



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

An Update on *PHIPA* from the IPC

April 10, 2018

Brian Beamish

Commissioner

Information and Privacy Commissioner of Ontario



Mandatory Breach Reporting

Health Privacy Breach Investigations

- The IPC investigates health privacy complaints under *PHIPA* arising from:
 - complaints from individuals
 - self-reported breaches
 - Commissioner's discretion
- Typical causes:
 - unauthorized access to health records (snooping)
 - misdirected information (wrong phone, email or fax)
 - insecure storage or destruction of records
 - loss or theft of devices (laptops, USB sticks, mobile phones)

Mandatory Breach Reporting

You must notify the IPC in cases of:

1. use or disclosure without authority
2. stolen information
3. further use or disclosure without authority after a breach
4. pattern of similar breaches
5. disciplinary action against a college member
6. disciplinary action against a non-college member
7. significant breach

SEPTEMBER 2017

GUIDELINES FOR THE HEALTH SECTOR

Reporting a Privacy Breach to the Commissioner

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

You May Not Need to Report a Breach if:

- it is accidental
- it is a one-off incident
- it is not part of a pattern

Accidental Breaches

Not every breach is significant

- nurse clicks on the wrong patient file
- records clerk opens the wrong file folder
- doctor walks into the wrong patient room

A Tale of Two Pharmacies

Now You See It, Now You Don't

- pharmacist placed a prescription on the countertop with the label facing the public for a very brief amount of time

Reuse, Recycle, Reveal

- pharmacist was reusing prescription containers and putting new labels over old ones
- new labels could be peeled off exposing PHI on the old label



Significant Breaches

Is it a significant breach?

Consider all relevant circumstances to determine if a breach is significant, including:

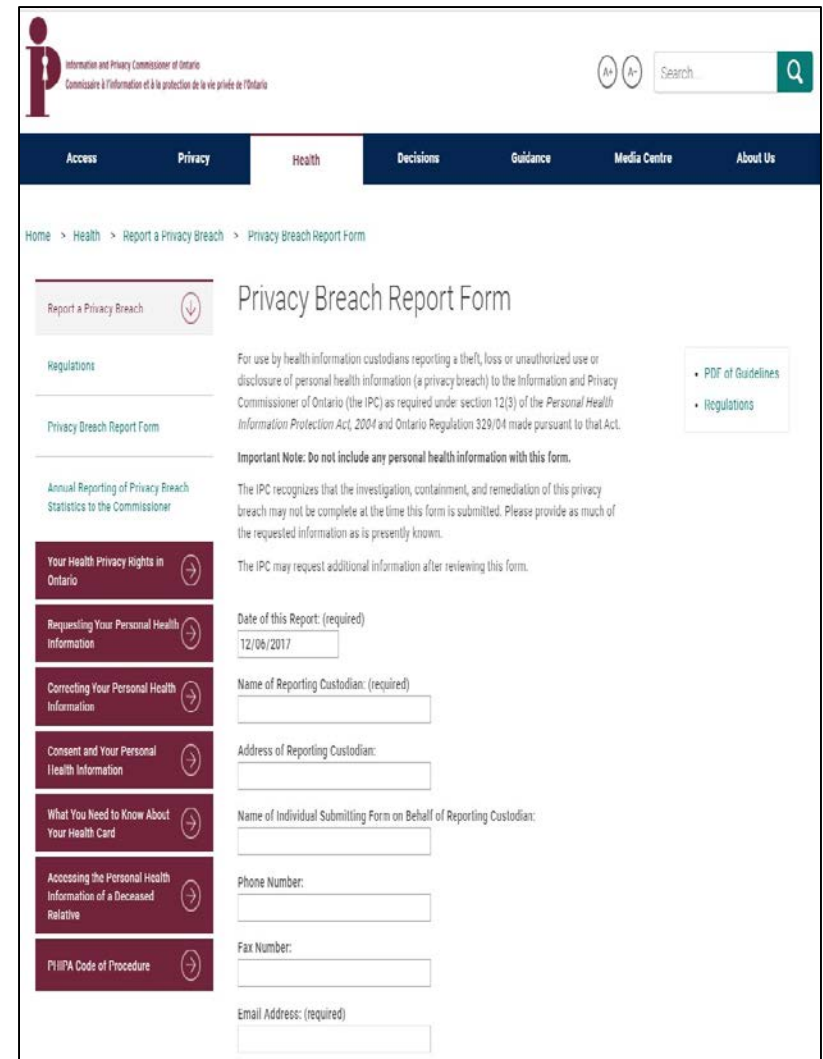
- How sensitive is the information?
- How much personal health information is involved?
- How many individuals are affected?
- Is more than one health information custodian or agent involved?

