Data Governance: A Regulator's Perspective

Sandra Ferguson

Director, Policy

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Infonex

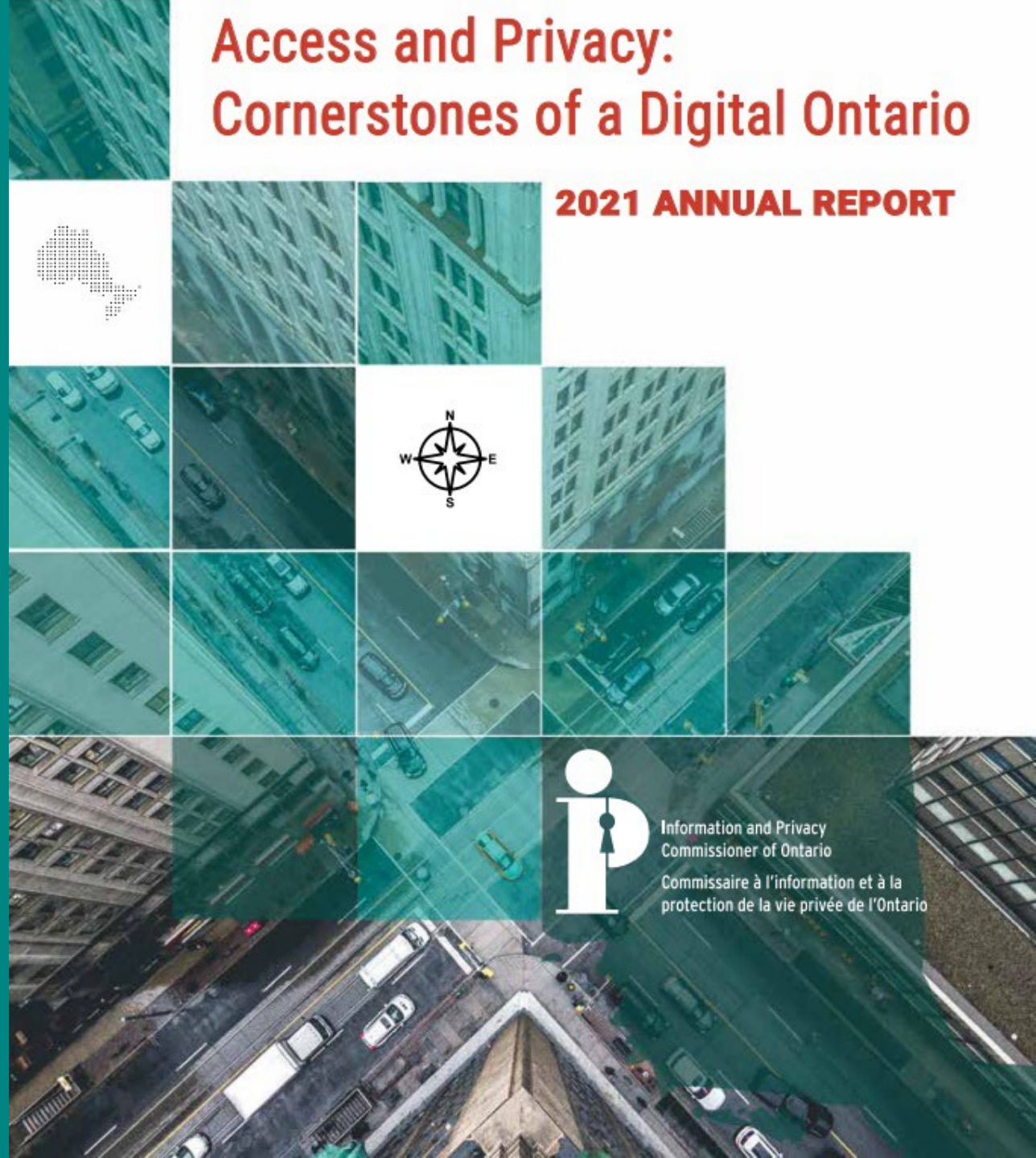
Data Governance for the Public Sector

Nov. 9, 2022

Introduction

About the IPC

- Oversees Ontario's access and privacy laws
- These laws establish the public's right to access government-held information and protect their personal privacy rights
- The IPC provides independent review of government decisions and practices on access and privacy
- Commissioner appointed by, reports to, Legislative Assembly to ensure impartiality



