

# Answers to Your Frequently Asked Access and Privacy Questions

David Goodis – Assistant Information and Privacy Commissioner

Renee Barrette – Director of Policy



Information and Privacy  
Commissioner of Ontario

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

2019 North Ontario  
Connections  
Summit, Sudbury

October 30, 2019

Can we store personal information using a US based cloud service?

# Cloud computing risks

Yes, but be aware of risks such as

- **loss of control** by customer over technology infrastructure/loss of governance
- **retention and secure destruction**
- **security**
- storage **location** (outside Canada, subject to another country's privacy laws, accessible by other country's law enforcement?)

# Report PC12-39 – MNR hunting and fishing licensing system

Two MPPs raised concerns about the collection and storage of personal information in the US in light of the *PATRIOT Act*

IPC investigation found Ontario's privacy laws do not prevent an institution from **outsourcing services** (inside our outside Canada)

Regardless of where information stored, institution is always **responsible** for privacy/security



*You can outsource data/services ...*

*...but you can't outsource accountability*

*You always remain accountable*

# Thinking about clouds?

- evaluate whether cloud computing services are **suitable**
- identify **risks** associated with using cloud computing
- outline strategies to **mitigate risks**



## Thinking About Clouds? Privacy, security and compliance considerations for Ontario public sector institutions

February 2016



Information and Privacy  
Commissioner of Ontario

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



# What is a Privacy Impact Assessment and how to conduct a PIA?

# What are PIAs?

- process/approach for **identifying and analyzing privacy risks** when creating or changing program or system
- a good PIA analysis gives senior management, program/system designers sufficient information to **reduce, mitigate or avoid privacy risks**



# PIA benefits

**ETHICAL:** respond to privacy rights, and best practices, and need to be transparent about information handling practices

**RISK MITIGATION:** tool to identify privacy risks, document and implement measures to mitigate risks

**COMPLIANCE:** directives, policies, law and other legal requirements

**SAVE TIME AND MONEY:** avoid re-designs, delays, risk of project cancellation

# PIA guide

- includes **tool** to identify privacy impacts and risks
- intended for *FIPPA* and *MFIPPA* institutions
- simplified **4-step methodology**
- basis for developing internal PIA policies and procedures



## Planning for Success: Privacy Impact Assessment Guide



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

# PIA methodology and tools

Key Steps	Tools
<b>1. Preliminary Analysis</b> Is personal Information involved?	Appendix A: Questionnaire
<b>2. Project Analysis</b> Gather project info, people and resources	Appendix B: Questionnaire
<b>3. Privacy Analysis</b> Identify and mitigate risks	Appendix C: Checklist
<b>4. PIA Report</b> Document findings, get approval, proceed	Appendix D: Template

Downloadable Worksheet containing all appendices can be found at [www.ipc.on.ca](http://www.ipc.on.ca)

When does the third party information exemption apply?

# Third party **business information**

Three-part test to determine if 3P exemption applies:

1. Does record contain **business information**

- o trade secrets, scientific information, technical information, commercial information, financial information, labour relations information

2. Was the information **supplied** in **confidence**, implicitly or explicitly, and

3. Could disclosure cause **harm to the 3P**

- o significant damage to competitive position, interference with contractual or other negotiations, similar information no longer being supplied, undue loss or gain

# Fact sheet – third party information exemption

- helps institutions understand how to use the three- part test
- additional information on how to **notify** affected third parties

## Third Party Information Exemption

Public institutions typically have information about outside, or “third party” organizations. Often this information is collected from organizations doing business with institutions. While Ontario’s *Freedom of Information and Protection of Privacy Act* and *Municipal Freedom of Information and Protection of Privacy Act* give people the right to access records held by institutions, there are exceptions to that right, including where disclosure could harm a third party’s business interests. This exception is commonly referred to as the “third party exemption.”

When an institution receives a request for records that include information related to a third party, it must determine if the third party exemption applies to justify withholding the records.