IPC Privacy Breach Online Report Form

Although you can report breaches by mail or fax, we recommend that you use our online report form.

You will be asked to provide:

- a description of the breach
- steps taken to contain the breach
- steps taken to notify affected individuals
- steps taken to investigate and remediate the breach



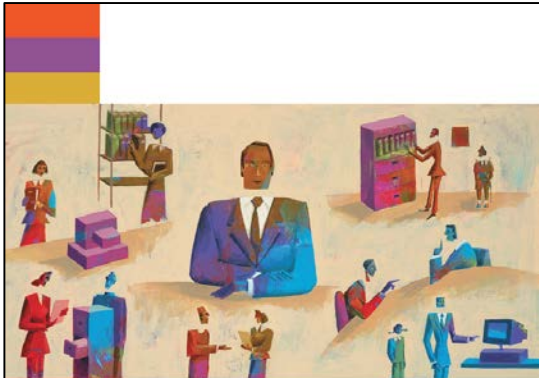
The screenshot shows the online report form for the Information and Privacy Commissioner of Ontario. The page is titled "Privacy Breach Report Form" and includes a navigation menu with options like "Access", "Privacy", "Health", "Decisions", "Guidance", "Media Centre", and "About Us". The main content area contains a sidebar with links to "Report a Privacy Breach", "Regulations", "Privacy Breach Report Form", and "Annual Reporting of Privacy Breach Statistics to the Commissioner". The main form area includes an "Important Note" and a "Date of this Report" field with a date of 12/08/2017. Other fields include "Name of Reporting Custodian", "Address of Reporting Custodian", "Name of Individual Submitting Form on Behalf of Reporting Custodian", "Phone Number", "Fax Number", and "Email Address".

