Recent *PHIPA* Amendments and Privacy/Security Considerations for Virtual Care

Patricia Kosseim and Manuela Di Re

Information and Privacy Commissioner of Ontario

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

Annual Privacy Officers' Virtual Professional Learning Event

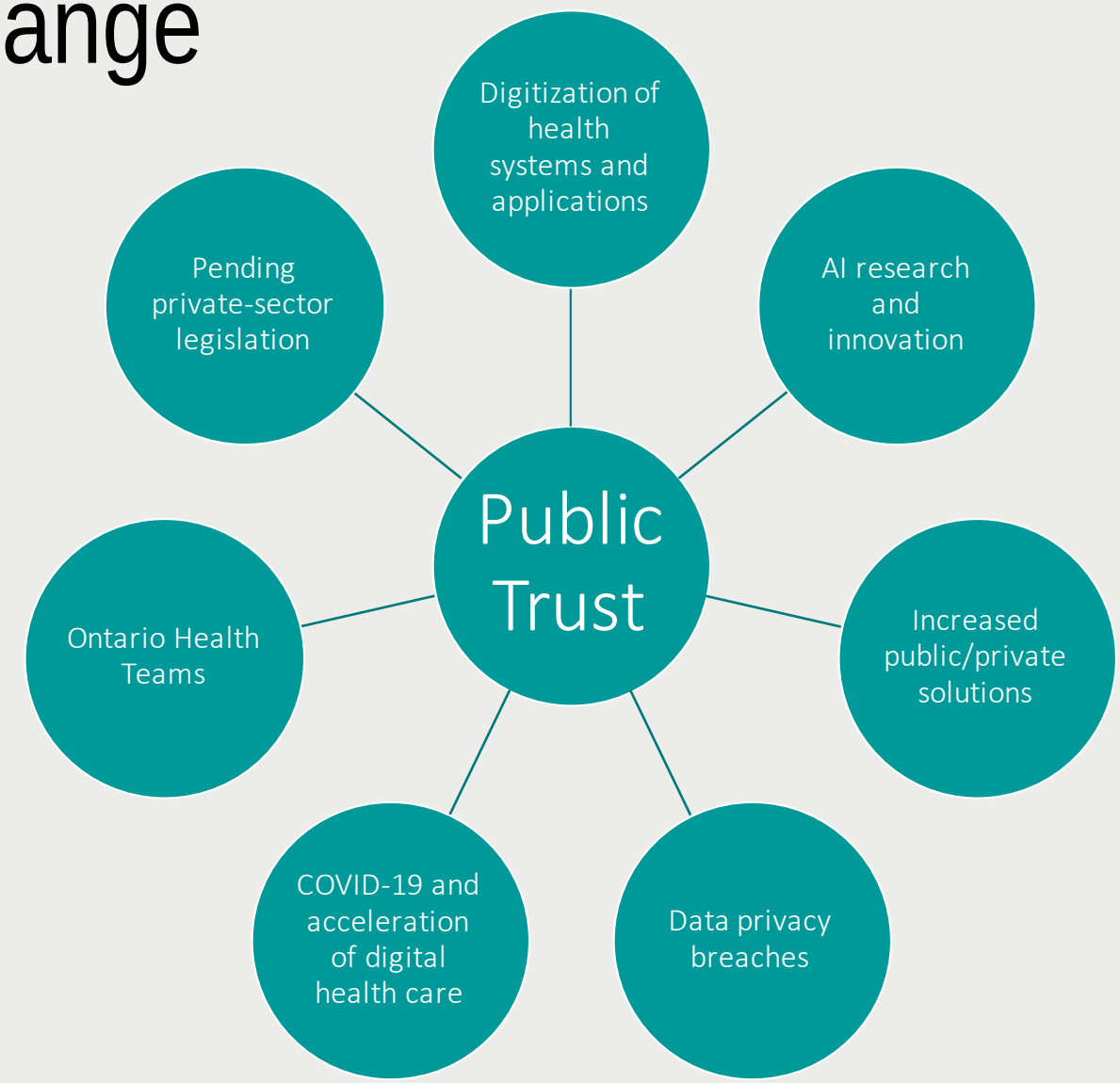
Alliance for Healthier Communities

September 22, 2020

Overview

- Drivers of Change
- *PHIPA* Amendments
  - Administrative penalties and offences
  - Regulation of de-identified information
  - Access to records in electronic format
  - Requirement to maintain an electronic audit log
  - Interoperability requirements
- Privacy and Security in Virtual Care
  - Key *PHIPA* provisions
  - Policy
  - Training and privacy breach management
  - Email
  - Videoconferencing

