Regulating the Use of Personal Health Information in Big Data Research

Joshua Shaw, LL.M. J.D.

Health Privacy Policy Analyst
Health Policy Department
Office of the 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

Clinical Trials Ontario's 2018 Annual Conference

March 28, 2018

Who is the Information and Privacy Commissioner of Ontario?

- IPC/O is appointed by the Legislative Assembly of Ontario and provides independent review of decisions and practices of:
  - government and
  - organisations and individuals involved in health care sector

  that affect access to information and privacy.
- Mandate includes:
  - public education and publication of guidance,
  - consultations with government or organisations on legislative or policy initiatives,
  - investigation, mediation, and adjudication of privacy complaints or decisions to refuse access to information,
  - review of the practices and procedures of certain entities or organisations.

Ontario's Legislative Framework

Public Sector	Health Sector	Private Sector
Government e.g. ministries, agencies, hospitals, universities, cities, police, schools, hydro *Freedom of Information and Protection of Privacy Act* (*FIPPA*) *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)	Individuals, organisations delivering health care e.g. hospitals, pharmacies, labs, doctors, dentists, nurses *Personal Health Information Protection Act* (*PHIPA*)	Private sector businesses engaged in commercial activities *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)
IPC/O oversight	IPC/O oversight	Privacy Commissioner of Canada oversight

Big data trends in the province

- Governments want to **share, link, analyse data** across agencies to obtain new insights, to support
  - policy development
  - system planning
  - resource allocation
  - performance monitoring.
- Big data analysis is sometimes called **data integration.**
- Benefits of big data may be compelling. For example:
  - higher quality evidence
  - better public policy
  - better use of money
  - fraud detection.

Big data trends in the province

- There are risks involved in big data analysis, which include:
  - unexpected uses of personal information
  - invasive
  - inaccuracy in linkages or representativeness of samples
  - discriminatory.
- Big data analysis goes against expectation that governments and organisations collect personal information **directly** from individuals to whom the information relates, and the expectation that information is not shared with others except in limited circumstances.
- So far, legislative approaches to big data in Ontario have been piecemeal.
  - e.g., *Child, Youth, Family Services Act, 2017*

Regulatory approaches preferred by the IPC/O

- *FIPPA* treats government institutions as silos; indirect collection, sharing/linking across government not envisioned
- IPC/O maintains that big data analysis should occur within a **single dedicated unit**, to:
  - collect personal information across government
  - link records securely
  - de-identify
  - make de-identified data available to public bodies to inform policy and system planning.
- Modelled from approach in *PHIPA*, e.g., s. 55.9 in context of electronic health record systems.
- Allows institution to: (1) avoid **replicating databases** and creating **profiles** of sensitive personal information across government, (2) maximise security of personal information, including minimising and controlling access, and localising security infrastructure.

Regulatory approaches preferred by the IPC/O

- Centralised model has further advantages over decentralised system:
  - Allows for ethical review at outset, prior to big data analysis,
  - Facilitates an organisation's capacity to be transparent in its information practices (e.g., ensure public knowledge of purpose, methodology, algorithm)
  - Makes it easier for an independent regulator to oversee information practices (e.g., IPC/O, including order-making, audit, inspection powers)
  - Facilitates the use of expertise needed to carry out analysis and minimise privacy and security risks.
- IPC/O now in discussions with Ontario government about legislative reform.

Lessons for big data in *PHIPA* context

- Potential uses of big data analysis

1) for planning or delivering programs or services, **or** risk management, improving or maintaining the quality of care or the quality of a program or service. For example:
   - section 37(1)(c) – (d) [use by custodian],
   - section 39(1)(d)(iii) [disclosure to custodian who provided healthcare].
   - Section 39(1)(c) and 45(1) [disclosure by custodian to prescribed entity to analyse or compile statistical information with respect to managing, evaluating, allocating resources, or planning health system].
   - section 47(2) [disclosure by custodian to health data institute]
   - section 55.9 [collection by MOHLTC for planning analysis or detecting and preventing fraud]

- Centralised structures, de-identification, encryption, secure transfer and destruction, privacy policies and procedures and training, auditing and monitoring.

