IPC Update

David Goodis

Assistant Commissioner
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

Lexpert Privacy and Data Protection

November 27, 2018

Who is the Information and Privacy Commissioner?

- Brian Beamish appointed by Ontario Legislature (March 2015)
- 5 year term
- reports to the Legislature, not government or minister
- independent government "watchdog"

Ontario's legislative framework

Public sector	Health sector	Private sector
Freedom of Information and Protection of Privacy Act *FIPPA* **provincial institutions** (ministries, agencies, hospitals, universities) *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) **local bodies** (municipalities, police, school boards, hydro)	*Personal Health Information Protection Act* *PHIPA* **health care providers** (hospitals, pharmacies, laboratories, doctors, dentists, nurses)	*Personal Information Protection and Electronic Documents Act* *PIPEDA* **private sector** businesses engaged in **commercial activities**
IPC oversight	IPC oversight	Privacy Commissioner of Canada oversight

Mission and mandate

MISSION: We champion and uphold the public's right to know and right to privacy

MANDATE:

- resolve access to information appeals and privacy complaints
- review information practices of public and health sector organizations
- conduct research, deliver education and guidance on access and privacy issues
- comment on proposed legislation, programs and practices

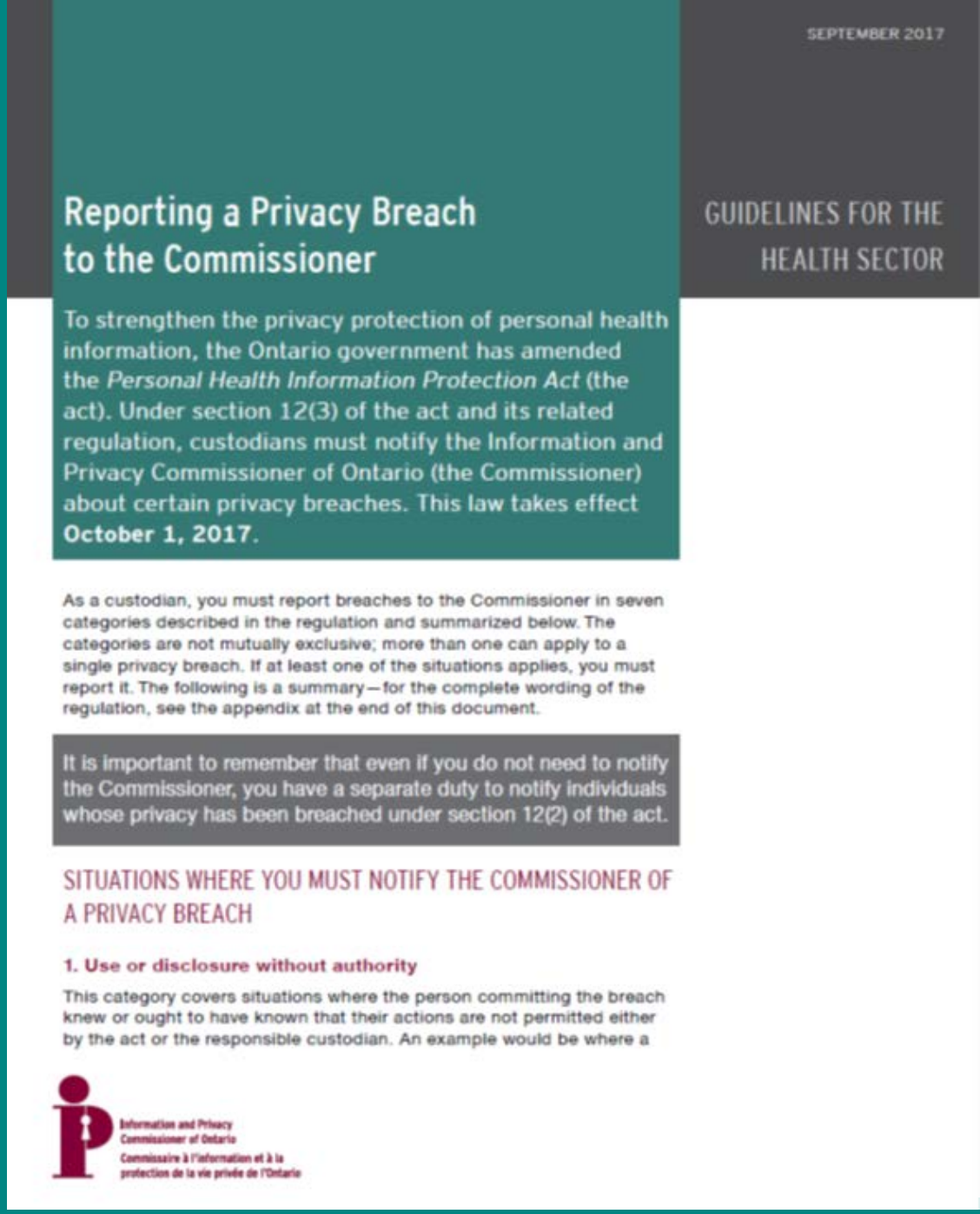
Update on personal health information

Breach reporting

- **mandatory breach reporting** to IPC [since October 2017]
- regulations prescribe what breaches must be reported
  - previously, health custodians must notify **affected individuals** if PHI stolen, lost, or used or disclosed without authority
  - now, custodians must also
    - notify **IPC** if theft, loss, unauthorized use or disclosure meets criteria in regulations ["significant breaches"]
    - give IPC annual statistical report of breaches

Breach reporting

- guidelines provide more detail about when a breach must be reported



SEPTEMBER 2017

Reporting a Privacy Breach to the Commissioner

GUIDELINES FOR THE HEALTH SECTOR

