CHILD, YOUTH, AND FAMILY SERVICES

NOVEMBER 2019

Providing Access to Personal Information under the *Child, Youth and Family Services Act*

A Guide for Service Providers

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

This guide is based on sections 312 to 314 of the ***Child, Youth and Family Services Act***, but should not be relied on as a substitute for the legislation itself or for legal advice. It is not an official legal interpretation of the *CYFSA* and does not bind the Office of the Information and Privacy Commissioner of Ontario. For the most up–to–date version of this guide, visit www.ipc.on.ca.

CONTENTS

INTRODUCTION

This guide has been created to help service providers understand their legal obligation to provide access to personal information under Ontario's *Child, Youth and Family Services Act*. It is aimed at staff who receive and process access requests.

Rights and obligations related to accessing information are set out in Part X of the *CYFSA* (sections 312 – 314). The law says that individuals have a right to access records of their personal information from service providers, subject to limited exceptions. Service providers must respond to access requests within 30 calendar days.

Part one of this guide explains an individual's right of access, while also explaining the exceptions to that right. Part two of the guide explains requirements and best practices for how to process access requests, including how to clarify and narrow a request, conduct a search for records and respond within set timelines.

If you are unsure if Part X of the *CYFSA* applies to your organization, or if you want to learn more about it, consult *Part X of the Child, Youth and Family Services Act: A Guide to Access and Privacy for Service Providers*. This guide is available at www.ipc.on.ca.

ABOUT THE IPC

The Office of the Information and Privacy Commissioner of Ontario provides oversight of the province's privacy and access to information laws, including the rules to protect and provide access to personal information under Ontario's child and family services law. As part of its mandate, the IPC investigates complaints about privacy and access to personal information.

We also provide information and education. We are available to consult with service providers to support their compliance with Part X of the *CYFSA*.

Please visit www.ipc.on.ca for the latest guidance on Part X, including frequently asked questions and orders or decisions made by our office.

PART ONE – UNDERSTANDING THE RIGHT OF ACCESS TO INFORMATION

Part one of this guide aims to help service providers understand the right of access and its exceptions.

For example, consider a scenario where a former client sends you an access request. She would like a copy of a specific record related to the services she received from you last year. You search your client record systems and find one record that is responsive to her request.

Now you must determine whether or not the former client, or "requester," has a right to access some or all of the information in the record. In making this determination, you will need to consider whether the record:

- contains the requester's personal information, is related to providing her a *CYFSA* service, and is in your custody or control
- is dedicated primarily to the provision of a service to the requester
- contains information subject to any of the six access exceptions

RECORDS OF PERSONAL INFORMATION, RELATING TO *CYFSA* SERVICES, IN YOUR CUSTODY OR CONTROL

To determine whether you have an obligation to release the record to the requester — in this case your former client — your first step is to determine whether the record is:

a) a record of her personal information

b) related to the provision of a *CYFSA* service to her and

c) in your custody or control

A) PERSONAL INFORMATION

The right of access only applies to records of personal information. Personal information means recorded information about an **identifiable individual**.

Information is about an identifiable individual if it is about the individual in a personal capacity, and they can be identified from the information (either alone or by combining it with other information). Even without a name, a record may contain personal information, if the individual can be identified.

Personal information can be recorded in any format, including paper or electronic records, or video footage.

You may sometimes receive a request for records that contain no personal information — for example, the requester may be seeking access to certain policies, procedural documents or contracts. In this case, Part X of the *CYFSA* would not apply. You might choose to release the records in some cases, but you are not required to do so under Part X.

The right of access only applies to records of personal information. Personal information means recorded information about an identifiable individual.

B) RELATED TO THE PROVISION OF A SERVICE TO THE INDIVIDUAL

The right of access only applies to records related to the provision of a "service" to the individual. Service is defined as a program or service provided or funded **under the *CYFSA*** or provided under the authority of a *CYFSA* licence.

The right of access does not apply to personal information unrelated to providing a service to the individual under the *CYFSA*. For example, it wouldn't apply to certain human resources records or records related to programs that are provided and funded under other legislation.

If an individual requests a record unrelated to the provision of a *CYFSA* service to them, Part X does not apply. In some cases you might choose to release the record, but you are not required to do so under Part X.

The requested records must relate to the provision of a service to the individual.

C) IN YOUR CUSTODY OR CONTROL

The right of access applies to records in the **custody or control** of your organization, regardless of where the information came from.

- **Custody:** You usually have "custody" of a record if it is in your possession (e.g., in your database or paper files). However, simply possessing the record is not enough to determine custody. To have custody of a record, you must also have some right to deal with it and some responsibility for its care and protection. For example, an employee's personal journal, unrelated to work, would not be in your custody even if it happens to be stored at their work station.
- **Control:** Even if a record is not in your possession, it could potentially be under your control. For example, if you have authority to manage a record related to your mandate and function and you rely on it for business purposes, it may be under your control regardless of whether or not you physically possess it. A record held by your consultant, for example, could be in your control in some circumstances.

