CHILD, YOUTH, AND FAMILY SERVICES

OCTOBER 2019

Guidelines for Submitting Annual Statistics to the IPC

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

GUIDELINES FOR SUBMITTING ANNUAL STATISTICS TO THE IPC

Child and family service providers are required to provide the Information and Privacy Commissioner of Ontario with an annual statistical report on requests for access and correction to records of personal information and privacy breaches during the previous calendar year. This applies to all service providers under Part X of the *Child, Youth and Family Services Act*.

The reporting deadline is March 31 for data collected from January to December of the previous year.

TRACKING INFORMATION

To prepare for this reporting requirement, service providers should develop a system to track their statistics.

At the end of this document, you will find a checklist of the categories to track throughout the year. You can also review our *Workbook for Submitting Your Annual Report to the IPC*.

INFORMATION USED OUTSIDE OF YOUR STATED INFORMATION PRACTICES

Under Part X, you must have a written statement about your information practices — your policies for collection, use, modification, disclosure, retention, and disposal of personal information — as well as the safeguards you have in place to protect the information, available to the public.

In your statistical report to the IPC, you must report the number of times records of personal information were used or disclosed *outside of the scope* of your stated information practices.

ACCESS REQUESTS

Service providers must submit statistics related to the number of written access requests received under Part X of the *Child, Youth and Family Services Act*, and the time you took to respond to them. You must count any access request as one request, regardless of the number of records involved, because it is about only one subject (the person asking for the information).

Under Part X, you are required to complete requests for access to records of personal information within 30 calendar days.

In cases where you need to review or search numerous records, or consult with other parties, you can extend the 30-day time limit for no more than an additional 90 days and remain in compliance with Part X. To extend the time limit, you must issue a *Notice of Extension* (a written explanation for the extension) to the requester within 30 days of receiving the access request.

To determine the number of requests that are in compliance or not in compliance with the timelines under Part X, you also need to track information related to the number of requests completed.

You should therefore track the number of access requests:

- received
- completed (total)
- completed within 30 days
- completed in over 30 days with an extension (Notice of Extension issued)

- completed in over 30 days without an extension (Notice of Extension not issued)
- completed within the time limit stated in the Notice of Extension (up to 90 additional days)
- where completed requests exceeded the permitted time limit stated in the Notice of Extension

OUTCOME OF ACCESS REQUESTS

You must submit information about how you handled each request for access to records of personal information. If a request had one or more outcome, you can enter it in each applicable category (you do not need to choose only one).

Track the number of access requests:

- resulting in full access to the requested records of personal information
- where you gave partial access because provisions of Part X were used to deny access
- where you gave partial access because some of the records of personal information do not exist or cannot be found
- where you gave partial access because Part X does not apply to the information requested
- where no information was released because the provisions of Part X were used to deny access
- where no information was released, because no record exists or none can be found
- where no information was released because Part X does not apply to the information requested
- that were unfulfilled because they were withdrawn or abandoned by the requester

PART X PROVISIONS APPLIED TO DENY ACCESS

Where provisions of Part X were used to deny access in whole or in part, you will need to track which specific provision(s) you relied on to deny access. If you relied on more than one of these provisions in responding to any given access request, you can choose all that apply (you do not need to choose only one).

You will need to track the number of requests where you denied access because:

- the record or the information in the record is subject to a legal privilege that restricts its disclosure to the individual
- another act or a court order prohibits its disclosure to the individual
- the information in the record was collected or created primarily in anticipation of, or for use in, a proceeding, and the proceeding, together with all appeals or processes resulting from it, has not concluded
- granting the access could reasonably be expected to result in a risk of serious harm to the individual or another individual
- granting the access could reasonably be expected to lead to the identification of an individual who was required by law to provide information in the record to the service provider

- granting the access could reasonably be expected to lead to the identification of an individual who provided information in the record to the service provider explicitly or implicitly in confidence (if the service provider considers it appropriate in the circumstances that the identity of the individual be kept)
- the request is frivolous or vexatious

CORRECTIONS AND STATEMENTS OF DISAGREEMENT

Under Part X of the *CYFSA*, if an individual believes that their record of personal information held by a service provider is inaccurate or incomplete, they have a right to request that the service provider:

- correct the record
- send a written notice of the correction to anyone to whom the service provider disclosed the information (unless it will not affect services to the individual)
- attach a statement of disagreement to the information — if the requested correction was not made — and disclose the statement at any time that the service provider discloses the information

To report statistics related to correction requests, you should track the number of correction requests:

- received
- completed (total)
- made in their entirety
- partially made
- refused
- withdrawn or abandoned by the requester before completion
- in which a statement of disagreement was added to the record
- in which notifications were sent to third parties
- completed within 30 days
- completed in over 30 days without an extension (Notice of Extension not issued)
- completed in over 30 days but within the extended time limit stated in the Notice of Extension (up to 90 additional days)
- where completion of the request exceeded the permitted time limit stated in the Notice of Extension

ANNUAL REPORTING OF PRIVACY BREACHES

Service providers are required to provide the commissioner with statistics on the number of times in the previous calendar year that records of personal information were subject to privacy breaches, the reasons for the breaches, and the number of people affected by the breaches. In the annual statistics report, you

must include all thefts, losses, or unauthorized uses or disclosures; even if you were not required to report to the IPC at the time the breach occurred.

You will need to track the number of times records of personal information were stolen, lost, used without authority, or disclosed without authority.

Do not count each incident more than once. If one incident includes more than one of the categories, choose the category that best fits. For example, if an employee accessed records of personal information, and then disclosed the information, you should count that incident as either a use or a disclosure, but not both.

STOLEN RECORDS OF PERSONAL INFORMATION

Keep track of the number of incidents where:

- records of personal information were stolen
- theft was the result of a cyberattack, and of the total number of cyberattacks, how many were ransomware attacks
- unencrypted portable electronic equipment (such as USB keys or laptops) was stolen
- paper records were stolen

Of the total in this category, the number of incidents where:

- theft was by an internal party (such as an employee, agent, or other service provider) or
- theft was by a stranger.

You will also need to report the number of breaches by theft where:

- one individual was affected
- 2 to 10 individuals were affected
- 11 to 50 individuals were affected
- 51 to 100 individuals were affected
- over 100 individuals were affected

LOST RECORDS OF PERSONAL INFORMATION

Track the total number of incidents where records of personal information were lost, due to:

- cyberattack, and of the total number of cyberattacks, how many were ransomware attacks
- loss of unencrypted portable electronic equipment (such as USB keys or laptops)
- loss of paper records

Of the total in this category, the number of incidents where:

- one individual was affected
- 2 to 10 individuals were affected

- 11 to 50 individuals were affected
- 51 to 100 individuals were affected
- over 100 individuals were affected

RECORDS USED WITHOUT AUTHORITY

Total number of incidents where records of personal information were used (viewed, handled) without authority and the reasons for it, including where:

- unauthorized use was through electronic systems
- unauthorized use was through paper records

Of the total in this category, the number of incidents where:

- one individual was affected
- 2 to 10 individuals were affected
- 11 to 50 individuals were affected
- 51 to 100 individuals were affected
- over 100 individuals were affected

RECORDS DISCLOSED WITHOUT AUTHORITY

Total number of incidents where records of personal information were disclosed without authority and the reasons for it, including where unauthorized disclosure was due to:

- misdirected faxes
- misdirected emails
- other means

Of the total in this category, the number of incidents where:

- one individual was affected
- 2 to 10 individuals were affected
- 11 to 50 individuals were affected
- 51 to 100 individuals were affected
- over 100 individuals were affected

TRACKING CHECKLIST

Number of times your organization used or disclosed personal information for a purpose not included in your written public statement of information practices	
Access requests received	
total received	
Access requests: time to completion	
completed within 30 days	
completed in over 30 days with an extension	
completed in over 30 days without an extension	
completed within the extended time limit stipulated in the Notice of Extension (up to 90 additional days)	
completed in a time that exceeded the permitted time limit stipulated in the Notice of Extension	
Outcome of access requests	
full access to records of personal information requested	
partial access because provisions of Part X were used to deny access	
partial access because some of the records of personal information do not exist or cannot be found	
partial access because Part X does not apply to the information	
no information was released because provisions of Part X were used to deny access	
no information was released because no record exists or none can be found	
no information was released because Part X does not apply to the information	
unfulfilled because the request was withdrawn or abandoned by the requester	
Provisions used where access was denied (in whole or part)	
the record or the information in the record is subject to a legal privilege that restricts its disclosure	
another act or a court order prohibits its disclosure	
the information in the record was collected or created primarily in anticipation of, or for use in, a proceeding, and the proceeding, together with all appeals or processes resulting from it, has not concluded	