To strengthen the privacy protection of personal health information, the Ontario government has amended the *Personal Health Information Protection Act* (the act). Under section 12(3) of the act and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (the Commissioner) about certain privacy breaches. This law takes effect **October 1, 2017**.

As a custodian, you must report breaches to the Commissioner in seven categories described in the regulation and summarized below. The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, you must report it. The following is a summary—for the complete wording of the regulation, see the appendix at the end of this document.

It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

1. Use or disclosure without authority

This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

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

Breach reporting in 2018

- in 2018
  - 439 breaches reported to IPC by HICs from January-October
- compare to 2017
  - 324 breaches reported to IPC by HICs (includes three months of mandatory breach reporting, October-December)

Unauthorized access — “snooping”

- IPC continues to receive very high number of reports of these breaches, where staff
  - do not have consent of the individual
  - are not providing health care to the individual
- of the 439 breaches reported so far in 2018, 108 were snooping incidents
- why?
  - curiosity (family member, friend, famous person)
  - interpersonal conflicts (seeking information about an ex-spouse’s new partner)
  - financial gain (sale of data)

Rouge Valley: legal consequences of snooping

- 2013-2014, Rouge Valley Health System breaches
  - hospital employees accessed PHI of new mothers without authorization
  - used or sold mothers' names/contact info to sell RESPs to the mothers
- IPC investigates; Order HO-013 requires hospital to take several steps, including
  - ensure hospital can audit all access to electronic PHI
  - limit ability of staff to conduct open-ended searches
  - review/revise privacy policies and procedures
  - review/revise training tools, implement training policies, conduct privacy training for all staff
- in addition to IPC review, other legal proceedings relating to this breach