### DETERMINING IF THE EXEMPTION APPLIES

The exemption applies if the record satisfies **all** three parts of this test:

1. the record contains certain types of business information
2. the information was supplied in confidence, either implicitly or explicitly
3. disclosure could cause harm to the third party

# Order PO-3721 – Ministry of Environment and Climate Change

Request to MOECC for access to storm water management plan for wind farm

Wind farm company appeals ministry decision to grant access, arguing contents would be exploited by anti-wind energy activists

IPC disagrees, upholds ministry's decision; **insufficient evidence** that contents of plan could be used to **harm** the company





Can we proactively disclose contracts?



# Open contracting – proactive disclosure of procurement records

Yes, this guide explains how to make **procurement records** publicly available, while protecting sensitive third party information and personal information

Steps to take towards open contracting include:

- make proactive disclosures the default
- be transparent about your transparency
- engage stakeholders
- designing procurement process with limited confidentiality exceptions



## Open Contracting: Proactive Disclosure Of Procurement Records

September 2015



Information and Privacy  
Commissioner of Ontario

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

# Legal Aid Ontario

[Home](#) | [Search](#) | [Careers](#) | [Contact](#) | [LAO Client Portal](#) | [Français](#)

## Legal Aid Ontario

We provide legal assistance for low-income people living in Ontario

[Getting Legal Help](#)

[Information for Lawyers](#)

[Newsroom](#)

[Publications & Resources](#)

[About LAO](#)

[Blog](#)

[Publications & resources](#)

[Open Data](#)

[Open government licence](#)

## Open Data

Legal Aid Ontario is committed to transparency and accountability in the justice sector. LAO is fully participating in the Government of Ontario's Open Data Directive.

Under this directive, provincial agencies are required to post a public data inventory of all the datasets they create, collect and/or manage. The rules, laws and directives for provincial agencies can be found at the [Open Data Directive](#).

## Privacy considerations

LAO is currently in the process of collecting and identifying datasets and the types of data that will be listed.

While we are required to identify datasets we are not required to post them. Under the Open Data Directive, all data should be considered open by default unless:

- The data contains personal or confidential information, has legal, copyright or security restrictions or compromises public safety
- The data is protected under the *Freedom of Information and Protection of Privacy Act, 1990*
- The data should not be disclosed for legal, security, confidentiality, privacy or commercial sensitivity reasons.

## Vendor contracts

### 2018/19 contracts

Reference number	Department	Name of vendor awarded contract	Date of contract	Contract details	Value
RFQ-Invitational	Human Resources	MIT Global Consulting Inc.	2018-09-21	HR related concerns	\$21,000.00
RFQ-Invitational	Human Resources	MIT Global Consulting Inc.	2018-10-11	HR related concerns	\$17,000.00
2018-002	Corporate Services	Optimus SBR	2018-04-23	5 Year Strategic Plan	\$103,564.50
2018-003	IT	Valencia	2018-04-27	Privacy and Threat Risk Assessment	\$136,600.00
2018-004	IT	Simalem Media Inc.	2018-05-30	Public Website	\$90,400.00
2018-005	IT/CLSC	Deloitte	2018-05-01	Client Digital Services	\$141,250.00
2018-006	Facilities	NUA	2018-07-17	Allsteel Systems Furniture	\$204,732.50
2018-007	Facilities	KBH Interior Design	2018-08-20	Facility Design	\$41,479.97
2018-009	CLSC	Sykes	2018-12-18	Brydges Hotline Services	\$1,410,000.00



# Order MO-3499 – Dufferin-Peel Catholic School Board

School board asked for details of successful bid – to whom awarded, winning price

Board notifies contractor that it intends to release details of **contract**

Contractor appeals, claims **record contained trade secrets**

IPC disagrees - claim did not meet third party exemption test

In general, contents of a contract are not **supplied** – they are negotiated

Can we release labour relations and employment information?

