Providing Electronic Services to Custodians

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

2019 PHIPA CONNECTIONS SUMMIT

December 3, 2019

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 Systems
5. “Circle of Care” and Shared Systems
6. PHIPA Decision 102 and Shared Systems

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')

- But now there are more acts (some are in force and some are not in force) 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 any prescribed exceptions

Electronic Service Providers (ESPs) (Cont'd)

- For non-agents ESPs:
  - Section 6 of the 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 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 custodian*

*See PHIPA Decisions 50 and 102 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 primarily enable the custodians to use electronic means to disclose 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 section 6 of 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 Systems

Challenges Posed by 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. Shared custody and control poses unique challenges for compliance with the *Act*
- 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 typically all participating custodians and their agents 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:
  - 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*

Governance Framework

- The governance framework should address:
  - Who will participate in and have access to the shared system
  - What information will be included in the shared system
  - What levels of access will be granted
  - For what purposes will health information be permitted to be collected, used and disclosed
  - The harmonized privacy policies and procedures that apply
  - The persons responsible and the process that will be used to make decisions regarding the above

Nature of Harmonized Privacy Policies and Procedures

- Harmonized privacy policies and procedures should be developed to address:
  - Privacy breach management
  - Consent management
  - Logging, auditing and monitoring
  - Access and correction
  - Privacy training and awareness
  - Privacy assurance
  - Privacy complaints and inquiries management
  - Governance

“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, 2, 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

PHIPA Decision 102 and Shared Systems

Shared Systems

PHIPA Decision 102

- The IPC received breach reports from three separate custodians about privacy breaches involving a shared electronic patient information system
- The IPC decided to take a broader look to assess whether the breaches raised common and systemic issues across the shared system
- Lengthy and complex investigation involving multiple files and custodians
- One of the custodians was the HINP responsible for the shared system

Shared Systems
PHIPA Decision 102

Cont'd

- The IPC's investigation found issues with respect to staff training, consistent auditing practices and timely notification of breaches, among other things
- While deficiencies were found, the custodians agreed to address the issues – no further review was warranted
- Decision offers good examples of common pitfalls of shared systems

Shared Systems

Cont'd

PHIPA Decision 102

What's a use and a disclosure in a shared system?

- Decision found that custodians participating in this shared system were considered to be the custodian of personal health information they created, contributed or collected
- Where an agent of a custodian accesses personal health information that has been created, contributed, or collected by the custodian on whose behalf the agent is acting, this would be considered a "use"
- Where an agent accesses personal health information that was not created or contributed or collected by the custodian on whose behalf the agent is acting, that is:
  - a "collection" by the custodian on whose behalf the agent is acting and
  - a "disclosure" by the custodian(s) with custody or control of the information
- Ultimately, does not matter in this case because, either way, the accesses were unauthorized

Shared Systems

Cont'd

PHIPA Decision 102

THE SIX BREACHES- Breach #1

- Hospital #1 received a complaint that a nurse of the hospital accessed a patient's file without authorization
- The hospital completed an audit. The audit identified 60 breaches dating back to 2010 that involved the personal health information of family, friends, high profile patients, an ex-spouse and the ex-spouse's girlfriend
- Some of the personal health information accessed was information of a patient that was treated at another hospital. The information was accessed by the nurse through the shared system

Shared Systems

PHIPA Decision 102

Cont'd

THE SIX BREACHES- Breach #2

- Hospital #2's privacy office received a report pertaining to the Ontario Laboratories Information System (OLIS)
- The hospital determined that a nurse viewed a patient's personal health information for whom the nurse was not part of that patient's circle of care
- A further audit was completed. The audit showed that the nurse had 144 accesses to personal health information of 21 patients between 2011 and 2015 without authorization, including friends, family and colleagues
- Some of the additional accesses identified were to personal health information of patients who were treated at another hospital in the shared system

Shared Systems

Cont'd

PHIPA Decision 102

THE SIX BREACHES - Breach #3:

- Hospital #3 received a complaint that a clerk had accessed her ex- spouse's personal health information without authorization. An investigation was initiated
- The hospital did not suspend the clerk's access during the investigation because the clerk required access to complete her job duties
- The hospital advised the clerk that her accesses were being investigated and not to access the personal health information of the ex-spouse
- The hospital's privacy office completed a further audit on the clerk's accesses. The audit identified access to the ex-spouse's file after the initial complaint and after the clerk was advised that her accesses were being investigated
- Audit also identified 35 additional unauthorized accesses to six additional patients (family and colleagues)

