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

University of Windsor

Faculty of Law

November 23, 2022

Introduction – the IPC

Mandate and structure

Major organizational priorities

Background: the IPC

- Provides oversight for provincial access and privacy laws establishing rules for how Ontario's public institutions, health care providers, children's aid societies (and other child and family service providers) may collect, use, and disclose personal information.
  - Freedom of Information and Protection of Privacy Act (FIPPA) and its municipal counterpart
  - Personal Health Information Protection Act (PHIPA)
  - Part X of the Child, Youth, and Family Services Act (CYFSA)
  - Anti-Racism Act
- Generally, these laws provide access rights to government and their own personal information while ensuring that any personal information remains private and secure within the bounds of the laws.
- As a result, we do spend a lot of our time resolving access appeals, investigating privacy breaches, and ensuring legal compliance

Background: the IPC (cont'd.)

- On top of regulatory duties, we also
  - Review privacy policies and information management practices
  - Provide comment on proposed government legislation and programs
  - Educate the public, media, and others about Ontario's access and privacy laws, as well as current issues affecting access and privacy

PHIPA – Purpose and Background

Disclaimer

Legislative Intent and Purposes

PHIPA within the broader IM legislative framework

Key concepts

PHIPA protects patient privacy and defines the obligations of all health system actors

Ontario's health sector is governed by the *Personal Health Information Protection Act, 2004* (PHIPA). PHIPA defines how personal health information ("PHI") is handled by everyone in the health care system, while enabling appropriate access to data to support high-quality patient care and critical functions in the health system.

Governs the Flow of PHI:

- Patient Access
- Collection/Use/Disclosure
- Security
- Consent
- Correction

Accountability:

- Defines actors and parties (e.g., health information custodians)
- Defines authorized collection/use/disclosure of Personal Health Information (PHI)
- Breach reporting and complaints to IPC

PHIPA

Enforcement:

- IPC powers and enforcement
- Breach prosecution
- Fines for breach up to $200,000 for individuals and $1,000,000 for businesses

Capacity:

- PHIPA enables the use of PHI without consent by a HIC for system planning; risk management, error management or to improve quality of care; educating agents; claims payment; and research

PHIPA - Purposes

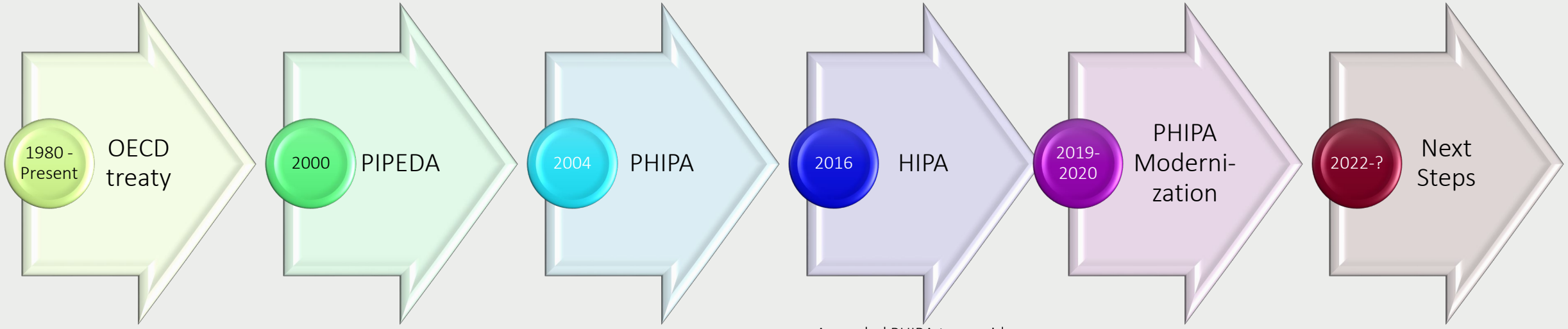
- PHIPA has five stated purposes
  - I – to establish rules for collection, use and disclosure ("c/u/d") of personal health information (PHI) that protect confidentiality of the information and privacy of individuals, while facilitating the effective provision of health care;
  - II – to provide a right 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.

- Leaving aside II – V, the key point of PHIPA is #1 – **which is a dual, co-equal purpose:**
  - **Protection of privacy**
  - **Facilitation of provision of care**

- **This is critical.** Some seem to view the purpose of PHIPA exclusively as the first part without considering the second.

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

- To be determined …

The Ontario **Information and Privacy Commissioner (IPC)** is an independent Officer of the Legislature who oversees the province's access and privacy laws, which includes both PHIPA and FIPPA.
The IPC provided input on the development of PHIPA and all its amendments

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.

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.