# Labour relations and employment records exclusions and exceptions

Most **employment and labour relations records are excluded** from *M/FIPPA* - acts do not apply

If excluded, records **can be released** outside of the FOI process (unless any other prohibition against disclosure in **other law or binding agreement**)

There are exceptions to the exclusion – *M/FIPPA* **does apply** to:

- agreement between institutions and trade union (**collective agreements**)
- agreement between institution and employee which ends proceeding before court/tribunal on employment-related matters (**minutes of settlement**)
- agreement between institution and employee resulting from negotiations between them about employment-related matters (**severance agreements**)
- expense accounts submitted by employee for reimbursement (**travel expense claim**)

# Releasing labour relations and employment records

## *M/FIPPA* applies

- determine whether any **exemptions** apply before releasing records, for example third party information, solicitor-client privilege, personal information

## Excluded

- use your **discretion to release** records outside of formal FOI process, if there are no prohibitions in other laws or agreements



# Order PO-3642 – Ministry of Community Safety and Correctional Services

Ministry received request for records relating to **nuclear emergency management** in the province

Ministry withheld a portion of a record about a new government facility because the information concerned workforce **labour relations** at the facility, therefore excluded

IPC orders release of record, explains that **exclusion cannot apply to part of a record**

When **examined as a whole**, the record was *not* about labour relations and therefore not excluded

Can we collect, use and disclose  
information with consent?

# Privacy rules under *M/FIPPA*

*M/FIPPA* sets out rules for **collection**, **use**, **disclosure** of personal information

---

To **collect** PI, it must be:

- expressly authorized by statute
- used for law enforcement purposes, or
- **necessary** to proper administration of lawfully authorized activity – **more than merely helpful**

---

You can only **use** PI:

- with consent
- for original purpose collected
- for **consistent** purpose

---

You can only **disclose** PI:

- with consent
- for **consistent** purpose
- to comply with legislation
- for law enforcement
- for health and safety reasons
- for compassionate reasons

# Collecting personal information directly/indirectly

General rule: personal information should be **collected directly** from the individual

Exceptions to this rule, if

- individual **consents** to indirect collection
- **Commissioner has authorized** the manner of collection
- information was collected for a **court or quasi-judicial proceeding**
- it is for the purposes of **law enforcement**

# Valid consent

Consent is considered **valid** when

- it is the consent of the individual
- it is knowledgeable
- it relates to the information
- is not obtained through deception or coercion

As a best practice, consent should be **in writing** and specifically mention the information to which it relates

If consent is not received in writing, institutions should **document**

- the specific personal information being used, disclosed or indirectly collected
- the purpose for which the information is being used, disclosed or indirectly collected
- the name of the individual and the date the consent is received
- the name of the institution receiving the consent

# When can we use video surveillance?



# Surveillance technologies

- IPC supports use of surveillance technologies to enhance community safety and deter unlawful activity, providing they are implemented in a manner that protects privacy
- privacy implications associated with surveillance technologies include:
  - potential to collect large amounts of personal information about individuals, including who they communicate with and what they communicate about
  - ability to track locations of individuals over time and to facilitate profiling of law-abiding individuals going about their everyday activities



# Video surveillance best practices

- ensure **lawful collection**
  - expressly authorized by statute
  - used for purposes of law enforcement or
  - **necessary** to proper administration of lawfully authorized activity – **more than merely helpful**
- **minimize** PI collected, used, retained, disclosed
  - ensure camera does not capture information from adjacent areas and locations
  - avoid collecting audio if possible
  - ensure lawful use and disclosure
  - limit retention of video to what's necessary to achieve purpose
- provide **notice of collection**
  - notify individuals about collection of their information

# Guidance for video surveillance



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

## Technology Fact Sheet

### Video Surveillance

November 2016

#### INTRODUCTION

This fact sheet provides institutions subject to the *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA, MFIPPA or the acts)* with basic information about how to use video surveillance in a way that protects individual privacy. More detailed guidance can be found in the IPC's **Guidelines for the Use of Video Surveillance**.

#### DOES YOUR INSTITUTION HAVE THE AUTHORITY TO INSTALL A VIDEO SURVEILLANCE SYSTEM?

Institutions can collect personal information through the use of a video surveillance system if the collection is authorized under *MFIPPA* or *FIPPA*. Video surveillance may be authorized in cases where the system is used for the purposes of law enforcement, for example the use of temporary cameras by police for planned protests. It may also be authorized when necessary for the administration of your institution's lawful activities.

Video surveillance may be considered *necessary* if:

- the goals or purposes of the collection cannot be achieved by less privacy intrusive means, and
- the surveillance is more than merely helpful

For instance, circumstances may justify a school board's or a public transit authority's use of video surveillance to ensure safety on school property or on buses and subway systems.