Lessons for big data in *PHIPA* context

- Potential uses of big data analysis

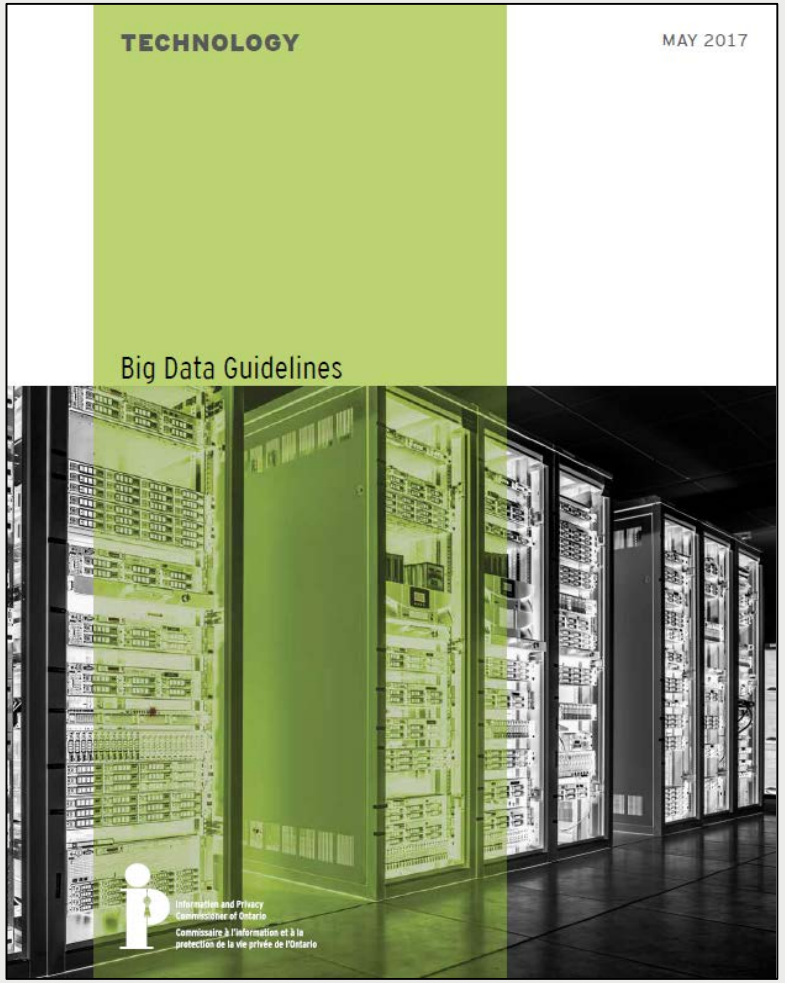
2) Research – in the sense of systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them.
    - sections 37(3) and 44.

- Follow conditions set out by REB process, follow limitations on further use and disclosure of identifying research data under *PHIPA*, limit and control access to identifying information with segregated or centralised organisational structures, de-identification, encryption, secure transfer and destruction, privacy policies and procedures and training, auditing and monitoring.

Lessons for big data in *PHIPA* context

- To minimise collection, use, and disclosure to what is directly relevant and necessary for achieving the specified purpose (section 30 of *PHIPA*), at a minimum, data elements collected or used in the course of analysis should be:
  - conceptually related to the subject-matter under study, and
  - directly informed by the question asked.
- All big data projects should be reviewed and approved by a REB, or a similar body where permitted under *PHIPA*.
- Describe projects with public notification on organisation's website.
- Consider privacy risks associated with publicly available personal information.
- Throughout data integration, analysis, and predictive profiling, organisations and researchers should work to minimise privacy and other ethical issues that arise, by following best practices issued by the IPC/O and any further limitations set by REB.