Legal consequences of snooping

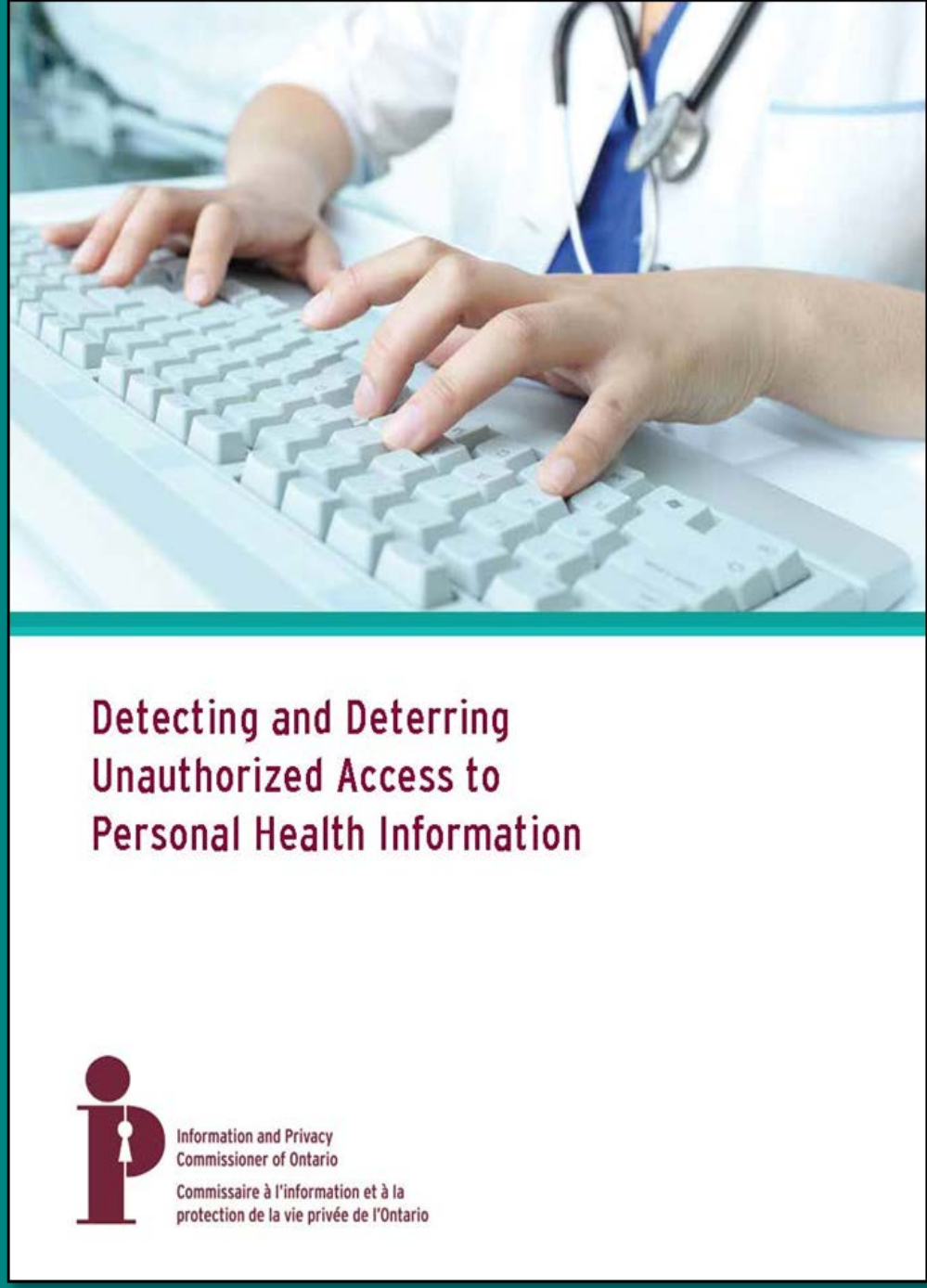
- *Securities Act* convictions
  - two RESP sales reps, hospital clerk convicted
  - two reps receive probation, community service, fines of $3,000 and $36,000, suspension of license
  - clerk receives probation, 300 hours community service, $36,000 fine
- *Criminal Code* convictions
  - secret commissions, using forged document
  - nurse, sales rep sentenced to 3 months' house arrest, 2 years' probation, community service
- professional discipline
  - Ontario College of Nurses disciplinary proceeding against nurse
  - she agrees to resign, not re-apply, appears before disciplinary panel for reprimand
- *Personal Information Protection and Electronic Documents Act*
  - Privacy Commissioner of Canada investigated, finds RESP dealer failed to ensure its sales rep complied with the act

Legal consequences of snooping

- **class action lawsuit** [*Broutzas v. Rouge Valley Health System*]
  - claims against hospital, hospital employees, RESP sales reps, RESP dealers for intrusion upon seclusion tort
  - certification motion dismissed by Ontario Superior Court of Justice (October 2018)
  - judge says 5 part test for certification not met
  - no factual basis for intrusion upon seclusion
    - contact info used and disclosed widely for a variety of purposes; little or no invasion of privacy when contact information alone is disclosed
    - also, fact of pregnancy not sufficiently confidential/sensitive
  - likely to be appealed?