#### ARE THERE LIMITS TO THE NUMBER AND PLACEMENT OF CAMERAS?

Yes. The video surveillance system should use as few cameras as possible. Cameras should be placed only in those locations where they are needed.



## Guidelines for the Use of Video Surveillance

October 2015



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

# Sudbury's "Eye in the Sky"

Sudbury Police operate the "Lion's Eye in the Sky" program, using cameras on downtown streets, live-monitored by volunteers

An expansion of the program led IPC to review it to ensure it complied with privacy law

IPC decided program and expansion were justified

Our policy department worked with police to make sure details of the surveillance program complied with privacy best practices

When can we disclose personal information to the police?

# Metrolinx disclosing personal information to police

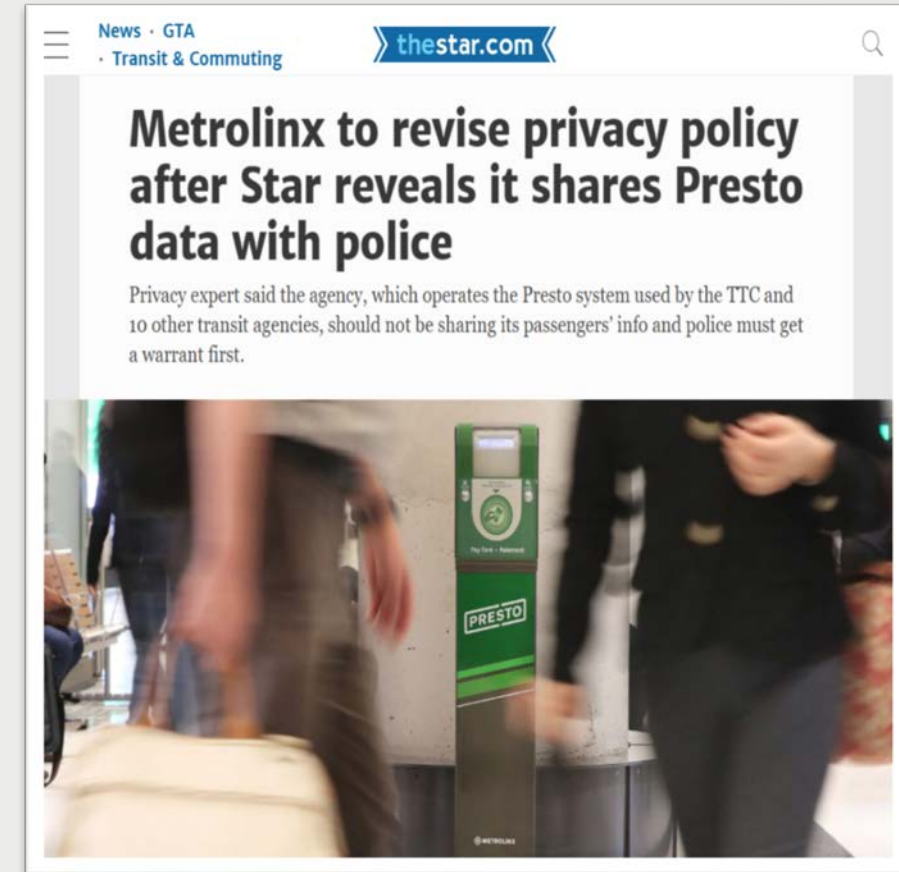
June 2017, Toronto Star reported that Metrolinx had been “quietly sharing Presto users’ information with **police**”

Star reported that

- Metrolinx has received 26 requests from police over previous 5 months, 12 of which it had granted
- requests related to alleged criminal offences and missing persons cases

Metrolinx committed to revising its privacy policy following Star investigation

Metrolinx legal and privacy team **consulted with IPC** during the review of their new policy



# Fact sheet: disclosure of personal information to law enforcement

When can an institution disclose personal information to a law enforcement agency?

- when legally required
- 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
- develop and publish policies about their practices

## 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.



# Dealing With law enforcement

- answers the public's frequently asked questions about access and privacy rights
- explains obligations of law enforcement agencies under Ontario law



The cover of the 'ACCESS FACT SHEET' features a background of a red padlock and a keyboard. The title 'ACCESS FACT SHEET' is in white on a dark grey background. Below it, the subtitle 'Police record checks' is in white on a red background. The main text area is white with a red border.