Shared Systems

Cont'd

PHIPA Decision 102

THE SIX BREACHES - Breach #4:

- Audit of two high profile patients of hospital #3 identified that an assistant of a customer of the shared system had accessed the personal health record of these two patients without authorization
- The further audit confirmed that the assistant had accessed the records of personal health information of 44 patients in the previous six months without authorization

Shared Systems

Cont'd

PHIPA Decision 102

THE SIX BREACHES- Breach #5:

- Audit of the two high profile patients completed by hospital #3 in relation to breach #4 also identified that a laboratory staff member of a fourth hospital (hospital #4) had accessed the personal health information of one of the high profile patients through the shared system without authorization

Shared Systems

Cont'd

PHIPA Decision 102

THE SIX BREACHES- Breach #6:

- Audit of the high profile patients identified that a pharmacy staff member of hospital #3 had accessed one of the high profile patient's personal health information without authorization
- Hospital commenced an investigation and a further audit was completed. The further audit identified additional unauthorized accesses

Shared Systems

Cont'd

PHIPA Decision 102

Issue 1 - Agreements

- Agreement governing shared system was entered into before *PHIPA* came into force
- Was not amended to specify the role of hospital #3 as the HINP in relation to the shared system or to outline the requirements set out in section 6 of *Ontario Regulation 329/04*
- Decision found: HINP and all health information custodians that are participating in a shared system should ensure that they have a written agreement and policies and procedures that reflect their respective legislated roles and responsibilities
- Agreement and policies and procedures should reference the applicable roles and responsibilities imposed by PHIPA and its regulation and assign duties and obligations that comply with these requirements
- Agreement also did not include all detailed requirements set out in section 6 of Reg

Shared Systems

Cont'd

PHIPA Decision 102

Issue 2 - Privacy Breach Management Policy:

- There was a shared system privacy breach management policy… but
  - it was not comprehensive, and
  - in same cases referred to local hospital policies that were not consistent with the shared system policy, or were simply incorrect or non-existent
- Shared system policy did not clearly indicate who was responsible for the notification of affected parties
- In one breach, a miscommunication between custodians resulted in a failure to notify patients of the breach at the first reasonable opportunity
- Policy also did not address deceased's patients
- Policies did not address breaches in OLIS - Ministry of Health has custody or control of the information contained in OLIS through their agent eHealth Ontario (now Ontario Health)

Shared Systems

Cont'd

PHIPA Decision 102

Issue 2 - Privacy Breach Management Policy …cont'd

- Decision found:
  - Custodians that are part of a shared system should all have consistent, comprehensive and legally accurate privacy breach management policies that include procedures addressing identification, reporting, containment, notification, investigation and remediation of suspected and actual privacy breaches
  - Privacy breach management policies must provide sufficient clarity so that custodians participating in a shared system are aware of what steps they are required to take and can be confident that patients who are entitled to be notified of a privacy breach involving their personal health information will, in fact, be notified

Shared Systems

Cont'd

PHIPA Decision 102

Issue 3 - Lock-box Policies and Procedures:

- Patient raised a concern about his ex-spouse, a clerk at a hospital. Hospital offered to monitor the clerk's accesses but did not discuss lock-box options with patient due to technical limitations. Clerk accessed the record again
- Technical limitations does not relieve custodians of the obligation to comply with the lock-box provisions of the *Act*
- Decision found: Hospital should have at least raised the lock-box provisions of the *Act* with the patient
- The patient would then at least be in a position to effectively assert his rights and understand the options available to implement a lock-box
- Patient could have explored other options that may have been available. The hospital subsequently indicated it can create a flag that will pop-up when a particular patient's personal health information is accessed in part of the shared system

Shared Systems

Cont'd

PHIPA Decision 102

Issue 3 - Lock-box Policies and Procedures …cont'd:

- There was no system wide lock-box policy that addressed how to deal with the lack of a technological ability to restrict a users' access to a particular patient's personal health record
- When participating in a shared system, other custodians accessing personal health information must be able to comply with patient lock-boxes through clear, comprehensive and system wide policies and procedures

Shared Systems

Cont'd

PHIPA Decision 102

Issue 4 - Privacy Training and Education:

