Electronic Health Record Systems – ESPs, HINPs, Shared Systems and Recent *PHIPA* Amendments

Brendan Gray, Health Law Counsel

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

IT and Privacy in Health Law

Osgoode Hall LLM

May 5, 2023

DISCLAIMER

THIS PRESENTATION IS:

- PROVIDED FOR INFORMATIONAL PURPOSES,
- NOT LEGAL ADVICE, AND
- NOT BINDING ON THE IPC.

Topics

1. What is the IPC?
2. Electronic Service Providers
3. Health Information Network Providers
4. Shared Electronic Health Record Systems
5. “Circle of Care” and Shared Systems
6. Part V.1 Provincial EHR
7. Recent *PHIPA* Amendments

What is the IPC?

Information and Privacy Commissioner of Ontario (IPC)

- The IPC is an officer of the legislative assembly
- Until very recently, the IPC only had authority under three acts:
  - *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - *Personal Health Information Protection Act, 2004* (the *Act* or *PHIPA*)

Information and Privacy Commissioner (IPC), cont'd

- But now there are more acts with an oversight role for the IPC, including
  - *Child, Youth and Family Services Act, 2017*
  - *Anti-Racism Act, 2017*

Electronic Service Providers

Electronic Service Providers (ESPs)

- Health information custodians are permitted to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information, subject to prescribed requirements
- A person who provides services for the purpose of enabling a custodian to use electronic means for the above activities may, or may not, be an "agent" of the custodian
- For agent ESPs:
  - Section 17 of the *Act* outlines the conditions and restrictions under which a custodian may permit an agent to act on its behalf. Among other things, agents require the custodian's permission to collect, use, disclose, retain or dispose of personal health information, subject to prescribed exceptions

Electronic Service Providers (ESPs), cont'd

- For non-agents ESPs:
  - Section 6 of regulation to the *Act* applies to ESPs who are not agents and, except as otherwise required by law, requires that they not:
    - use any personal health information to which they have access in the course of providing the services for health information custodians except as necessary in the course of providing the services
    - disclose any personal health information to which they have access in the course of providing the services
    - permit their employees or any person acting on their behalf to have access to the information unless the employee or person acting on their behalf agrees to comply with the restrictions that apply to the ESP
  - Broadly speaking, the rules for agent and non-agent ESPs reflect the fact that the person who provides services is not the decision-maker with respect to the personal health information and acts at the direction of the health information custodian*

*See PHIPA Decision 50 and Halyna Perun, Michael Orr and Fannie Dimitriadis, *Guide to the Ontario Personal Health Information Protection Act* (Irwin Law: Toronto, 2005), 65

Health Information Network Providers

Health Information Network Providers (HINPs)

- A HINP is a person who provides services:
  - To two or more custodians
  - Where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another
- In short, a HINP is a special type of ESP that is subject to additional obligations
- A HINP must fulfill the duties and obligations in the regulation to the *Act*, including to:
  - Notify custodians if an unauthorized person accessed information or the HINP accessed information for unauthorized purposes
  - Conduct and provide a copy of the results of privacy impact assessments and threat, vulnerability and risk assessments to the custodians
  - Enter into an agreement with the custodians describing the services and safeguards related to confidentiality and security of the information
  - Make available to custodians, on request, a record of all accesses and transfers to the extent and in a manner reasonably practical

Shared Electronic Health Record Systems

Custody and Control of Shared Electronic Health Record Systems

- In Ontario, a custodian generally does not have sole custody or control over the health information in a shared system
- Custody and control is usually shared, as is accountability
- Typically a custodian only has custody or control of health information that the custodian:
  - Creates or contributes to the shared system
  - Collects from the shared system
- Shared custody and control poses unique challenges for compliance with the *Act*

Challenges Posed by Shared Electronic Health Record Systems

- Lack of clarity as to which custodian(s) is/are responsible for undertaking each duty and fulfilling each obligation in the *Act*
- Lack of clarity about who is the HINP and how the HINP's duties are satisfied
- Increased risk of unauthorized use and disclosure because all participating custodians and their agents may have access to all the information in the system
- Attracts hackers and others with malicious intent

How to Address These Challenges

- A governance framework and harmonized privacy policies and procedures are needed to address the challenges
- The governance framework and harmonized policies must, among other things:
  - Identify who will be participating in the shared system
  - Set out the roles, responsibilities and obligations of each custodian participating in the system
  - Identify the HINP for the system
  - Set out how the responsibilities and obligations of the HINP have been or will be satisfied
  - Set out the expectations for all custodians and agents accessing health information in the system
  - Set out how individuals may exercise their rights under the *Act*

“Circle of Care” and Shared Systems

Assumed Implied Consent

- Sometimes referred to as “Circle of Care”

- Section 20(2) of the *Act* provides:

  (2) A health information custodian described in paragraph 1, 3 or 4 of the definition of “health information custodian” in subsection 3 (1), that receives personal health information about an individual from the individual, the individual’s substitute decision-maker or another health information custodian for the purpose of providing health care or assisting in the provision of health care to the individual, is entitled to assume that it has the individual’s implied consent to collect, use or disclose the information for the purposes of providing health care or assisting in providing health care to the individual, unless the custodian that receives the information is aware that the individual has expressly withheld or withdrawn the consent.