Prescribed Registries and Prescribed Entities

- PRs are registries of PHI to facilitate the provision of care.
    - They must be named in regulation (i.e., "prescribed") and have practices and procedures approved triennially by the IPC. (Without IPC approval, they are not authorized to collect PHI under this authority.)
    - There are currently 5 prescribed persons, operating six registries:
        - Ontario Health, for the Cancer Screening Registry and the Cardiac and Vascular Registry
        - INSCYTE Corporation for the Cytobase (cytology) registry
        - Hamilton Health Sciences, for the Critical Care Information System
        - CHEO – Ottawa Children's Treatment Centre, for the Better Outcomes Registry and Network ("BORN")
        - Ontario Institute of Cancer Research, for the Ontario Tumour Bank
- PEs conduct analysis for the management of, evaluation or monitoring of, the allocation of resources to, or planning for all or part of the health system, including delivery of services.
    - Like PRs, they must undergo triennial IPC review of their policies, practices, and procedures.
    - There are currently 4 PEs:
        - Canadian Institute for Health Information ("CIHI")
        - Ontario Health (under its former Cancer Care Ontario authority)
        - Institute for Clinical/Evaluative Sciences ("IC/ES")
        - Pediatric Oncology Group of Ontario ("POGO")

Health Data Institutes (“HDIs”)

- PHIPA also contemplates the existence of a “Health Data Institute” under the heading of “Disclosure for Analysis of the Health System”
- No HDI has ever been formed.
- They would undergo similar IPC review to PEs.
- The Minister would have authority to order disclosure to an HDI, but would not have access to identifiable data
- The duties of an HDI would be described by its corporate objects and would be required to
- follow the practices and procedures described in clause (9) (b) that the Commissioner has approved;
    - perform the analysis and linking with other data that the Minister requires;
    - de-identify the information;
    - provide the results of the analysis and linking, using only de-identified information, to the Minister or to the persons that the Minister approves;
    - not disclose the information to the Minister or to the persons that the Minister approves except in a de-identified form; and
    - not disclose to any persons the information, even in a de-identified form, or any information derived from the information

Part V.1: Electronic Health Record

What is the electronic health record?
What is the prescribed organization?
What is unique about Part V.1?
Where does Ontario Health fit in with all this?

The EHR

- Right now, it's (legally speaking) extremely easy to share information between providers for care, but the process of sharing imagines a provider sharing a copy of information with another provider upon request
- An EHR inverts that, though: it's possible just to look someone up. This presents opportunities for improvement of health outcomes but also potential problems for privacy violations.
- Part V.1, enacted in October 2020, attempts to solve these concerns with province-level digital assets, which are
    - Ontario Laboratory Information System ("OLIS"), for which the Minister of Health is the HIC
    - Digital Health Drug Repository ("DHDR"), for which the Minister of Health is currently the sole HIC
    - Digital Imaging – Common Service ("DI-CS"), which has multiple HICs
    - Acute Care Clinical Data Repository (acCDR), which has multiple HICs and is unstructured data
- The EHR is designed as a means for the sharing of information from provider to provider, for the purposes of providing care. Other purposes (with highly limited exceptions) are not permitted.

The Prescribed Organization

- Ontario Health (Digital Excellence in Health) – formerly eHO – is named in regulation as the prescribed organization for operating the EHR.
- **OH does not have custody and control of the contents of the EHR.** The agency's responsibility is to operate the systems that make up the EHR on behalf of the HICs that contribute.
- Because the HICs contribute the data, there needs to be some way to incorporate the principle of consent into operation of the EHR.
    - Ontario has chosen the policy that individuals' information will go into the EHR, but that the prescribed organization must manage consent directives on their behalf to limit access to PHI if requested.
    - This model sustains the principle of assumed implied consent – providers can assume that their patients consent to the c/u/d of their PHI unless they specifically say not to – while maintaining the principle that it is for health care.
    - Two exceptions were recently (2020) carved out: medical officers of health, and coroners, each of which have independent authorities (i.e., outside PHIPA) to collect and use PHI.
- Consent management for the EHR remains an extremely complex issue and the IPC's policy view is that current regulations are insufficient for appropriate patient consent management.
- OH will soon be able to act "as if it were a custodian" in releasing PHI directly to individuals, through digital means (i.e., health apps). This would represent a significant jump in individual access to PHI.

Part V.1 – Other Features

- By regulatory authority under Part V.1, contributions to the EHR by HICs (or classes of HICs) may be mandated.
- "Level of specificity" of consent directives may be set by regulation.
- Under Part V.1, a consent directive could be overridden without consent if there is risk of serious bodily harm.
- An advisory committee must be set up to advise both the prescribed organization and the Minister of Health on EHR practices and procedures, including on when to recommend non-health care uses.
- The Ministry of Health could collect from the EHR under authority of FIPPA Part III.1 as part of the government's broader data integration initiative.
- Coroners and medical officers of health are able to access the EHR for non-care purposes.

Ontario Health - Uniquenesses

- Ontario Health is still a new entity, and is still determining the exact information authorities it will hold over the long and how they will interact.
- OH is a PE (CCO), PR (CCO, CorHealth), PO (eHO), health information network provider ("HINP"), Agent (of the Ministry, and of others)
- In each role, its authorities to collect, to use, and to disclose personal health information may be different.
- It has multiple types of mandates and access to – but not always control of – many datasets with PHI

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 may be pending.
- “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

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