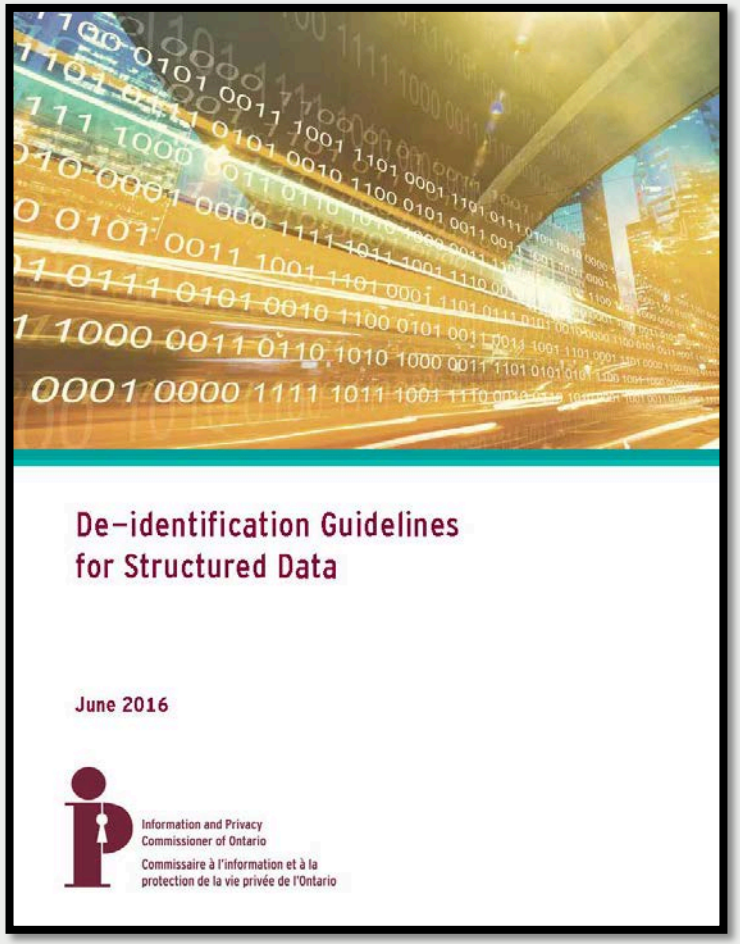
Big Data Guidance



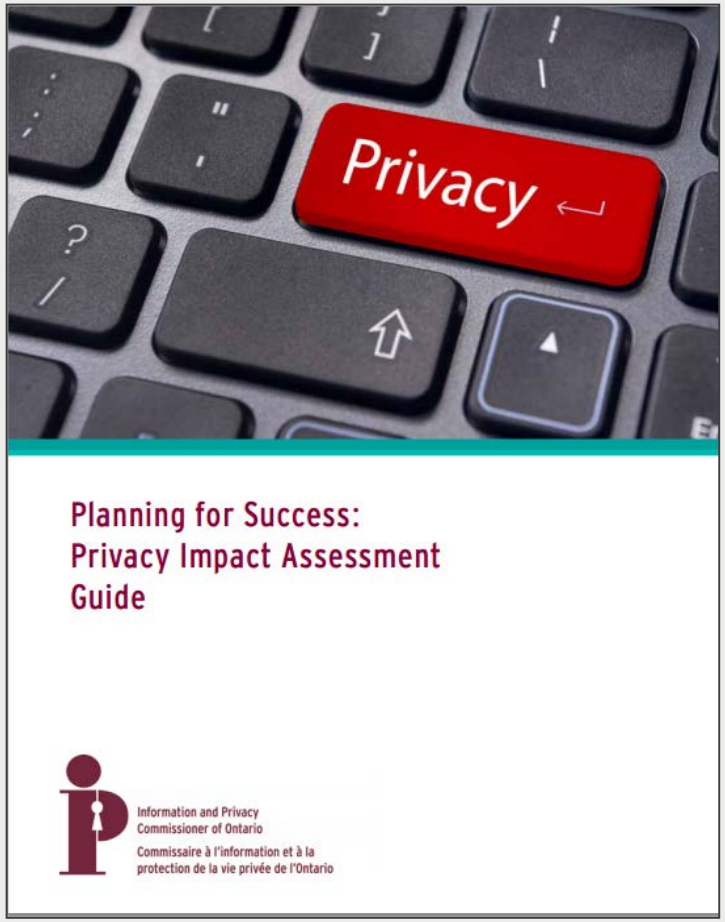
- Key issues, best practices when conducting big data projects involving personal information.
- Considerations at each stage:
  - collection
  - integration
  - analysis
  - profiling.

De-identification

- Risk-based, step-by-step process to assist organisations to de-identify.
- Key issues when publishing
  - release models
  - types of identifiers
  - re-identification attacks.
- IPC wins global privacy award for excellence in research [International Conference of Data Protection and Privacy Commissioners, Hong Kong 2017].



Planning for Success: Privacy Impact Assessment Guide



- Tools to identify privacy impacts and risk mitigation strategies.
- Step-by-step advice on how to conduct a privacy impact assessment
- Not required by legislation, but considered privacy best practice

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