granting the access could reasonably be expected to result in a risk of serious harm to the individual or another individual	
granting the access could reasonably be expected to lead to the identification of an individual who was required by law to provide information in the record to the service provider	
granting the access could reasonably be expected to lead to the identification of an individual who provided information in the record to the service provider explicitly or implicitly in confidence	
the request is frivolous or vexatious	
Correction requests	
total received	
Outcome of correction requests	
corrections made in their entirety	
partial correction was made	
request for correction was denied	
request withdrawn or abandoned by the requester before completion	
a statement of disagreement was attached to the information when the correction was not made	
notifications sent to third parties, who in the past received the records of personal information, regarding the correction or the statement of disagreement	
Correction requests: time to completion	
completed within 30 days	
completed in over 30 days without an extension	
completed in over 30 days but within the extended time limit stipulated in the Notice of Extension (up to 90 additional days)	
completed in a time that exceeded the permitted time limit stipulated in the Notice of Extension	
PRIVACY BREACHES	
Number of incidences where records of personal information were stolen	
of the total number, how many in which theft was by an internal party (such as an employee or electronic service provider)	
of the total number, how many in which theft was by a stranger	

theft was the result a cyberattack	
of the total thefts due to cyberattacks, how many were ransomware attacks	
unencrypted portable electronic equipment (such as USB keys or laptops) was stolen	
paper records were stolen	
other (theft was a result of something else or other items were stolen)	
number of people affected (of the total in this category, the number of incidents where): • one individual was affected • 2 to 10 individuals were affected • 11 to 50 individuals were affected • 51 to 100 individuals were affected • over 100 individuals were affected	
Total number of incidents where records of personal information were lost	
loss was the result a cyberattack	
of the total losses due to cyberattacks, how many were ransomware attacks	
unencrypted portable electronic equipment (such as USB keys or laptops) was lost	
paper records were lost	
other (loss was a result of something else or other items were lost)	
of the total in this category, the number of incidents where: • one individual was affected • 2 to 10 individuals were affected • 11 to 50 individuals were affected • 51 to 100 individuals were affected • over 100 individuals were affected	
Total number of incidences where records were used without authority	
unauthorized use was through electronic systems	
unauthorized use was through paper records	
other means	

of the total in this category, the number of incidents where: • one individual was affected • 2 to 10 individuals were affected • 11 to 50 individuals were affected • 51 to 100 individuals were affected • over 100 individuals were affected	
Total number of incidences where records were disclosed without authority	
through misdirected faxes	
through misdirected emails	
through other means	
of the total in this category, the number of incidents where: • one individual was affected • 2 to 10 individuals were affected • 11 to 50 individuals were affected • 51 to 100 individuals were affected • over 100 individuals were affected	

HOW TO SUBMIT YOUR QUESTIONNAIRE

To submit a statistical report to the IPC using the Online Statistical Reporting System at **https://statistics.ipc.on.ca**, you will need a login id and a password. You can request login credentials by sending an email to statistics.**ipc@ipc.on.ca**. Include the following:

- the name of your organization
- the name and e-mail address of the head of the organization
- the name and e-mail address of the person responsible for the content of the report (management contact)
- the name, mailing address, e-mail address, and telephone number of the person responsible for completing the report (the primary contact)
- your language preference (English or Français)

Faxed or mailed statistics will NOT be accepted. Please submit your report online at: **https://statistics.ipc.on.ca**.

If you have specific questions that are not answered by this guide, please email **statistics.ipc@ipc.on.ca** or call the Information and Privacy Commissioner of Ontario's main switchboard 416-326-3333. If you are calling long distance, use our toll free line: 1-800-387-0073.

Additional guidance on reporting privacy breaches to the IPC, frivolous and vexatious requests, preventing privacy breaches and responding to access and correction requests are available at **www.ipc.on.ca**.

Guidelines for Submitting Annual Statistics to the IPC

Information and Privacy
Commissioner of Ontario

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

2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

www.ipc.on.ca
416-326-3333
info@ipc.on.ca

October 2019