IPC's mandate

- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - covers 300 provincial institutions
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - covers 1,200 municipal organizations
- *Personal Health Information Protection Act* (*PHIPA*)
  - covers individuals and organizations involved in the delivery of health care services
- *Child, Youth and Family Services Act* (Part X) (*CYFSA*)
  - children's aid societies, child/youth service providers
- *Anti-Racism Act (ARA)*
  - oversight of the privacy protective rules

Three-Pronged Vision

- Working with relevant partners to enhance Ontarians' trust that their access and privacy rights are being respected

  - **Accountability**: maintaining the organizational excellence and accountability of the IPC
  - **Advocacy**: actively advancing Ontarians' rights in key strategic areas that impact their lives
  - **Responsiveness**: responding to complaints and appeals in a fair, timely, and meaningful manner

IPC VISION

Enhance Ontarians' trust that their access and privacy rights will be respected by ...

APRIL 2021

IPC Strategic Priorities 2021–2025

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

Privacy and Transparency in a Modern Government

Advance Ontarians' privacy and access rights by working with public institutions to develop bedrock principles and comprehensive governance frameworks for the responsible and accountable deployment of digital technologies.

Trust in Digital Health

Promote confidence in the digital health care system by guiding custodians to respect the privacy and access rights of Ontarians, and supporting the pioneering use of personal health information for research and analytics to the extent it serves the public good.

Children and Youth in a Digital World

Champion the access and privacy rights of Ontario's children and youth by promoting their digital literacy and the expansion of their digital rights while holding institutions accountable for protecting the children and youth they serve.

Accessibility & Equity

Collaboration & Consultation

Vision & Pragmatism

Knowledge Development

Next-Generation Law Enforcement

Contribute to building public trust in law enforcement by working with relevant partners to develop the necessary guardrails for the adoption of new technologies and community based approaches that protect both public safety and Ontarians' access and privacy rights.

Investigations

Investigations – The "Trilogy"

Use of cloud-based educational services by Ontario school boards:

1. MC18-48 – Security of attendance reporting platform (13 Apr 2021)

2. MC17-52 – Use of Google G-Suite for Education (23 Jul 2021)

3. MC18-17 – Use of third-party apps (7 Feb 2022)

Full text of these decisions available at:
www.ipc.on.ca/decisions

Cont'd

Investigations – The "Trilogy"

- Three privacy complaint investigations involving Ontario school boards' use of online educational services.
- Investigations differed in important ways, but all involved:
  - procurement and use of cloud-based services of third-party private-sector service providers acting as agents
  - direct access and use by students of online, account-based services
  - Parent concerns about improper collection, use and disclosure of students' personal information

The Trilogy and Data Governance

- IPC investigators found school boards broadly in compliance with MFIPPA, but made recommendations to address some deficiencies, notably to:
  - improve transparency of information management practices, including enhanced notices of collection
  - establish clear privacy and security requirements, consistent with MFIPPA obligations, when contracting online educational services
  - ensuring privacy and security requirements in contracts are kept up to date, and enforced

PHIPA Decision 175

Issue 4: Did the custodian take reasonable steps to protect the PHI at issue?

Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PHIPA DECISION 175

HI19-00007

A Group of Medical Clinics and Related Entities

March 25, 2022

Summary: This investigation file was opened following the publication of a Toronto Star article in 2019 (the Article). The Article reported that a company that sells and supports electronic medical record software in primary care practices in Ontario, was anonymizing health data and selling the data to a third party corporation. In response to the article, the Office of the Information and Privacy Commissioner of Ontario commenced a review under the *Personal Health Information Protection Act* (the *Act*) and sought to identify the individual or entity who allegedly de-identified and sold the data.

The corporation that was identified as having sold the information was named as a respondent in this investigation and a number of other respondents were also added, one of which was identified as the health information custodian.