- In the context of a disclosure, the disclosure must be made to another health information custodian

“Circle of Care” in Shared Systems

- It is essential that shared system policies specify the purposes for which agents are permitted to collect, use and disclose personal health information
- Shared systems pose unique challenges for determining the legal authority for non-consensual collections, uses and disclosures of personal health information - different legal authorities may apply to different parts of a record
- Because of this, many shared systems restrict:
  - custodians to only collecting, using and disclosing personal health information for the purposes of providing or assisting in the provision of health care, with narrow exceptions; and
  - participation in the shared system to only custodians

Part V.1 Provincial EHR

Responsibility for Developing and Maintaining the Provincial EHR

- The provincial EHR is developed and maintained by one or more prescribed organizations
- One organization has been prescribed: Ontario Health
- The prescribed organization is 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 Commissioner within one year of Part V.1 coming into force and every three years thereafter

Custody or control and Collection, Use and Disclosure

- Custodians don't have sole custody or control of PHI in the provincial EHR – it is shared. Custodian only have custody or control of PHI if it:
  - creates and contributes the PHI to the provincial EHR, or
  - collects the PHI from the provincial EHR
- Special definitions of collection, use and disclosure apply:
  - A **collection** occurs when a custodian views, handles or deals with PHI contributed to the EHR by another custodian for the first time
  - A **use** occurs when a custodian views, handles or deals PHI that it contributed to the EHR or when a custodian views, handles or deals with PHI contributed by another custodian on a subsequent occasion after a previous collection
  - A **disclosure** only occurs when another custodian collects PHI from the EHR (and not when the disclosing custodian provides the PHI to the prescribed organization)

Collection, Use and Disclosure and Authorities

- In general, custodians are only 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

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
- Regulations have been made specifying the data elements that may not be subject to a directive
- The regulations provide that you cannot impose a consent directive on basic demographic information

Consent Directives, cont'd

- Regulations under *PHIPA* further limit the PHI that may be blocked by a consent directive. Individuals only have the right to block the entirety of their health record – unless a more granular block is "reasonably possible"
- Note that this aspect of the regulation does not apply to consent directives previously made in the systems that have become the EHR (and where no new directive has been made)

Consent Overrides

- A custodian will be permitted to override a directive:
  - with the express consent of the individual; or
  - 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 or group 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 PHI is 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 is 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 another person or group, provide additional written notice to the Commissioner
- Regulations to *PHIPA* specify the content of these notices

Directed Disclosures

- The Minister of Health will be able to direct the disclosure of PHI contributed by more than one custodian:
  - to prescribed registries (e.g. Cardiac Care Network of Ontario) for the purposes of section 39(1)(c) of *PHIPA*
  - to prescribed entities (e.g. ICES) for the purposes of section 45 of *PHIPA*
  - to certain public health authorities (e.g. medical officers of health) for the purposes of section 39(2) of *PHIPA*
  - for research purposes in accordance with section 44 of *PHIPA*
- Prior to directing the disclosure, the Minister must submit the request received to, and must consult with, the advisory committee
- Note that coroners and medical officers of health also have direct access to EHR

Breach Notification

- In the context of the provincial EHR, the custodian must notify the individual at the first reasonable opportunity if PHI is collected without authority
- The Commissioner must also be notified if the circumstances surrounding an unauthorized collection meets certain prescribed requirements
    - Prescribed circumstances in which the Commissioner must be notified of an unauthorized collection from the EHR match those for an unauthorized use or disclosure in the non-EHR context
- The Prescribed Organization (Ontario Health) must also notify the Commissioner immediately where it (or a third party retained by it) views, handles, deals with, makes available or releases PHI other than in accordance with *PHIPA* or its regulations

Access to records in the EHR

- Where custodians have custody or control of records of personal health information in the EHR, they are required to respond and provide access (subject to exceptions) – like other records over which they have custody or control .

