privacy frameworks (e.g., GDPR)

- Would have required *express* consent for collections, uses, disclosures, of PHI for health care

- Met the substantially similar requirement of PIPEDA
- Supported effective delivery of health care with clear obligations and rights of patients

- Amended PHIPA to provide additional privacy protections while also enabling digital health solutions
- Enabled creation of a "Prescribed Organization" to manage the Electronic Health Record

- Numerous legislative and regulatory amendments designed to facilitate information sharing while improving security and enforcement

- Enhancing access?
- Enhancing data sharing for non-health purposes?
- AI?
- Cybersecurity?

Some Key Concepts: PHI, HIC, Consent

- Personal Health Information

  Identifying information about an individual, in oral or recorded form, if it concerns physical or mental health of that individual, relates to the provision of care, is a plan of service for home/community care, relates to payments or eligibility for health care, relates to donation of body parts or substances, is the health number, or identifies a substitute decision maker ("SDM")

  What it is NOT: aggregated information; de-identified information; separated information unrelated to health care that might be held by a provider.

  BUT: the "mixed record" rule applies: if other personal information is combined with any PHI, then it becomes part of the PHI. (e.g., your name and address, when combined with your health number)

- Health Information Custodians

  A person or organization who has custody and control ("C&C") of PHI as a result of or in connection with performing their duties, including health care providers, the Ministry (in some instances), home care SPOs, hospitals, long-term care homes, retirement homes, pharmacies, labs, etc., but including any person or organization prescribed.

  HICs do not just have rights under PHIPA; they also have obligations, some of which may be considered (by some) to be onerous.

- Consent

  PHIPA is consent-based information legislation, but there are multiple forms of consent, and there are also allowable transfers of information without consent.

  "Implied" and "assumed implied" consent allow for the c/u/d of PHI <u>for health care purposes</u> without having to ask for express consent – to enable the "dual purpose" described earlier.

More on Consent

Personal Health Information

- For consent to be valid, the consent must:
  - Be the consent of the individual or his or her substitute decision-maker (where applicable)
  - Be knowledgeable
    - It must be reasonable to believe that the individual knows the purpose of the collection, use or disclosure and that he or she may give or withhold consent
  - Relate to the information, and
  - Not be obtained by deception or coercion

- 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 PHI
- A Notice of Purposes:
  - Must be posted where it is likely to come to the attention of the individual (or provided directly to the individual)
  - Must outline the purposes for which the custodian collects, uses or discloses PHI
  - Should advise the individual that he or she has the right to give or withhold consent

Capacity to Consent

Personal Health Information

- An individual is capable of consenting to the collection, use or disclosure of their personal health information if they are able to:
  - Understand the information that is relevant to deciding whether to consent to the collection, use, or disclosure, as the case may be; and
  - Appreciate the reasonably foreseeable consequences of giving, not giving, withholding, or withdrawing the consent.
- An individual may be capable of consenting to the collection, use, or disclosure of some parts of their personal health information, but incapable of consenting with respect to other parts.
- If the individual is determined to be incapable, the following persons may act on his/her behalf (in the following order):
  - The individual's guardian of the person or guardian of property
  - The individual's attorney for personal care or attorney for property
  - The individual's representative appointed by the CCB
  - The individual's spouse or partner
  - A child or parent of the individual
  - A parent of the individual with only a right of access
  - A brother or sister; or
  - Any other relative

Assumed Implied Consent: the "Circle of Care"

- Certain health information custodians may assume implied consent to collect, use or disclose personal health information in certain 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*
- In order to rely on assumed implied consent with regard to the collection, use and disclosure of personal health information, all of the following six conditions must be met.