This Decision concludes that the act or process of de-identifying personal health information is a "use" within the meaning of section 2 of the *Act*, and that the use of personal health information for the purpose of de-identification is permitted without the consent of the individual, where the conditions set out under subsection 37(1)(f) of the *Act* are met. At the time of this investigation, the health information custodian's written public statement about its information practices did not comply with section 16(1)(a) of the *Act*. However, this issue has since been remedied and the custodian's updated privacy policy now meets the requirements of the *Act* by explicitly describing its practice of de-identifying personal health information and selling the information to a third party for a number of purposes, including for health-related research. With regard to the de-identified personal health information, the custodian has complied with subsection 12(1) of the *Act*, in that reasonable steps have now been taken to ensure the protection of personal health information by amending the sale agreement to include additional privacy and security controls.

Consultations

Policy Consultations

Considering a consultation with the IPC? We encourage you to reach out!

Protecting privacy, safeguarding information, and providing access to information can be challenging, especially in a quickly evolving digital world.

As one of our stakeholders, you might be seeking feedback or guidance on new programs, projects, technologies, or processes that you are considering. To the extent our resources permit and subject to our discretion, we would be pleased to offer comment on the privacy and transparency implications of proposed legislative schemes and government programs or the information practices of custodians and children service providers.[1] Through consultation, the IPC can provide meaningful comments and general guidance to help you manage privacy and information security risks. We can also direct you to resources to help you safeguard information and better understand your obligations under the applicable access and privacy laws.

Our office oversees compliance with **several provincial laws**, which protect the access and privacy rights of Ontarians. These laws include the:

- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
- *Personal Health Information Protection Act* (*PHIPA*)
- Part X of the *Child, Youth, and Family Services Act* (*CYFSA*)
- *Anti-Racism Act* (*ARA*)

www.ipc.on.ca/about-us/policy-consultations/

What We Look For in a Consultation

- *What information will be collected? By whom? From whom?*
- *How will the information be used and for which purposes?*
- *To whom will the information be disclosed (or shared) and for what purposes?*
- *How will the information flow through the proposed program, project, technology, or process you are considering?*
- *How is the information being protected at each step?*
- *Are you or another organization performing each step within the data flow, and under what authority?*
- *How are individuals being notified about the process? How can they exercise their rights, such as to access their information?*

Guidance

De-Identification (and other privacy enhancing technologies)

***Governance question**: Now that you've de-identified data, how will you keep it that way?*

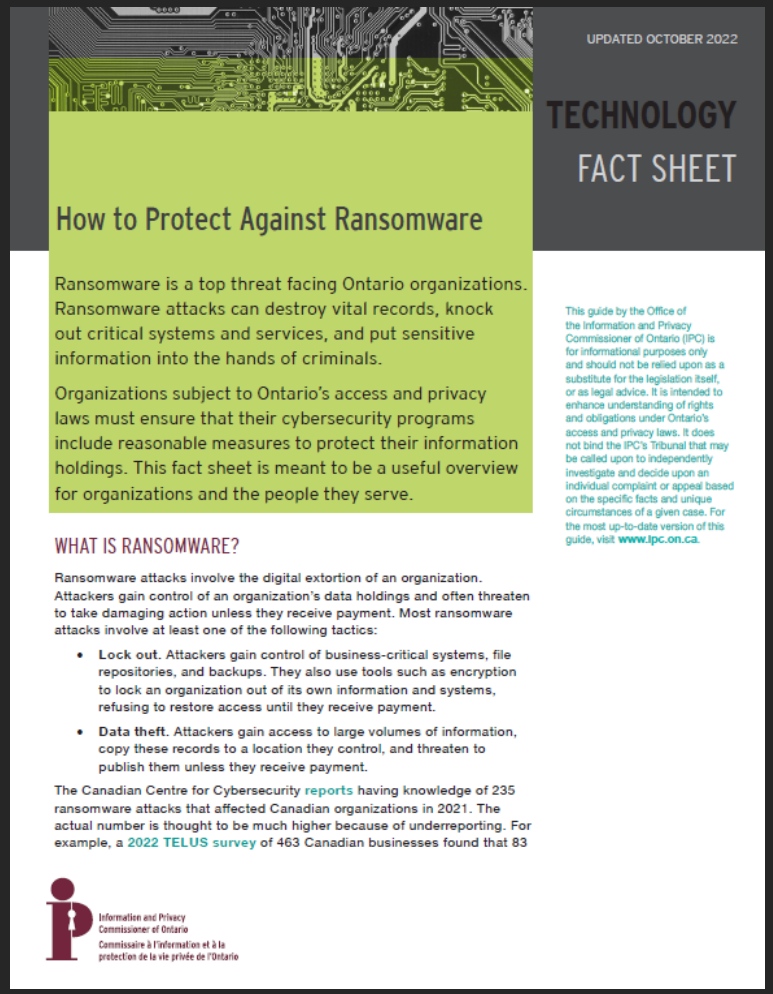
De-identification Guidelines for Structured Data