AUGUST 2019

## ACCESS FACT SHEET

### Police record checks

In Ontario, the *Police Record Checks Reform Act* sets the rules for police record checks. This fact sheet describes the different types of checks, the information they contain, and your rights under the law.

The *PRCRA* applies to all police record checks in Ontario except where the legislation establishes an exception, such as for screening related to child custody, adoption, and children's residential care.

#### WHAT IS A POLICE RECORD CHECK?

When you apply for certain jobs, volunteer positions, educational programs or licenses, you may be asked to consent to a police record check. A police record check involves a search of police record-keeping systems such as the Canadian Police Information Centre database. A check may also involve the search of a local police service's records.

Police records contain information about the people police interact with, in both criminal and non-criminal situations. They may describe interactions that range from informal contacts with a police officer to being found guilty and convicted of a criminal offence. A police record check only includes some of the information in police records.

#### WHAT KINDS OF POLICE RECORD CHECKS ARE PERMITTED?

The *PRCRA* sets out three types of record checks that can be used for screening purposes and the kinds of information those checks can disclose.

## Release of personal information to police: your privacy rights

Ontario public sector organizations, such as provincial ministries and agencies, municipalities, schools, and transit systems, are required by law to protect your personal information and to follow certain rules when collecting, using, and disclosing your personal information.

Ontario public sector organizations, such as provincial ministries and agencies, municipalities, schools, and transit systems, are required by law to protect your personal information and to follow certain rules when collecting, using, and disclosing your personal information.

This fact sheet describes the key situations where institutions can share your personal information with a law enforcement agency. For information on disclosure of your personal information to police by a private organization, such as a cellphone company, contact the Office of the Privacy Commissioner of Canada, which oversees the rules for how businesses handle personal information.

### WHAT IS PERSONAL INFORMATION?

Under Ontario's access and privacy laws, personal information means, "recorded information about an identifiable individual." For a full explanation of the definition, see our fact sheet *What is Personal Information?*

Should we contact IPC if we have a  
privacy breach?



# Privacy breaches: guidelines for public sector organizations

- What is a privacy breach
- How to respond to a breach
- How and when to notify affected parties
- When to report a breach to IPC
- What to expect when you report a breach

PRIVACY

Privacy Breaches  
Guidelines for Public Sector  
Organizations



# Notification - individuals

Institutions should notify **individuals** affected by a breach as soon as reasonably possible if the breach poses a **real risk of significant harm** to the individual

Institutions should notify directly i.e. by telephone, letter, email or in person

Notice to individuals should include

- details of the extent of the breach
- steps taken to address the breach
- contact information for someone within the institution
- information about their right to make a complaint to IPC

# Notification - IPC

Institutions should notify the **IPC** of a **significant breach** as soon as reasonably possible , e.g. breaches that may involve sensitive personal information, or large number of individuals

If contacting a large number of affected individuals, contact the IPC prior to starting the notification process

IPC can assist institutions with their breach response plan

What should we do about increasing  
cybersecurity threats?

# Ontario city of Burlington out \$503,000 after staff member falls for phishing scam

*They say the staff member made a single transaction to a 'falsified bank account' after receiving an email requesting to change banking information*

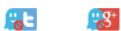
## Canadian Underwriter

YOUR GUIDE TO INSURANCE SUCCESS. SINCE 1934

News

### Cyber attack in Canada spawns \$60 million lawsuit

March 29, 2019 by By Colin Perkel - THE CANADIAN PRESS



Print this page

Share

TORONTO – As many as 200,000 people may have had their personal information stolen in a hack on servers at one of Ontario’s most popular casinos, a lawyer for the plaintiffs pressing a proposed class action argued on Thursday.

However, a lawyer for Casino Rama countered that, at most, 10,000 to 11,000 people were victimized and the plaintiffs’ definition of who should be included in the proposed class action was far too broad.

The case arose in November 2016 when Casino Rama announced it had been victim of a cyberattack in which a large quantity of sensitive personal information had been stolen. The attacker, who apparently gained access through a phishing scam, posted the information – including names, addresses, credit files, gambling losses, income and place of employment – of about 10,900 people publicly on Nov. 11, 2016.