Snooping guidance

- impact of unauthorized access
- how to reduce risk
  - policies and procedures
  - training
  - privacy notices and warning flags
  - confidentiality agreements
  - access management
  - logging, auditing, monitoring
  - privacy breach management
  - discipline



Reducing risk of privacy breaches - best practices

Administrative	Technical	Physical
• privacy and security policies • auditing compliance • privacy and security training • data minimization • confidentiality agreements (alone or part of broader contracts) • other ways to communicate privacy messages (privacy notices, warning flags) • PIAs	• strong authentication and access controls • detailed logging, auditing, monitoring • strong passwords, encryption • patch and change management • firewalls, hardened servers, intrusion detection and prevention, anti-virus, anti-spam, anti-spyware • protection against malicious and mobile code • threat risk assessments, ethical hacks	• controlled access to premises • controlled access to locations within premises where PI is stored • access cards and keys • identification, screening, supervision of visitors

NOTE – when determining appropriate safeguards consider

- sensitivity and amount of information
- number and nature of people with access to the information
- threats and risks associated with the information

What to do when faced with a privacy breach

- *PHIPA* sets out the rules that health information custodians must follow when collecting, using, disclosing, retaining and disposing of personal health information
- guidance to health information custodians when faced with a privacy breach

What happens when IPC reviews a breach?

- IPC may
  - ensure adequate containment, notification
  - interview appropriate individuals
  - review the organization's position on the breach
  - ask for status report of actions taken by the organization
  - review and give advice on current policies
  - report with recommendations (rarely order)

De-identification

- What is de-identification?
  - process of removing personal information from a record or data set
- Why is it important?
  - once de-identified, a data set is no longer personal information
- Where/how/when can it be useful?
  - research
  - integration of different government data sets in compliance with public sector privacy law
  - providing public access to government data sets (responding to access requests or through open data initiatives) while respecting individuals' privacy

De-identification guide

- IPC won global privacy award for excellence in research (International Conference of Data Protection and Privacy Commissioners, Hong Kong 2017)
- risk-based, step-by-step process to assist organizations to de-identify structured data

Other Recent Developments Of Note

Privacy oversight and regulation of political parties

- political parties not covered by privacy laws in Ontario, federally, or in most other provinces (except BC)
- Facebook/Cambridge Analytica matter highlighted how PI can be collected and used to target political messages (Brexit vote, 2016 US president election)
- IPC's 2017 Annual Report, recommend Ontario's political parties be subject to privacy regulation and oversight
- Commissioners in other provinces, and federal Privacy Commissioner have called for privacy oversight of political parties in their respective jurisdictions

Smart cities

- a community that uses connected technologies to collect and analyze data to improve services for citizens
  - energy conservation sensors that dim streetlights when not in use
  - parking apps that indicate nearest available public parking spot
  - garbage cans that send a signal when full

Privacy risks

- information may be collected by municipalities, private sector companies
- must ensure collection, use and disclosure is authorized (*MFIPPA/PIPEDA*)
- information must be safeguarded from cyberattack
- must ensure smart cities do not become infrastructures for mass surveillance

Minimize privacy risks

- strong safeguards can protect personal information
  - privacy impact and threat/risk assessments
  - data minimization
  - de-identified data
  - encryption
  - privacy and access governance
  - contracts with private sector partners that address ownership, control of data
  - community engagement and project transparency
- IPC working with municipalities and federal government
  - encourage transparency
  - ensure that privacy protections are built into smart city initiatives

Minimizing privacy risks in smart cities

- conduct PIAs/TRAs when designing new technologies and programs
- limit PI collection to what's necessary
- collect, use and retain de-identified data where possible
- obtain informed consent where required by law
- comprehensive data governance program, including
  - strong oversight of 3Ps
  - security and breach policies
- community engagement, communication, transparency

APRIL 2018

TECHNOLOGY FACT SHEET

Smart Cities and Your Privacy Rights

New technologies promise to help municipalities better manage urban environments and deliver services in a more effective and efficient way. They can help to make communities more liveable, sustainable, and fair. Many involve the collection and use of large amounts of information, including personal information. Cities or municipalities that use these connected technologies are often described as "smart cities."

This fact sheet was developed to help members of the public understand smart cities and how they can impact an individual's privacy

The Office of the Information and Privacy Commissioner of Ontario (IPC) provides independent oversight of the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*). This act protects the privacy of personal information by setting rules for its collection, use and disclosure by municipalities and municipal institutions. These rules also give individuals the right to access their own personal information.

The IPC has developed this fact sheet to help the public understand smart cities and how they can impact an individual's privacy.