Drivers of Change



PHIPA AMENDMENTS

Introduction to *PHIPA* Amendments

- Since 2019, the Ministry of Health has been seeking to "modernize" the *Personal Health Information Protection Act* (*PHIPA*)
- This process has resulted in amendments to *PHIPA* in:
  - *Bill 138, Plan to Build Ontario Together Act, 2019*
  - *Bill 188, Economic and Fiscal Update Act, 2020*
- Some amendments are in force and some are not
- This has also resulted in changes and proposed changes to the regulation to *PHIPA*

Introduction to *PHIPA* Amendments, cont'd

- 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 Information and Privacy Commissioner of Ontario (IPC) to issue an order requiring a person who has contravened *PHIPA* or its regulation to pay an administrative penalty
- The IPC is the first Canadian privacy commissioner to have this power
- 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
  - As these regulations have not yet been 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 (in force as of July 31, 2020)
    2. Bill 138 also created an offence for willfully contravening this prohibition on the use of de-identified information to re-identify an individual (in force as of July 31, 2020)
    3. Bill 188 amended the definition of "de-identify" to enable requirements to be prescribed for how personal health information is to be de-identified (not yet in force)

Access to records in electronic format

- 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 health information 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 personal health information in an electronic format that meets prescribed requirements (in force but has no effect because no requirements have been prescribed)
    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, 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 personal health information, 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

Requirement to maintain an electronic audit log

- The IPC has held that electronic audit logs must be maintained and monitored by custodians to detect and deter unauthorized access to personal health information
- This obligation flows from the requirement in *PHIPA* for custodians to take reasonable steps to protect personal health information, for example, against theft, loss and unauthorized use or disclosure
- Bill 188 clarified this obligation by specifically requiring that custodians maintain and monitor an electronic audit log of accesses to personal health information, subject to prescribed exceptions, and to provide that log to the IPC upon request
- These provisions are not yet in force and exceptions, if any, have not yet been prescribed

Interoperability requirements

- There is an increasing concern that personal health information in electronic form cannot be easily communicated between electronic systems (e.g. hospital information systems, electronic medical records)
- To address this concern, Bill 138 amended *PHIPA* to add regulation-making authorities governing electronic interoperability requirements
- The government further posted proposed regulations for public comment, along with an associated policy document

Interoperability requirements, cont'd

- The proposed regulatory scheme would authorize Ontario Health to set and publish interoperability specifications
- Interoperability specifications may be made at the direction of the Minister of Health and must be approved by the Minister to be effective
- Custodians will be required to ensure that their electronic systems comply with applicable interoperability specifications
- Ontario Health would have the ability to monitor compliance
- If a custodian does not comply, this regulation would be enforced through a complaint to the IPC

Interoperability requirements, cont'd

- The IPC made a submission on the proposed regulations
- The IPC generally supports the goal of increased interoperability, but recommended amendments to:
  - Require broader and earlier consultation with the IPC on the content of interoperability specifications
  - Make it easier for Ontario Health to monitor compliance
  - More comprehensively regulate private sector entities accessing the digital personal health information of Ontarians
- These proposed regulations have not yet been finalized and brought into force

PRIVACY AND SECURITY IN VIRTUAL CARE

Introduction to Virtual Care

- Virtual care can include a combination of email (messages and/or photos), telephone consultation, and live videoconferencing
- *PHIPA* applies to virtual care as it does to in-person care
- Health information custodians must comply with *PHIPA* when communicating with patients or clients and when communicating with other agents or custodians about these patients or clients
- Although virtual care can be advantageous for both providers and patients or clients, it raises an additional set of privacy and security concerns
- For example, there is the risk that information could be intercepted by an unauthorized third party or inadvertently misdirected, which may result in the unauthorized disclosure of personal health information

Key *PHIPA* Provisions

Electronic service providers (s. 10(4) and O. Reg. 329/04 s. 6)