Records can be in the custody or under the control of the service provider — it doesn't have to be both. "Custody" and "control" are not defined in the *CYFSA* and must be determined on a case-by-case basis.

Factors to consider when determining whether a record is in the custody or control of an organization include:

- Does the content of the record relate to the organization's mandate and functions?
- Does the organization have a right to possess the record?
- Did an officer or employee of the organization create the record?
- Does the organization have the authority to regulate the record's content, use and disposal?

It **is** possible to have custody or control of a record that was not originally created by your organization. For example, if a child is referred to you by another service provider and you maintain and rely on the referral records to provide services to the child, the referral records would likely be in your custody or control even though they were authored by the other provider.

It is also possible for a record (or a copy of a record) to be in the custody or control of more than one service provider. For example, if two providers are authorized to share certain records relating to a child they are both serving, it is possible for both providers to have custody or control of the records.

In some cases you may determine that a requested record is not in your custody or control. For example, if an individual asks a children's aid society to provide access to certain records, the society may determine that the records are actually in the custody or control of a **different** children's aid society. The society that has custody or control of the records should be the one to make a decision about access to those records.

If you are unsure whether you have custody or control of a record after considering these factors, you may want to seek legal advice.

EXCLUSIONS

Access and other rights under Part X do not apply to some personal information, even if it relates to providing a *CYFSA* service and is in your custody and control. These are commonly referred to as exclusions. Part X excludes the following information:

- adoption information, once the adoption is finalized
- records in Ontario's Child Abuse Register
- records subject to court-ordered production to a children's aid society (*CYFSA*, subsections 130(6) and 130(8))
- court-ordered assessment reports related to potential admission of a child to secure treatment, where a court order withholds all or part of the report from the child (*CYFSA*, subsection 163(6))

In addition, if a request includes information covered by the *Youth Criminal Justice Act*, you must consider whether prohibitions in the *YCJA* take precedence over Part X. The *YCJA* prohibits the release of certain information.

IS THE RECORD DEDICATED PRIMARILY TO THE PROVISION OF SERVICE TO THE INDIVIDUAL?

You have now confirmed that the record requested by your former client is a record of her personal information, related to providing her services, and is in your custody or control. You have also decided that none of the exclusions apply to the information in the record.

Your next step is to ask whether the record is **dedicated primarily** to the provision of services to her.

If a record is dedicated primarily to the provision of services to the requester, she has a right of access to the entire record — subject to the exceptions explained in the next section — even if it incidentally contains information about other individuals and other matters. Note that Part X does not include an overarching access exception that requires you to always redact another individual's personal information. It does, however, contain other exceptions (such as where access will lead to a risk of serious harm) that **may** require redaction of other people's personal information in some cases.

If the record is not dedicated primarily to the provision of services to the requester, she has a right to access only her own personal information that can be severed from the rest of the record. The personal information, once severed, would also be subject to the exceptions explained below.

For example, joint logs or progress reports relating to multiple clients may not be dedicated primarily to the requester. In these cases, the requester's personal information is but one part of a larger record dedicated to several clients.

Or you might determine that a service plan or case note is related to the provision of service to a family with three children, but is dedicated **primarily** to providing services to one particular child in the family. If so, the other siblings would have a right of access to only their own personal information that could be reasonably severed from the record.

Determining whether a record is dedicated primarily to providing services to an individual is important because it dictates the extent of the individual's right of access to the record. Deciding this issue under similar legislation, the IPC has considered:

- Would the record exist if it weren't for the provision of service to the individual?
- Is providing a service to the individual central to the purpose for which the record exists?
- Is the record related to other matters, for example, legal advice?
- Would the record typically be found in an individual's file?
- Does the record contain information about many individuals to whom service has been provided (such as a schedule)?
- Is the record several steps removed from the actual service experience?

The evaluation of whether a record is dedicated primarily to providing services to a certain individual should be done on a record-by-record basis. It may not always be the case that every record you have filed under an individual's name is dedicated primarily to providing services to that person.

The following example is based on a complaint made to the IPC under Ontario's health privacy law, the *Personal Health Information Protection Act*. Several health privacy examples are included in this guide because of the similarities between the right of access under Part X of the *CYFSA* and under *PHIPA*.

> Under Ontario's health privacy law, an individual requested access to records of his health information from a hospital. Some of the records were emails between hospital staff which listed several other patients to be referred for further health care. The hospital determined that these records were not "dedicated primarily to" the personal health information of the requester. The individual made a complaint to the IPC.

In *PHIPA* Decision 57, the IPC agreed with the hospital. It found that the individual's health information was not central to the purpose of the emails, and that they would exist regardless of whether they contained his information. The individual's right of access to the emails was therefore limited to the portions of his own personal health information that could reasonably be severed from the rest of the record.

DO ANY ACCESS EXCEPTIONS APPLY TO THE INFORMATION IN THE RECORDS?