June 2016

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Ransomware



UPDATED OCTOBER 2022

TECHNOLOGY FACT SHEET

How to Protect Against Ransomware

Ransomware is a top threat facing Ontario organizations. Ransomware attacks can destroy vital records, knock out critical systems and services, and put sensitive information into the hands of criminals.

Organizations subject to Ontario's access and privacy laws must ensure that their cybersecurity programs include reasonable measures to protect their information holdings. This fact sheet is meant to be a useful overview for organizations and the people they serve.

This guide by the Office of the Information and Privacy Commissioner of Ontario (IPC) is for informational purposes only and should not be relied upon as a substitute for the legislation itself, or as legal advice. It is intended to enhance understanding of rights and obligations under Ontario's access and privacy laws. It does not bind the IPC's Tribunal that may be called upon to independently investigate and decide upon an individual complaint or appeal based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guide, visit **www.ipc.on.ca**.

WHAT IS RANSOMWARE?

Ransomware attacks involve the digital extortion of an organization. Attackers gain control of an organization's data holdings and often threaten to take damaging action unless they receive payment. Most ransomware attacks involve at least one of the following tactics:

- **Lock out.** Attackers gain control of business-critical systems, file repositories, and backups. They also use tools such as encryption to lock an organization out of its own information and systems, refusing to restore access until they receive payment.
- **Data theft.** Attackers gain access to large volumes of information, copy these records to a location they control, and threaten to publish them unless they receive payment.

The Canadian Centre for Cybersecurity reports having knowledge of 235 ransomware attacks that affected Canadian organizations in 2021. The actual number is thought to be much higher because of underreporting. For example, a 2022 TELUS survey of 463 Canadian businesses found that 83

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

***Governance question**: What processes are in place to ensure confidentiality, integrity and availability of key information?*

FPT Joint Resolution – Secure Communications in Health Care

***Governance question**: Have you identified the weak spots in your policies and procedures?*

Securing Public Trust in Digital Healthcare

Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombudspersons with Responsibility for Privacy Oversight

September 21, 2022

Context

1. Canada's health sector continues to experience serious resource constraints and staff shortages, aggravated by more than two years of surges in demand for emergency care brought on by the ongoing COVID-19 pandemic.
2. These and other complex problems facing the health sector during the pandemic have spurred innovation and change in the delivery of services, including through virtual care visits and other forms of digital health communications.
3. However, despite these rapid digital advancements in the health sector, breaches continue to be caused by the use of insecure communication technologies such as traditional fax [1] machines and unencrypted emails, unauthorized access to health records by employees (often in the form of 'snooping'), and cybersecurity attacks (including ransomware).
4. Personal health information is one of the most sensitive types of information about an individual. Data breaches in the health sector can cause significant harm to affected individuals, including potential discrimination, stigmatization, financial and psychological distress.