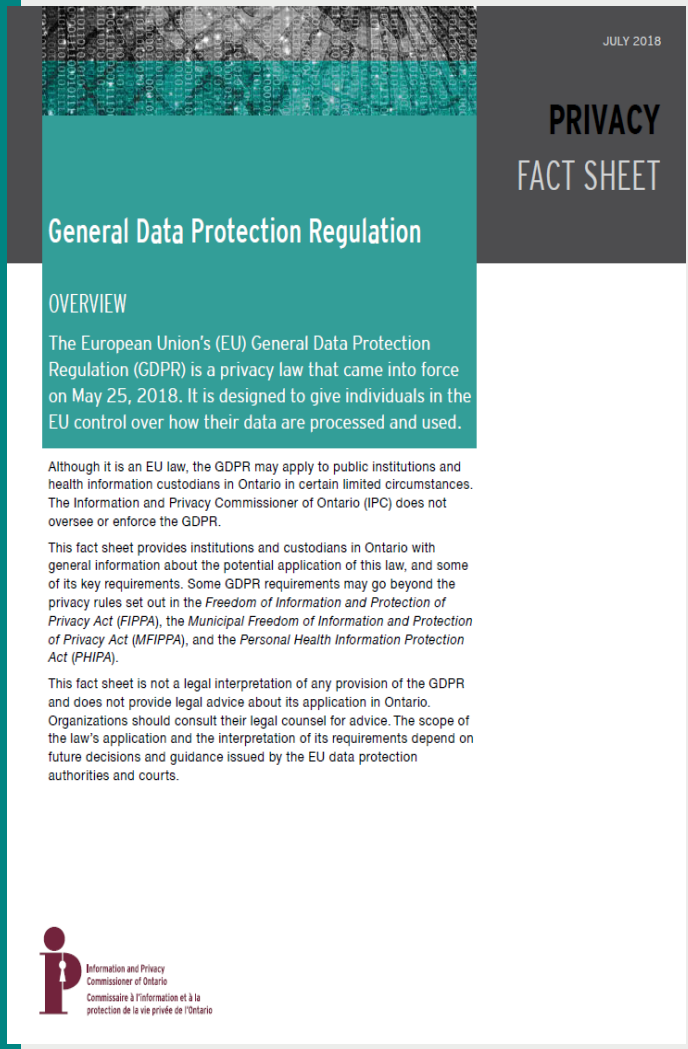
WHAT ARE "SMART" CITIES?

Smart cities use technologies that collect data to improve the management and delivery of municipal services, support planning and analysis, and promote innovation within the community. By collecting large amounts of data, often in real-time, municipalities can gain a greater understanding of the quality and effectiveness of their services. For example, commuter traffic flow data can identify congestion

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

Europe's General Data Protection Regulation (GDPR)

- basic guidance tailored to Ontario public institutions
- GDPR in effect May 2018
- applies to the collection, use and disclosure of personal data by organizations inside the EU
- may apply to organizations based in Ontario if they:
  - offer goods/services to individuals in EU
  - monitor behaviour of individuals in EU
- how the law is interpreted and applied will depend on EU data protection authorities and courts



JULY 2018

PRIVACY
FACT SHEET

General Data Protection Regulation

OVERVIEW

The European Union's (EU) General Data Protection Regulation (GDPR) is a privacy law that came into force on May 25, 2018. It is designed to give individuals in the EU control over how their data are processed and used.

Although it is an EU law, the GDPR may apply to public institutions and health information custodians in Ontario in certain limited circumstances. The Information and Privacy Commissioner of Ontario (IPC) does not oversee or enforce the GDPR.