- *PHIPA* requires electronic service providers who are not agents of the health information custodian to comply with the following prescribed requirements:
  - Must not use any personal health information to which it has access in the course of providing services for the custodian except as necessary in the course of providing the services
  - Must not disclose any personal health information to which it has access in the course of providing services for the custodian
  - Must not permit its employees or any person acting on its behalf to be able to have access to the information unless the employee or person acting on its behalf agrees to comply with the restrictions

Key *PHIPA* Provisions, cont'd

Health Information Network Providers (HINPs) (O. Reg. 329/04 s. 6(2) and (3))

- 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 electronic service provider that is subject to additional obligations

Key *PHIPA* Provisions, cont'd

Security of personal health information (s. 12)

- Custodians must take steps that are reasonable in the circumstances to ensure that:
  - personal health information is protected against theft, loss and unauthorized use or disclosure
  - records of personal health information are protected against unauthorized copying, modification and disposal

Handling of records (s. 13)

- *PHIPA* requires health information custodians to ensure that records of personal health information are retained, transferred and disposed of in a secure manner

Key *PHIPA* Provisions, cont'd

Data minimization (s. 30)

- Custodians must not collect, use or disclose:
  - personal health information if other information will serve the purpose
  - more personal health information than is reasonably necessary to meet the purpose

Policy

- Custodians should develop and implement a written policy applicable to virtual care
- The policy should address when and how care may be provided virtually, any conditions or restrictions on doing so, and what administrative, technical and physical safeguards will be implemented
- Principle of least privilege: agents should have access to only the minimum amount of personal health information necessary to perform their job duties

Training and Privacy Breach Management

Training and Education

- Comprehensive privacy and security training is essential for reducing the risk of unauthorized collection, use and disclosure of personal health information

Privacy Breach Management

- Custodians are expected to have a privacy breach management protocol in place that identifies the reporting, containment, notification, investigation and remediation of actual and suspected privacy breaches
- See the IPC's *Responding to a Health Privacy Breach: Guidelines for the Health Sector*

Emails between custodians and patients and clients

Custodians must implement technical, physical and administrative safeguards to protect personal health information. For example:

- Firewalls and anti-malware scanners (technical safeguard)
- Keeping portable devices in secure location (physical safeguard)
- Using professional—not personal—email accounts (administrative safeguard)

Emails between custodians and patients and clients, cont'd

Where feasible, custodians should use encryption for communicating with their patients. Where it is not feasible, custodians should determine whether it is reasonable to communicate through unencrypted email, including by considering:

- Are there alternative methods?
- How sensitive is the personal health information to be communicated?
- How much and how frequently will personal health information be communicated?

See the IPC's *Fact Sheet: Communicating Personal Health Information by Email*

Videoconferencing: Planning

- Determine if videoconferencing is the appropriate method in the circumstances:
  - Will the provider be able to meet the necessary standard of care?
  - Will the provider be able to uphold their obligation to protect the privacy of the patient or client's personal health information?
- Choose a videoconferencing tool/platform with sufficient security safeguards, such as:
  - End-to-end encryption
  - Two-factor authentication
  - Most recent software updates have been applied

Videoconferencing: Preparation

- Place your device in a private location, and ensure that the patient or client is able to place their own device in a private location
- Use a secure internet connection, rather than, for example, a free public wireless connection
- Check the meeting settings:
  - Ensure that participants cannot enter the meeting without the moderator's permission
  - Record the meeting only if necessary and only with the patient or client's consent to do so

Videoconferencing: During the meeting

- If there are others present, ensure that the patient or client consents to their presence during the virtual visit
- Use headphones rather than speakers for increased privacy
- Communicate a back-up plan in case the video connection fails

Other obligations and resources

- Document the virtual visit in the same manner as an in-person visit. The same record retention and access requirements also apply.
- Be aware of any policies the applicable regulatory college has published (e.g. the College of Physicians and Surgeons of Ontario's Telemedicine policy)
- Consider resources such as the Ontario Telemedicine Network's Privacy Toolkit
- Prepare to consider how the regulations, once made, regarding
  - consumer electronic service providers and
  - interoperability specifications

  might apply to the virtual provision of health care

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