- Note:
  - There are special rules for obtaining access to personal health information from the prescribed organization, which are not yet in force (see s. 51(5) of *PHIPA* and s. 18.1.1 of O. Reg. 329/04). This includes a phased-in schedule for different repositories.
  - There are special rules for obtaining access from custodians for records of when they viewed, handled or otherwise dealt with personal health information in the EHR, which are also not yet in force (see s. 51(6) and s. 18.1.2 of O. Reg. 329/04). In short, they are only required to provide a summary.

PHIPA AMENDMENTS

Introduction to *PHIPA* Amendments

- Relatively recent changes to *PHIPA* and its regulation cover several novel and important privacy and access to information issues, including:
  - Administrative penalties and offences
  - Regulation of de-identified information
  - Access to records in electronic format
  - Requirement to maintain an electronic audit log
  - Interoperability requirements

Administrative penalties and offences

- Bill 188 amended *PHIPA* to allow the IPC to issue an order requiring a person who has contravened *PHIPA* or its regulation to pay an administrative penalty
- Administrative penalties may be issued to:
  - encourage compliance with *PHIPA* and its regulation; or
  - prevent a person from deriving any economic benefit as a result of a contravention

Administrative penalties and offences, cont'd

- The amount of an administrative penalty will be determined in accordance with regulations yet to be prescribed
  - Until these regulations are prescribed, the IPC cannot issue administrative penalties
- Administrative penalties must be paid to the Ministry of Finance
- Bill 188 also amended *PHIPA* to double fines for offences
- Fines are now up to $200,000 for individuals and $1,000,000 for corporations. Individuals can also be imprisoned for up to 1 year
- These amendments are in force

Regulation of de-identified information

- There has been increasing concern about the ability of organizations to use large data sets of de-identified health information to re-identify individuals
- In light of these concerns, three amendments were made to *PHIPA*

1. Bill 138 amended *PHIPA* to prohibit a person from using or attempting to use de-identified information to identify an individual, subject to certain exceptions
2. Bill 138 also created an offence for willfully contravening this prohibition on the use of de-identified information to re-identify an individual
3. Bill 188 amended the definition of "de-identify" to enable requirements to be prescribed for how PHI is to be de-identified

Access to records in electronic format and portals

- With the increase in electronic forms of communication, there was a concern that an individual's right of access under *PHIPA* would become outdated
- Individuals are also increasingly taking steps to manage their own PHI through patient portals and health apps
- In light of these changes, two amendments were made to *PHIPA*
    1. Bill 188 amended *PHIPA* to give individuals the right to access their records of PHI in an electronic format that meets prescribed requirements
    2. Bill 188 also amended *PHIPA* to regulate a new class of persons called "consumer electronic service providers" (CESPs)

Access to records in electronic format and portals , cont'd

- Currently, regulations require custodians to provide individuals with access to records in a PDF file or any other format agreed to by the individual and custodian (including a patient portal).
- On July 1, 2023, the regulation will be amended to allow Ontario Health to start specifying electronic formats, subject to various procedural requirements (such as consulting with the IPC).

Access to records in electronic format and portals , cont'd

- CESPs are defined as:
  - persons who provide electronic services to individuals at their request, primarily for the purpose of allowing those individuals to access, use, disclose, modify, maintain or otherwise manage their records of PHI, or for such other purposes as may be prescribed (e.g. apps used by individuals to access copies of physician reports and prescriptions)
- Many of the specific requirements relating to CESPs are left to be prescribed in regulation
- The CESP provisions are not yet in force and no regulations have been made

Interoperability Requirements

- Increased use of electronic information systems in health care has created another problem: silos of information in one electronic system that cannot be read or understood by other systems
- *PHIPA* was recently amended to allow regulations to be made governing the interoperability between health information custodians' systems. Regulations came into force on January 1, 2021.
- This is not in Part V.1 of *PHIPA.*
- This is sometimes referred to as the Digital Health Information Exchange (DHIEX).
- Regulations require Ontario Health to set "interoperability specifications" relating to custodian's "digital health assets". Again, Ontario Health must comply with various procedural requirements, including consulting with the IPC in certain circumstances

Interoperability Requirements, cont'd

- Custodians will be required to use digital health assets that comply with the interoperability specifications
- Ontario Health will be responsible for monitoring custodian's compliance with the interoperability specifications and consulting with custodians on compliance issues. Custodians must co-operate with and assist Ontario Health.
- The IPC may receive complaints that custodians have selected digital health assets that do not comply the interoperability specifications, and adjudicate compliance (which could include issuing orders). Ontario Health may make complaints and provide information it gathers to the IPC
- Selecting compliant digital health assets does not relieve custodians of their other obligations. For example, custodians must still comply the with security requirements in *PHIPA*

QUESTIONS?

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