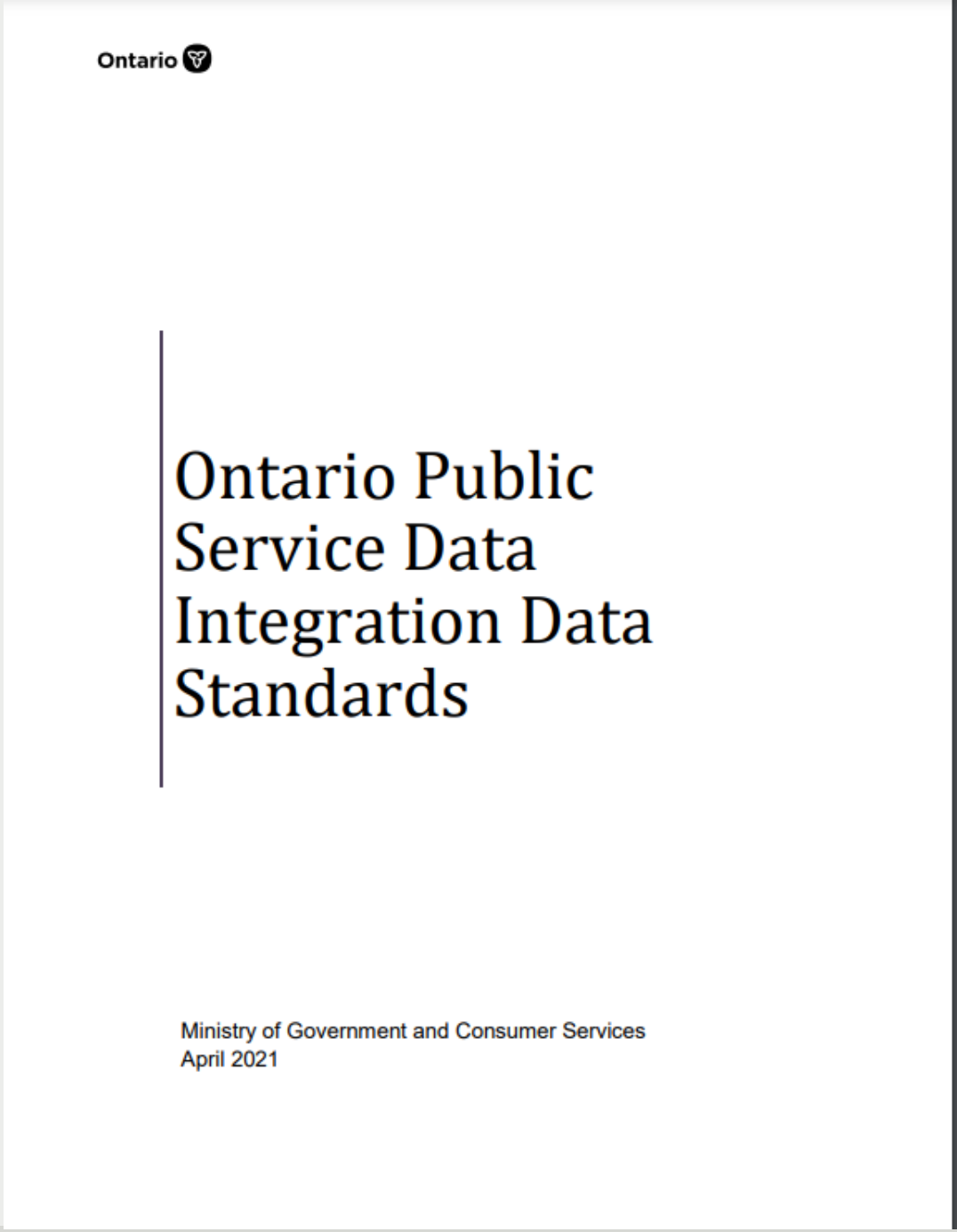
Legislation

Introduction to the Data Integration Framework

- Part III.1 of *FIPPA* enables prescribed data integration units to collect personal information for linking to create and enable access to de-identified datasets for the purpose of analysis in relation to:
  - the management or allocation of resources;
  - the planning for the delivery of programs and services provided or funded by the Government of Ontario; and
  - the evaluation of those programs and services.
- Currently, 6 prescribed Ministry Data Integration Unit and 3 prescribed Inter-Ministerial Data Integration Units (IMDIUs)
  - To date, IPC has reviewed and approved one IMDIU, and a second review is underway