Six Conditions to be Satisfied to Assume Implied Consent

1. The health information custodian must fall within the category of custodians entitled to rely upon assumed implied consent
2. The personal health information in question must have been received from the individual to whom the information pertains, his/her substitute decision-maker, or another custodian;
3. The personal health information must have been received for the provision of health care to the individual;
4. The purpose of the collection, use, or disclosure must be for the purpose of providing health care to the individual to whom the information relates;
5. In the context of a disclosure, the disclosure must be to another health information custodian; and
6. The health information custodian that receives personal health information must not be aware that the individual has expressly withheld or withdrawn consent

Collection, Use, Disclosure

Direct and indirect collection

Allowable uses by health information custodians

Disclosures and limitations

Collection

- Collection of PHI can be done with consent by providers, directly, but there are also provisions where collection can be done indirectly, and there are others where collection is mandatory.
- Indirect collection can occur
  - With express consent
  - When reasonably necessary for care and not reasonably possible to collect directly
  - When part of a FIPPA institution and it's necessary for investigating possible law violations, for proceedings, or the statutory function of the custodian
  - For the purposes of carrying out approved research
  - For Prescribed Entities ("PEs" – to be discussed later) under s. 45(1)
  - Commissioner says it's OK
  - Required by law/treaty/agreement/arrangement under law
  - Subject to arrangements under such laws, etc.
- It's also possible to collect information directly for health care purposes even if the person is not capable of consenting, if the collection is reasonably necessary for health care and it's not reasonably possible to obtain the information in a timely manner.
- Also, collection is involuntary for certain elements of administration of the health system (e.g., the health number, by the ministry, for the purposes of payment, etc.)

Use

- Allowable uses of PHI are described in s. 37 of PHIPA.
- These uses are allowed once a custodian has legally collected the information, and really underpin a lot of how the value of PHI is unlocked.
    - For the purposes of what it was collected for, but not if it was collected with consent and the individual requests otherwise
    - For a purpose under law that requires someone else to disclose it to the HIC
    - For planning or delivering programs either provided or funded by the HIC, or allocation of resources, evaluating those programs/services, detecting, monitoring, or preventing fraud or unauthorized receipt of services or benefits related to any of them.
    - Risk or error management, or quality improvement
    - Education of agents to provide health care
    - For the purposes of seeking consent about something, when limited to contact information to seek that consent.
    - Proceedings or contemplated proceedings
    - Obtaining payments, or processing, monitoring, verifying, or reimbursing claims for payment for health care provision or related goods and services
    - For research conducted by the custodian (unless otherwise not allowed)
    - If permitted or required under another law (subject to prescribed requirements and restrictions (if any)

Disclosure

- Unlike the collection and use provisions, the disclosure provisions are considerably more expansive, and are covered from s.38 to s. 50.
- Disclosures are permitted to a wide variety of individuals and groups for a wide variety of possible purposes:
  - For health care
  - For health or other programs (including to Prescribed Registries (“PRs”))
  - Related to risks
  - For proceedings
  - To a successor (including to archives)
  - Related to PHIPA or other Acts
  - For research
  - For planning and management of the health system (i.e., to prescribed entities)
  - For health payments (mandatory disclosure)
  - For analysis of the health system
  - With the Commissioner’s approval
  - Outside Ontario

Segue: a couple of points

- The "data minimization" principle applies to all disclosures
  - That is, a HIC should not disclose more information than is required for the purposes.
- Disclosures are mostly voluntary
  - There are exceptions (e.g., s. 46) but there is not a requirement to disclose in most cases
- Some disclosures can be made without consent
  - E.g., to PRs and PEs
- Disclosure for research requires additional scrutiny
  - The researcher must submit a request in writing; have a research plan that sets out the affiliation of each person involved in the research, the nature and objectives of the research, as well as its anticipated public or scientific benefit, and all other prescribed issues; and submit a copy of its REB approval.
  - The REB has to consider whether the research objectives could be met without the PHI, whether there are adequate safeguards in place, whether the public interest is met, and whether obtaining the consent of the individuals' PHI is impractical.
  - A research agreement between the discloser and the researcher is required.