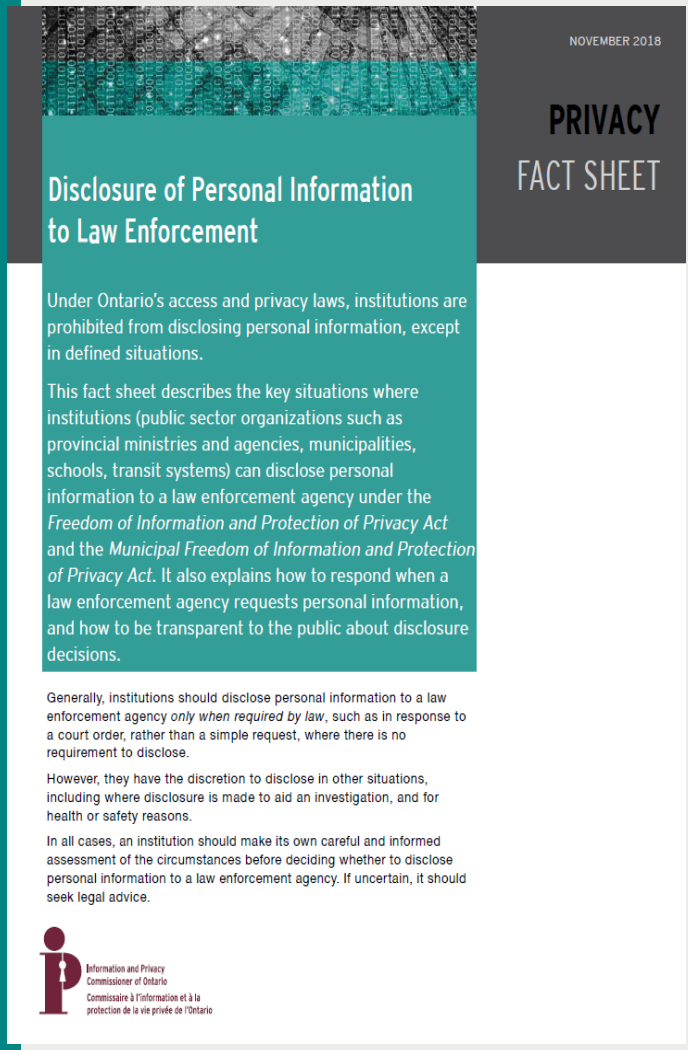
This fact sheet provides institutions and custodians in Ontario with general information about the potential application of this law, and some of its key requirements. Some GDPR requirements may go beyond the privacy rules set out in the *Freedom of Information and Protection of Privacy Act* (*FIPPA*), the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*), and the *Personal Health Information Protection Act* (*PHIPA*).

This fact sheet is not a legal interpretation of any provision of the GDPR and does not provide legal advice about its application in Ontario. Organizations should consult their legal counsel for advice. The scope of the law's application and the interpretation of its requirements depend on future decisions and guidance issued by the EU data protection authorities and courts.

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

Privacy fact sheet: Disclosure of personal information to law enforcement

- when can public institutions disclose PI to a law enforcement agency?
  - when legally required (court order)
  - to aid a law enforcement investigation
  - for health or safety reasons
- disclosing institutions need to
  - document disclosure requests and court orders
  - be transparent about their decisions
  - publish policies about how they make and document decisions about disclosure



NOVEMBER 2018

PRIVACY
FACT SHEET

Disclosure of Personal Information to Law Enforcement

Under Ontario's access and privacy laws, institutions are prohibited from disclosing personal information, except in defined situations.

This fact sheet describes the key situations where institutions (public sector organizations such as provincial ministries and agencies, municipalities, schools, transit systems) can disclose personal information to a law enforcement agency under the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*. It also explains how to respond when a law enforcement agency requests personal information, and how to be transparent to the public about disclosure decisions.

Generally, institutions should disclose personal information to a law enforcement agency *only when required by law*, such as in response to a court order, rather than a simple request, where there is no requirement to disclose.

However, they have the discretion to disclose in other situations, including where disclosure is made to aid an investigation, and for health or safety reasons.

In all cases, an institution should make its own careful and informed assessment of the circumstances before deciding whether to disclose personal information to a law enforcement agency. If uncertain, it should seek legal advice.

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

Doctors' billings

- background
  - Toronto Star seeks access to total amounts paid to top 100 billing physicians, their names and medical specialties
  - Ministry disclosed dollar amounts and most specialties, but withheld all of the physicians' names and some specialties under the personal privacy exemption of *FIPPA*
- Order PO-3617, IPC finds withheld information not personal information, so privacy exemption does not apply
- even if exemption did apply, compelling public interest in disclosure clearly outweighs purpose of the exemption
- IPC orders Ministry to disclose the record in full

Doctors' billings

- Ontario Divisional Court dismisses JR application
  - IPC adjudicator not bound by previous decisions of the IPC
  - decision is "reasonable"
  - requester does not need a reason to obtain the information – public is entitled to government-held information
- Ontario Court of Appeal dismisses appeal
  - an individual's gross professional or business income is not a reliable indicator of their actual personal finances or income, and is therefore not PI
- doctors seeking leave to appeal to Supreme Court of Canada

Questions?

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