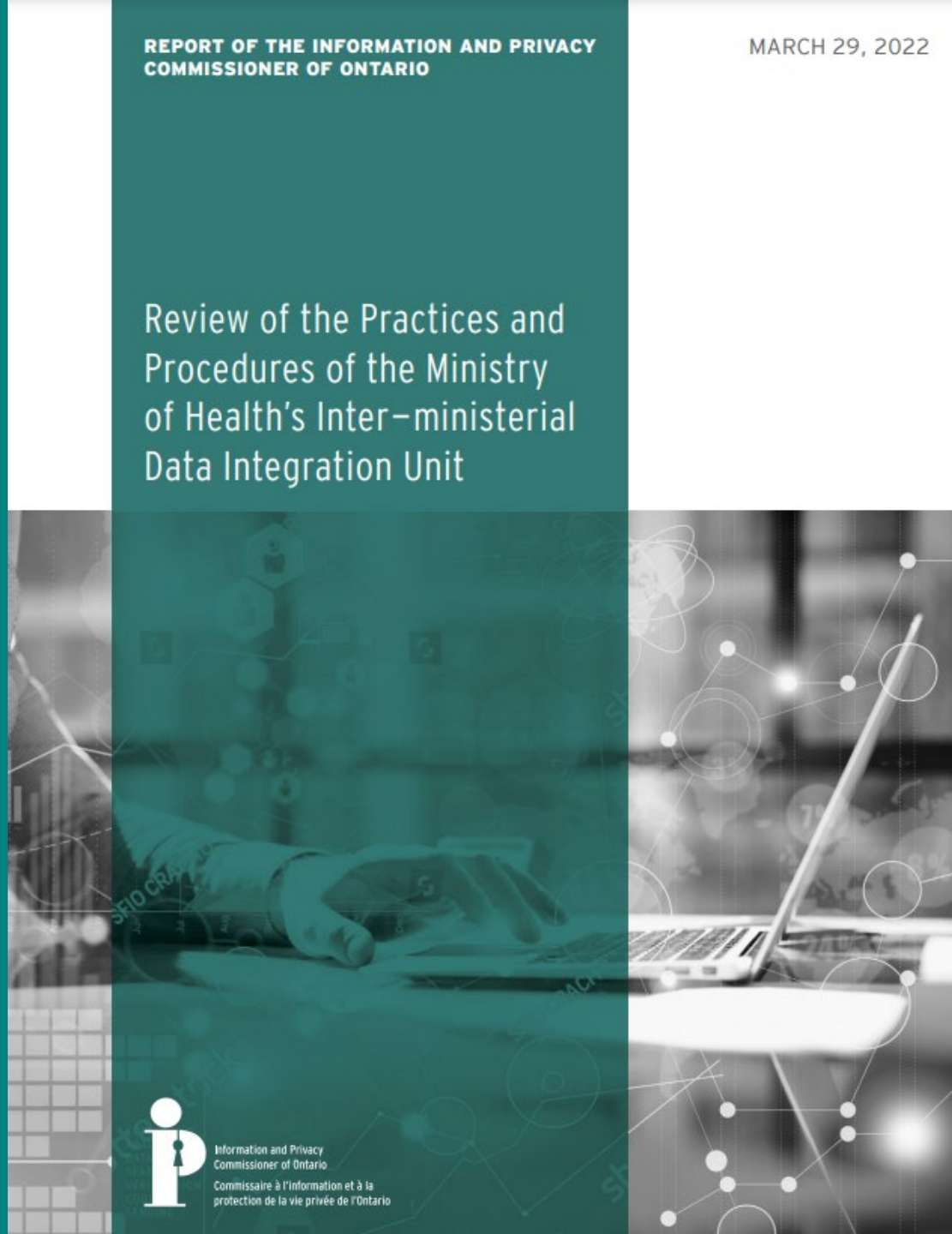
The Data Standards

- Approved by the IPC in 2021
- 27 requirements across 7 categories:
  - General requirements
  - Collection, use and disclosure
  - Secure retention and transfer
  - Secure disposal and secure destruction
  - Retention period
  - De-identification and linkage
  - Public notice and annual reporting



The IMDIU Experience

***Governance question**: Could a new staff person pick up your policies and procedures and know what has to be done to meet them?*



Conclusion / Takeaways

HOW TO 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