Guidance Documents Available from the IPC

www.ipc.on.ca



Detecting and Deterring Unauthorized Access to Personal Health Information



What to do When Faced With a Privacy Breach: Guidelines for the Health Sector



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

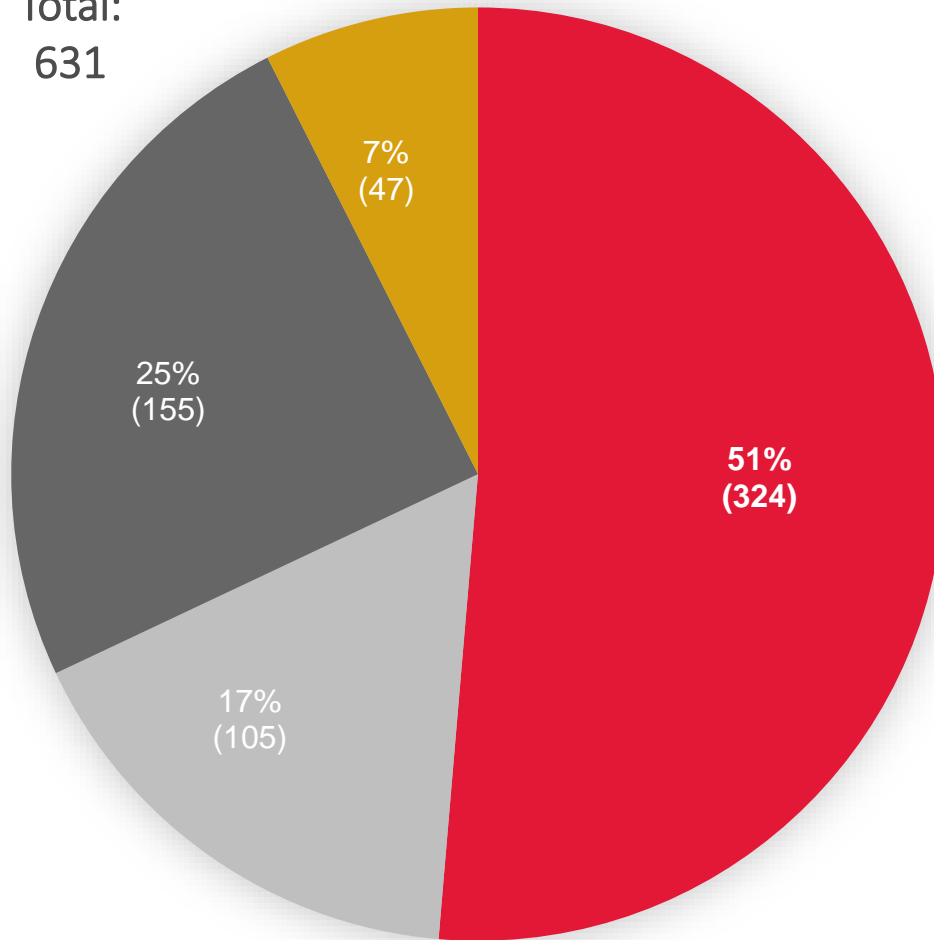
This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

Duty to Notify Individuals

It is important to remember that even if you do not need to notify the IPC, you have a separate duty to notify individuals under section 12(2) of *PHIPA*.

Health Sector Privacy Complaints 2017

Total:
631



■ 1 ■ 2 ■ 3 ■ 4

Of the 324 self-reported breaches:

- 60 snooping incidents
- 8 ransomware/cyberattack

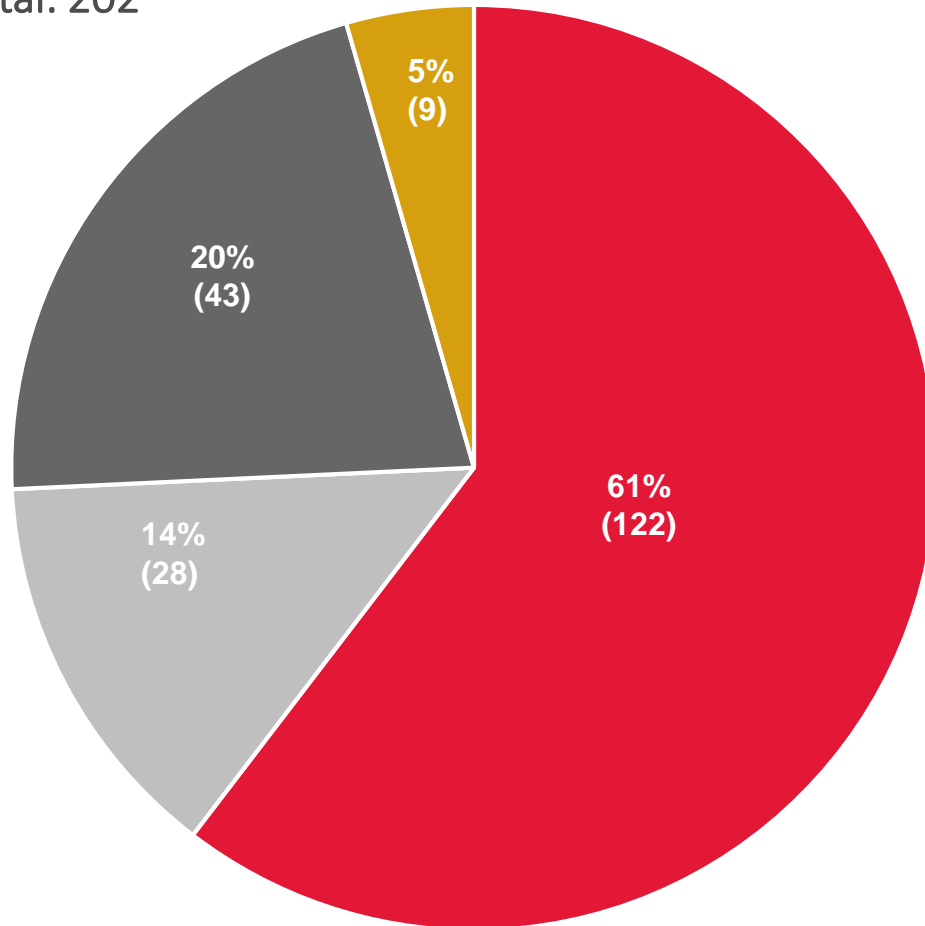
Remaining 256 were:

- lost or stolen PHI
- misdirected information
- records not properly secured
- other collection, use and disclosure issues

2018 So Far

Health Sector Privacy Complaints

Total: 202



■ 1 ■ 2 ■ 3 ■ 4

Of the 122 self-reported breaches:

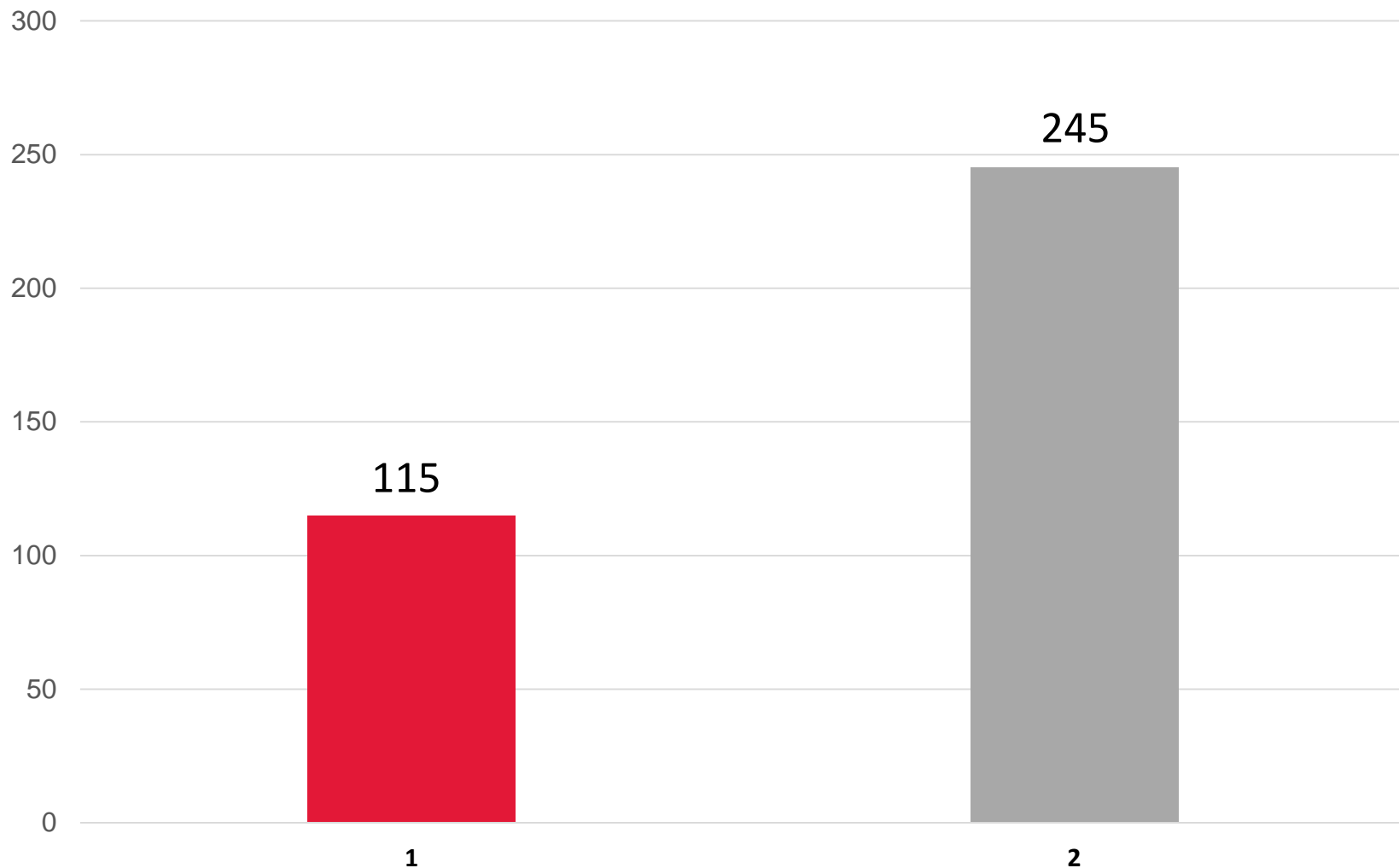
- 23 snooping incidents
- 2 ransomware/cyberattack

