Privacy Best Practices - Lessons from Ontario

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

Professional Regulation and Discipline

Infonex

April 10, 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. Manual For The Review And Approval Of Prescribed Persons And Prescribed Entities
3. Responding to a Privacy Breach

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* (*PHIPA*)

Information and Privacy Commissioner (IPC) (cont')

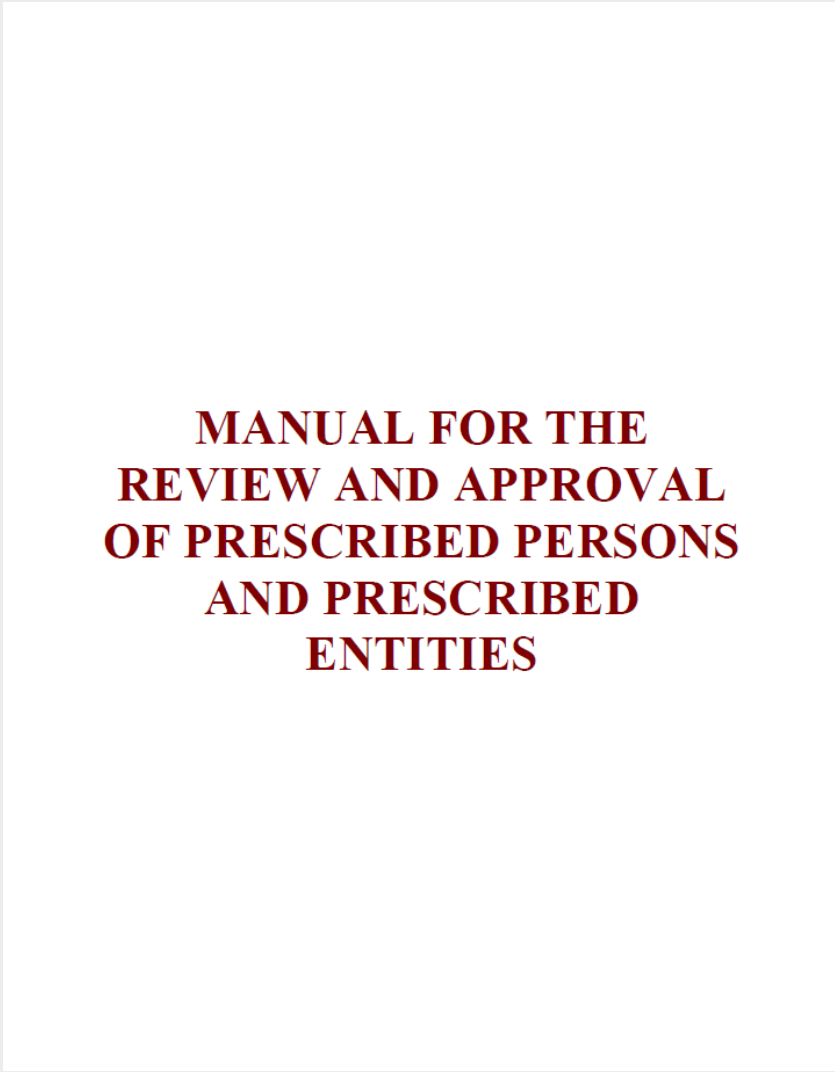
- But now there are more acts (some are in force and some are not in force) with an oversight role for the IPC, including
  - *Child, Youth and Family Services Act, 2017*
  - *Anti-Racism Act, 2017*

Manual For The Review And Approval Of Prescribed Persons And Prescribed Entities

Review and Approval of Prescribed Persons and Prescribed Entities

- Under *PHIPA*, the IPC is required to review the practices and procedures of prescribed entities and prescribed persons every three (3) years
- This applies to organizations such as Cancer Care Ontario, the Institute for Clinical Evaluative Sciences, etc.
- The IPC publishes a manual (the Manual) that describes the documentation we expect prescribed entities and prescribed persons to have in place

https://www.ipc.on.ca/wp-content/uploads/2016/08/MANUAL-FOR-THE-REVIEW-AND-APPROVAL-OF-PRESCRIBED-PERSONS-AND-PRESCRIBED-ENTITIES.pdf



Review and Approval of Prescribed Persons and Prescribed Entities (Cont'd)

- The Manual provides a good overview of the minimum content of the documentation that should be part of a privacy program
- The minimum content required by the Manual is divided into 4 parts:
  - Privacy Documentation
  - Security Documentation
  - Human Resources Documentation
  - Organizational and Other Documentation

