PHIPA Amendments and Reasonableness Requirements

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

Privacy Leaders' Professional Learning Event

Alliance for Healthier Communities

October 3, 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. Recent *PHIPA* Amendments
3. Section 12(1) - Steps that are reasonable in the circumstances

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*

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

- The 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 was amended to also allow Ontario Health to start specifying electronic formats (again including patient portals), 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*

Section 12(1) - Steps that are reasonable in the circumstances

Section 12 (1) of *PHIPA*

A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. [Emphasis added]

What does section 12(1) require?

- The standard in section 12(1) is reasonableness
- It does not require perfection
- It does not provide a detailed prescription for what is reasonable
- Section 12(1) covers both preventing breaches and responding to breaches when they occur

PHIPA DECISION 153 - HR18-118 (Part 1 of 2)

- A hospital reported three privacy breaches to the IPC
- The hospital's audit identified some questionable accesses to patients' health records by an employee and interviewed the employee to obtain an explanation
- The hospital imposed an unpaid suspension, reported the employee to the College of Nurses of Ontario, and advised her that further unauthorized accesses would result in termination of employment.

PHIPA DECISION 153 - HR18-118 (Part 2 of 2)

- The hospital implemented a learning plan for the employee, which included content directed at privacy obligations and processes. The hospital informed the IPC that the learning plan consists of high level goals and guiding principles, then more detailed goals, learning objectives and success indicators. In this particular case, the detailed goals consisted of: privacy and confidentiality, accountability, professional standards, ethics, circle of care and leadership. The employee completed this learning plan.
- Also as a result of this incident, the hospital audited this employee's accesses to the EMR every 2-3 months to confirm that the individual is following its processes.
- In the circumstances, the hospital responded adequately to the apparent privacy breaches by investigating the circumstances, and taking remedial action.

PHIPA DECISION 213- HC18-7 (Part 1 of 2)

- Allegations that a hospital and a doctor who had privileges at the hospital used and disclosed the complainant's personal health information in violation of her withdrawal of consent following her allegations of sexual assault by the doctor, and her request that the doctor no longer be involved in her health care.
- The hospital focused on the fact the complainant never explicitly asked the hospital to "lock" her records of personal health information. This was unreasonable.

PHIPA DECISION 213- HC18-7 (Part 2 of 2)

- "Given the nature of the complainant's concerns, it would have been appropriate in this circumstance for the hospital to actively ascertain the complainant's wishes with respect to her personal health information vis-à-vis the doctor, and to document those wishes. The hospital's failure to do so in this case was a violation of its obligations under section 12(1) of PHIPA to take reasonable steps to protect personal health information in its custody or control against unauthorized uses and disclosures. In fact, this failure resulted in the unauthorized uses and disclosure described above."

PHIPA DECISION 44 - HC14-16 (Part 1 of 3)

- A physician alleged that some of his colleagues engaged in unauthorized uses or disclosures of his personal health information, and that the hospital took inadequate steps to protect the privacy of his health information and respond to his complaints.
- Focus on auditing and logging practices, automatic timed logouts, and training of agents, as these are raised by the circumstances of this complaint.
- <u>Auditing and Logging:</u>
  - Adjudicator agreed that the failure to distinguish between scrolling and viewing events diminishes the utility of the auditing system. In this case, the system logs pauses while scrolling through a worklist with a keyboard in the same manner as if a user reads a report containing a patient's diagnosis. Agents may take a telephone call, or may simply become distracted, while scrolling through a worklist. This could create the misleading impression that such an agent had read a detailed record containing personal health information, as opposed to simply sitting at their workstation performing other tasks while a name is continuously highlighted on a worklist.
  - While the Adjudicator did not conclude that the hospital's auditing and logging practices fall below the "reasonable" standard required by section 12 of the Act, she recommended that the hospital consider making improvements.

PHIPA DECISION 44 - HC14-16 (Part 2 of 3)

- Automatic timed logouts
  - Physician stated that if he is working on a list of examinations and is called away to see a patient or perform a procedure, the highlighted name may remain highlighted for the duration of his absence from the work station, creating the impression that the record has been "accessed" for a significant period of time.
  - This raised an issue of automatic log-outs after periods of inactivity
  - "There is no uniform approach to automatic logouts from electronic information systems, as the appropriate automatic logout time period may depend on factors such as the location of terminals, the number of staff or members of the public that have access to the area, the existence of lock screens, the type of information contained in the system and other policies and practices in place to protect the privacy of personal health information in the system. In this case, I have not concluded that any deficiencies in automatic logout practices resulted in unauthorized accesses. However, given the submissions from the physicians, I will recommend that the hospital review its practices with respect to automatic logouts."

PHIPA DECISION 44 - HC14-16 (Part 3 of 3)

- Training:
  - While the hospital had provided the IPC with numerous of its policies prior to the Notice of Review being sent, none of these policies addressed or described the content of training provided to the four doctors.
  - "Training is a fundamental administrative safeguard health information custodians must perform. While the specific content of the training required may vary by situation, health information custodians must train their agents in order to comply with section 12(1) of the Act . Otherwise, health information custodians would be providing personal health information to their agents, without guiding their agents on what they can do with this information."
  - The Adjudicator was concerned that the hospital's periodic mandatory training of its agents did not address data minimization requirements (which was the breach she found) and ordered the hospital to fix this.

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