Remaining 97 were:

- lost or stolen PHI
- misdirected information
- records not properly secured
- other collection, use and disclosure issues

Self-Reported Breaches

Before and After Mandatory Breach Reporting



Annual Reporting of Privacy Breach Statistics

- Health information custodians must provide the IPC with annual privacy breach statistics starting in March 2019.
- They must track incidents commencing on January 1, 2018 where personal health information was:
 - stolen
 - lost
 - used without authority
 - disclosed without authority
- This annual report must also include breaches that do not meet the criteria for immediate mandatory reporting to the IPC.

Annual Reporting of Privacy Breach Statistics to the Commissioner

REQUIREMENTS FOR
THE HEALTH SECTOR

Starting in March 2019 health information custodians will be required to provide the Commissioner with an annual report on privacy breaches occurring during the previous calendar year.

This requirement is found in section 6.4 of Ontario Regulation 329/04 made under to the *Personal Health Information Protection Act, 2004*, as follows:

- (1) On or before March 1, in each year starting in 2019, a health information custodian shall provide the Commissioner with a report setting out the number of times in the previous calendar year that each of the following occurred:
 1. Personal health information in the custodian's custody or control was stolen.
 2. Personal health information in the custodian's custody or control was lost.
 3. Personal health information in the custodian's custody or control was used without authority.
 4. Personal health information in the custodian's custody or control was disclosed without authority.
- (2) The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner.

For custodians to prepare for this reporting requirement, they must start tracking their privacy breach statistics as of January 1, 2018. The following is the information the IPC will require in the annual report.

WELCOME TO
BIENVENUE AU



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

Online Statistics Submission
Website

Site Web de présentation des
statistiques annuelles

Login/ Nom d'utilisateur:

Password/Mot de passe:

LOGIN

Forgot your password? [Please Click Here](#).
Vous avez oublié votre mot de passe? Si il vous plaît [Cliquez ici](#).

Significant *PHIPA* Investigations and Decisions

PHIPA Decision 49

A Doctor's Office

- A doctor received an email from a former patient containing an image of a computer screen in the doctor's examination room that showed the PHI of 72 individuals.
- The doctor's lawyer asked the patient to delete the photo but he refused.
- Our office found that the patient was a recipient of PHI and had used the information in contravention of *PHIPA*.
- The patient was ordered to securely dispose of the PHI of other individuals in the image.
- Order has been filed with Superior Court – our office is bringing a contempt motion to enforce it.