Requests For Access

Right of Access

- In general, individuals have a right of access to records of personal health information about themselves that are in the custody or under the control of a health information custodian, with some exceptions such as:
  - The record is subject to legal privilege that restricts disclosure of the record to the individual
  - Another Act, an Act of Canada, or a court order prohibits disclosure of the record to the individual;
  - Granting the access could reasonably be expected to
    - Result in a risk of serious harm to the treatment or recovery of the individual or a risk of serious bodily harm to the individual or another person

Requesting Access to a Record of PHI

- An individual may exercise a right of access to a record of personal health information by making a written request to the health information custodian
- The request must contain sufficient detail to enable the custodian to identify and locate the record

Responding to a Request for Access

- Health information custodians receiving requests from individuals for access to a record of their personal health information shall:
  - Make the record available to the individual and, at the request of the individual, provide a copy of the record
  - Give a written notice to the individual stating that, after a reasonable search, the custodian has concluded that the record does not exist, cannot be found, or is not a record that applies
  - If the custodian is entitled to refuse the request, in whole or part, (e.g. due to risk of harm), the custodian must give a written notice to the individual stating that the custodian is refusing the request and provide a reason for the refusal and that the individual is entitled to make a complaint to the Commissioner

Regulatory and enforcement role; Ongoing and emerging policy issues

Where the IPC fits into PHIPA and how it regulates

Types of enforcement options

Emerging issues

Complaints Processes

- A person who believes that PHIPA has been (or is about to be) contravened may make a complaint to the Commissioner.
- The Commissioner may investigate the complaint and either dismiss the case, inquire further, initiate a mediation process, make an order to alter operations, or work with custodians to alter their processes to be compliant.
- The Commissioner may also initiate a review of the subject matter covered by a complaint if there are reasonable grounds to do so.
- The Commissioner has broad inspection powers to conduct a review or investigation.
- The Commissioner's powers are enumerated in s. 61 of PHIPA.
- There is the right of appeal of an order also.
- A case may also be referred for prosecution when an offence (under s.72) occurs.

Other Regulatory roles

- Three-year review processes are crucial
- Administrative monetary penalty powers are now possible
- “Modern and effective” regulatory authority
  - Moving from process-based to risk-based assessments
  - Focusing on desired outcomes of processes rather than the processes themselves
  - Desire to work towards a “just culture” model of regulatory involvement and enforcement
- Overlap with FIPPA, Coroners Act, CYFSA

Emerging issues

- Ontario Health / Ontario Health Teams and regulations around sharing of personal health information for population health management and integrated care models
- Audit logging of digital systems
- Removal of insecure methods of transmission of information (“Axe the fax”)
- Digital identity technologies
- Implications of artificial intelligence and machine learning
- Administrative Monetary Penalties / “Just Culture” development
- Consumer Electronic Service Provider Regulations

Emerging issues (cont'd.)

- De-Identification for broader use
- Cybersecurity / cyberattacks
- Virtual care
- "Data for Good" and privacy/security implications
- Implications of Artificial Intelligence

Breach Reporting

Mandatory Reports to IPC

Statistical Reporting

Reporting Breaches

- When breaches occur, there are seven instances specified where, in addition to letting the individual know, you are obliged to report the breach to the IPC:
  - Use or disclosure without authority
  - Stolen information
  - Further use or disclosure after a breach
  - Pattern of similar breaches
  - Disciplinary action against a member of a College
  - Disciplinary action against a non-member of a College
  - "Significant" breaches
    - Sensitivity, volume of records, number of individuals affected, more than one custodian involved

Annual Statistical Reporting

- Custodians are required to provide the IPC with an annual report of the previous calendar year's statistics.
- Note that these statistics include privacy breaches that did not meet the threshold for reporting the breach to the IPC.
- For more information about submitting annual statistics, please see ***Annual Reporting of Privacy Breach Statistics to the Commissioner***.

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

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

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

Direct: andrew.drummond@ipc.on.ca