- All hospitals provided training to their agents upon hire.
- However, not all agents of the hospitals consistently received training prior to accessing personal health information or annually thereafter
- At the time that the breaches took place, only hospital #4 provided its agents with privacy training on an annual basis
- Hospital #2 did not provide its physician agents with any privacy training, either initially or thereafter
- Policies governing the shared system did not specifically require hospitals to provide any training to agents
- HINP/hospital #3 considered training the responsibility of each custodian and stated that each custodian was responsible for their own interpretation of the *Act*

Shared Systems

Cont'd

PHIPA Decision 102

Issue 4 - Privacy Training and Education …cont'd:

- Decision found: Where custodians are pooling their personal health information in a shared system, it is untenable for each custodian to be responsible for their own interpretation of the *Act*
- Where one custodian is granting access to a system containing personal health information in its custody or control to an agent of another custodian, that agent must be instructed on the terms under which access is granted (including conditions and restrictions on access)
- Without consistent and comprehensive training across all custodians with access to the shared system, there can be confusion among the agents of the various custodians as to what is, and is not, permitted in the shared system
- The custodians are participating in the shared system are granting other custodians' agents access to personal health information in their custody or control in the absence of steps to ensure those agents understand what they are permitted to do

Shared Systems

Cont'd

PHIPA Decision 102

Issue 4 - Privacy Training and Education …cont'd:

- Privacy Officer training:
  - Information displayed on the audit reports conducted by the hospitals varied. Hospital #1's audit report did not display the length of time the user accessed the various screens of a patient's personal health record in the shared system. The other hospitals in this investigation were able to produce audit reports that included this information
  - The privacy officer was unaware of how to run a report displaying this information
- All privacy officers with access to the same shared system should have the same tools when monitoring agents for unauthorized access and know how to effectively use the available auditing systems

Shared Systems

Cont'd

PHIPA Decision 102

Issue 5 and 6 – Confidentiality Agreements and Privacy Notices:

- All the hospitals involved had their agents' sign a confidentiality agreement at the time of hire
- Only hospital #4 consistently had agents re-sign confidentiality agreements annually and tracked the signing of confidentiality agreements. The re- signing and tracking at the other hospitals involved was inconsistent or nonexistent
- At hospital #3, agents were not required to re-sign confidentiality agreements. The confidentiality agreements were only re-signed when warranted such as when there was a privacy incident
- In breach #6, hospital #3 advised that the pharmacy staff member had signed a confidentiality agreement but hospital #3 was unable to locate a copy of the signed confidentiality agreement
- The group of custodians had no written document that established minimum standards regarding confidentiality agreements across the shared system

Shared Systems

Cont'd

PHIPA Decision 102

Issue 5 and 6 – Confidentiality Agreements and Privacy Notices:

- At the time of the breaches, the shared system did not have a privacy notice that agents accessing the shared system would view prior to accessing personal health information
- During the course of the IPC's investigation, a privacy notice was implemented on the shared system

Shared Systems

Cont'd

PHIPA Decision 102

Issue 7– Auditing:

- All the hospitals involved advised that random and targeted audits were completed
- However, the frequency of audits and length of period audited were not consistent
- Hospital #4 advised that the functionality of the user audit log within Meditech only permitted auditing of two weeks of historical information - which did not comply with the shared system auditing policy
    - Interestingly, the other hospitals were able to complete longer audits on their users' accesses to the shared system
- Information that displayed on the audit reports conducted by the hospitals varied. As noted above, hospital #1's audit report did not display the length of time the user accessed the various screens in the shared system. The other hospitals in this investigation were able to produce audit reports that included this information

Shared Systems

Cont'd

PHIPA Decision 102

Issue 7– Auditing…cont'd:

- The custodians agreed to establish a minimum standard of auditing capability.
- The minimum standard for auditing will include a standard for the type of data displayed and a minimum standard retention period that is significantly longer than 2 weeks.
- Group also developed and implemented training for their privacy officers on Meditech's auditing capabilities so that privacy officers of custodians with access to the shared system are aware of all of the features and capabilities of the system.

Shared Systems

PHIPA Decision 102

Cont'd

Issue 8– HINP compliance:

- There was no agreement that would comply with all of the requirements of paragraph 7 of section 6(3) of the Regulation
  - The agreement did not describe the administrative, technical and physical safeguards relating to the confidentiality and security of the information
- HINPs are required to provide each custodian a plain language description of the services it provides
  - The HINP advised that it only provided such a plain language description upon request
- HINPs are required to make certain information available to the public. This information includes a general description of the safeguards implemented by the HINP in relation to the security and confidentiality of the information
  - The HINP had not made the above noted information available to the public

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