PHIPA Decision 52

St. Michael's Hospital

- Complainant sought access to all the electronic data about himself, in its native, industry-standard electronic format.
- Hospital did not provide the complainant with the raw data from which information was derived, such as in medical devices or databases associated with each electronic system.
- Complainant only has a right of access to underlying raw data that the hospital can itself extract.
- Hospital is entitled to reasonable cost recovery in providing access.
- Due to the significant staff time and resources that would be required to extract a certain type of data, it was **not reasonably available** to the hospital itself.

PHIPA Decision 56

An Insurance Company

- Insurance company was collecting OHIP numbers through its application process for purchasing supplementary health insurance plans.
- This collection of OHIP numbers contravened *PHIPA*.
- However, collecting and using OHIP numbers when emergency travel claims were **filed** was found to be permissible.
- Insurance company discontinued its practice of collecting OHIP numbers and deleted OHIP numbers from its administrative system.

PHIPA Prosecutions

Prosecutions

To date, six individuals have been prosecuted:

- 2011 – Nurse at North Bay Health Centre
- 2016 – Two radiation therapists at a Toronto Hospital
- 2016 – Registration clerk at a regional hospital
- 2017 – Social worker at a family health team
- 2017 – Administrative support clerk at a Toronto hospital

Most Recent *PHIPA* Prosecution

- Administrative support clerk in the emergency department of a GTA hospital.
- Accessed the health records of 44 individuals without authorization, in some cases printing their personal health information.
- In October 2017 the clerk pled guilty and the court imposed a fine totaling \$10,000.

Child, Youth and Family Services Act

Child, Youth and Family Services Act

- The *CYFSA* received Royal Assent on June 1, 2017
- Part X:
 - sets out new rules for the collection, use and disclosure of personal information by service providers, including children's aid societies (CASs)
 - establishes new rights for individuals to access their personal information from service providers, and request corrections

Proclamation

- Part X will:
 - be proclaimed along with the rest of the *CYFSA* on April 30, 2018, but
 - not become effective until January 1, 2020

Background

- Part X of the *CYFSA* represents a big step forward for Ontario's child and youth sectors:
 - closes a legislative gap for access and privacy
 - promotes transparency and accountability
- Child welfare records have long been subject to public sector privacy legislation in other provinces
- The IPC and Ontario Association of Children's Aid Societies have both made multiple recommendations that CASs should be subject to access and privacy legislation

Strengths of Part X

- modelled after *PHIPA*
- consent-based framework
- individuals' right of access to their personal information
- mandatory privacy breach reporting
- clear offence provisions
- adequate powers for the IPC to conduct reviews of complaints
- facilitates transparency and consistency among CASs' information practices

Part X – Privacy Protection

- Part X protects privacy by creating rules regarding personal information:
 - collection
 - use
 - disclosure
 - retention
 - disposal
- **Data minimization requirements** limit a service provider's authority to collect, use or disclose personal information

Part X – Individual’s Right of Access

- Part X gives individuals the right to access:
 - records of their **personal information (PI)**
 - in a service provider’s **custody or control** and
 - that **relate to the provision of a service to the individual**
- **No fees** can be charged for access except in prescribed circumstances (currently, none are prescribed)

Privacy is not a Barrier to Releasing Non-Identifying Statistics

- Our office was contacted by reporters who experienced difficulties getting statistical information on the number of local flu-related deaths.
- This information was seen to be in the public's interest as an indicator of how serious the flu threat was in particular communities.
- Local health authorities refused to release the information citing privacy concerns.
- Privacy laws **do not** prohibit the release of non-identifying statistical information.
- Health data of this type can provide critical insights about disease trends — information the public has a right to know.
- If health authorities have non-identifying statistical information, they should release it.

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

www.ipc.on.ca

info@ipc.on.ca