Privacy Documentation Includes

- General Privacy Policies, Procedures and Practices - an overarching privacy policy that describes legislative status and authorities
- Policies and procedures describing:
  - the purposes for which personal health information is collected, used, and disclosed
  - the types of personal health information collected, used and disclosed
  - who this information is collected from, or disclosed to
  - the legal authorities for these collections uses and disclosures

Privacy Documentation Includes (Cont'd)

- Lists of data holdings containing personal health information
- Policies and procedures regarding
  - data sharing agreements and agreements with third party service providers, including template agreements with minimum content
  - privacy impact assessments, and when they will be conducted
  - privacy breach management
  - responding to privacy complaints
  - privacy audits
- Policies and procedures on transparency and what information will be made available.

Security Documentation Includes

- Overarching information security policy requiring that reasonable steps be taken to ensure that personal health information is protected
- Policies and procedures regarding physical security describing
  - The physical safeguards implemented to control access to premises containing personal health information, such as locks, alarms, restricted or monitored access.
  - Granting and terminating access by agents
  - Theft, loss and misplacement of ID cards, access cards, and keys
  - Audits of agents with access to premises
  - Tracking visitors within premises

Security Documentation Includes (Cont'd)

- Policies and procedures for secure retention of records containing personal health information:
  - in paper and electronic format
  - on mobile devices
  - remote access
- Policies and procedures for secure transfer and disposal of personal health information
- Policies and procedures regarding security audits including threat and risk assessments, security reviews, vulnerability assessments, ethical hacks, etc.
- Information security breach management.

Human Resources Documentation Includes

- Policies and procedures regarding training agents, including
  - The time frame within which agents must receive initial privacy and security training (which must be before being given access to personal health information)
  - Ongoing annual privacy and security training
  - The minimum content of privacy and security training
  - The person responsible for providing privacy and security training
  - Logs tracking attendance at privacy and security training
- Agents must be required to comply with privacy and security policies and procedures and notify the prescribed person/ prescribed entity of a breach.

Human Resources Documentation Includes (Cont'd)

- Policies and procedures for having agents execute confidentiality agreements, including
  - confidentiality agreements must be executed before being given access to personal health information and annually thereafter
  - template confidentiality agreements
  - tracking who has executed confidentiality agreements
- Job descriptions for positions managing privacy and security programs day-to-day
- What happens on termination/cessation
- Discipline and correction action

Organizational and Other Documentation Includes

- Privacy and Security Governance and Accountability Framework:
  - who has day-to-day authority to manage privacy and security program
  - reporting relationship with CEO/Executive Director (who must be ultimately accountable) and required updates to Board of Directors
- Corporate Risk Management Framework to address privacy and security risks
- Tracking recommendations from PIAs, security audits, etc.
- Business Continuity and Disaster Recovery Plan

Responding to a privacy breach

Responding to a Privacy Breach

Step 1: Immediately implement privacy breach protocol, including

- Notify all relevant staff of the breach
- Develop and execute a plan designed to contain the breach and notify those affected
- Report the matter to the IPC (if applicable)

Responding to a Privacy Breach

Step 2: Stop and contain the breach, including

- Identify the scope of the breach and take the necessary steps to contain it, including:
  - Retrieve and secure any personal information/personal health information that has been disclosed
  - Ensure that no copies of the personal information/personal health information have been made or retained by the individual who was not authorized to receive the information
  - Determine whether the privacy breach would allow unauthorized access to any other personal information/personal health information and take the necessary steps, such as changing passwords, identification numbers and/or temporarily shutting your system down

Responding to a Privacy Breach

Step 3: Notify those affected by the breach, including

- Notify those individuals whose privacy was breached at the first reasonable opportunity
- When notifying individuals affected by a breach:
    - Provide details of the breach, including the extent of the breach and what personal information/personal health information was involved
    - Advise of the steps you are taking to address the breach and that they are entitled to make a complaint to the IPC (if applicable). If you have reported the breach to the IPC, advise them of this fact
    - Provide contact information for someone within your organization who can provide additional information and assistance

Responding to a Privacy Breach

Step 4: Investigation and remediation, including

- Conduct an internal investigation, including:
  - Ensuring that the immediate requirements of containment and notification have been met
  - Reviewing the circumstances surrounding the breach
  - Reviewing the adequacy of your existing policies and procedures in protecting personal information/personal health information
  - Ensuring all staff are appropriately educated and trained

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