# PHISHING SCAM LEADS TO SUSPENSION OF ONLINE ACCESS FOR HUNDREDS OF STAFF ACCOUNTS

February 13, 2019 | By Joshua Ambar

Facebook

Twitter

Google+

LinkedIn

Pinterest

Algonquin was hit with yet another cyber attack on Tuesday, Jan. 29, when hundreds of employees opened a sophisticated phishing email that looked as if President Cheryl Jensen sent it.



Ontario police warn of recent cyberattacks targeting local governments

Toronto

### Ontario police warn of recent cyberattacks targeting local governments



Attacks launched through direct hacking into vulnerable systems or through phishing emails, OPP said

The Canadian Press · Posted: Sep 14, 2018 4:39 PM ET | Last Updated: September 14, 2018



Eastern Ontario community hit with ransomware attack

Ottawa

### Eastern Ontario community hit with ransomware attack



The Nation, Ont., has computer networks frozen in online attack

CBC News · Posted: Jul 08, 2019 8:37 PM ET | Last Updated: July 9



asked employees to fill out the information required. Employees were asked to provide their user ID and password, which in some cases were used to access systems.

On Feb. 4, that ITS immediately limited access to systems and asked employees to reset their passwords. To take more time to reset passwords, employees were asked to do so by Thursday, Jan. 31.



MENU

news

Ottawa Hospital targeted by cyberattack

Ottawa

### Ottawa Hospital targeted by cyberattack



Hackers target four computers but no data compromised, says hospital

The Canadian Press · Posted: Mar 13, 2016 9:26 AM ET | Last Updated: March 13, 2016



# Phishing

Guides public institutions on how to protect personal information from phishing attacks

- What is phishing
- Impacts of phishing attacks
- How to recognize phishing messages
- How to protect against phishing attacks
- How to respond to a phishing attack

## Protect Against Phishing

Phishing is a common method hackers use to attack computer systems. Successful phishing attacks pose a serious threat to the security of electronic records and personal information.

Ontario's privacy laws require public and healthcare organizations to have reasonable measures in place to protect personal information in their custody or control.

Phishing attacks pose a serious threat to the security of electronic records and personal information

### WHAT IS PHISHING?

Phishing is a type of online attack in which an attacker — using both technological and psychological tactics — sends one or more individuals an unsolicited email, social media post, or instant message designed to trick the recipient into revealing sensitive information or downloading malware.

Malware (malicious software) is any software intentionally designed to disrupt, damage, or gain unauthorized access to a computer system.

Phishing attacks can be generic or customized, and can target both individuals and entire organizations. Attacks that target a specific individual or organization are commonly referred to as spear phishing attacks.

The main goal of a phishing attack is to get the individual to do something that compromises the security of their organization. Attackers achieve this when recipients:

- reply to phishing emails with confidential information



# Guard against ransomware

## Protect your organization

- Train employees
- Limit user privileges
- Use software protections and back-ups
- Have an incident response plan in place

## Protecting Against Ransomware

July 2016

Ransomware has become an increasingly common and dangerous threat to the security of electronic records. This fact sheet provides information on how public institutions and healthcare organizations in Ontario can protect themselves against it.

### WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or “malware,” that encrypts files on your device or computer, including any mapped or network drives, and then demands payment in exchange for the key needed to decrypt the files. It essentially locks you out of your data and holds the means of regaining access for ransom.

### HOW DO COMPUTERS GET INFECTED?

Hackers use different techniques to install ransomware on computers. In general, these fall into two categories: “phishing” attacks and software exploits.

#### Phishing Attacks

Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

In the case of ransomware, the hacker will often try to impersonate an “official” correspondence relating to a common business transaction, such as a shipping notice or invoice from a delivery company. The hacker may also try to fake an “urgent matter,” such as an unpaid invoice or notice of audit. More advanced versions (also known as “spear phishing”) target specific individuals or places of business.

Ransomware may be installed if the recipient opens a file attachment or clicks on a link in the body of the message.



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](http://www.ipc.on.ca)

E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)

Media: [media@ipc.on.ca](mailto:media@ipc.on.ca) / 416-326-3965