You have now reviewed the record requested by your former client, and have confirmed that it is dedicated primarily to providing her services.

The final step is to determine whether any **access exceptions** apply to the information in the record. If so, the former client does not have a right of access to that part of the information.

There are six "access exceptions" in Part X of the *CYFSA* (section 312(1)). Individuals do not have a right to access a record of their personal information if:

1. It is subject to a legal privilege
2. Another law or court order prohibits its disclosure to the individual
3. The information was collected primarily for a proceeding which has not concluded
4. Access could result in a risk of serious harm to any individual
5. Access could identify an individual who was required by law to provide the information, or
6. Access could identify a confidential source, and you consider it appropriate to keep their identity confidential

If one or more of these exceptions applies, the individual does not have a right of access to that information in the record. You are still required to grant access to the **remainder** of the record, unless it can't reasonably be severed from the information that is not accessible under Part X.

The six access exceptions each provide a separate and independent ground for refusing access. However, it is possible for more than one exception to apply to the same information.

If one or more access exceptions apply, the individual does not have a right to access that information in the record. However, you may still be required to grant access to the remainder of the record.

ACCESS EXCEPTION ONE: LEGAL PRIVILEGE

Individuals do not have a right of access where the record, or the information in the record, is subject to a legal privilege that restricts its disclosure to the individual (section 312(1)(a)).

The term "legal privilege" includes several different types of privileges, including solicitor-client privilege, litigation privilege and settlement privilege.

For example, communications between employees of a service provider and their legal counsel may be subject to solicitor-client privilege. This privilege protects direct communications of a confidential nature between a lawyer and client, or their agents or employees, made for the purpose of obtaining or giving professional legal advice. The privilege applies where information is passed by the solicitor or client to the other as part of the continuum of communications aimed at keeping both informed so that advice may be sought and given as required.

Once it is established that a record constitutes a protected communication between a lawyer and client, the entire communication is generally subject to privilege. Solicitor-client privilege may only be waived (abandoned or given up) by the client in the solicitor-client relationship, and they are under no obligation to do so. For example, a service provider who receives legal advice may choose to waive privilege and release the information in response to an access request. However, if the service provider chooses not to waive privilege, the individual does not have a right to access the information.

Litigation privilege protects records, including a lawyer's work product and material going beyond solicitor-client communications, created for the dominant purpose of litigation. The purpose is to create a "zone of privacy" for lawyers and their clients to prepare for ongoing or reasonably contemplated litigation.

ACCESS EXCEPTION TWO: PROHIBITED BY A LAW OR COURT ORDER

Individuals do not have a right of access to a record where another act, an act of Canada or a court order prohibits its disclosure to the individual (section 312(1)(b)).

This means that if a court has made an order, for example under the *CYFSA*, prohibiting release of a record to an individual, then they cannot gain access to it through Part X. This is also the case if another provincial law, or a federal law like the *YCJA*, prohibits the release of certain information to the individual.

Service providers cannot release information if another law or court order prevents its release. Where this exception applies, you must deny access.

ACCESS EXCEPTION THREE: INFORMATION FOR A LEGAL PROCEEDING

Individuals do not have a right of access where 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 been concluded (section 312(1)(c)).

"Proceeding" is defined broadly in Part X to include proceedings held in, before or under the rules of:

- a court, tribunal, commission, justice of the peace or coroner
- a committee of a College within the meaning of the *Regulated Health Professions Act*

- a committee of the Ontario College of Social Workers and Social Service Workers under the *Social Work and Social Service Work Act*
- an arbitrator or mediator

This exception will not necessarily apply to all records used in a proceeding — it is specific to those collected or created primarily for use in a proceeding.

The exception may apply where proceedings are anticipated but have not yet started. However, the potential for these proceedings must be more than speculative. The proceedings must be **reasonably anticipated**.

Even if a record was collected or created primarily for use in a proceeding, the exception will no longer apply once all appeals or processes resulting from the proceeding have concluded.

If a client requests access to a record and you determine that it was collected or created primarily for use in a proceeding that has not concluded, you may withhold access. If you decide to release a record covered by this exception, consider seeking legal advice before doing so, as releasing the information could affect the proceeding.

ACCESS EXCEPTION FOUR: RISK OF SERIOUS HARM

Individuals do not have a right of access where granting the access could reasonably be expected to result in a risk of serious harm to the individual or another individual (section 312(1)(d)(i)).

Serious harm is not limited to physical harm, and could include other forms of harm as well, such as psychological harm. The risk of serious harm could be to any individual, not just the person seeking access to the information. There is no requirement that the risk of serious harm be imminent.

> Individuals do not have a right of access where granting the access could result in a risk of serious harm to any individual.

You aren't required to prove that disclosure will result in serious harm. However, you must be able to show that the risk of harm is well beyond the merely possible or speculative. It isn't sufficient to take the position that the risk of harm is self-evident. If you deny access based on this exception and the individual complains to the IPC, you must be able to provide evidence about the potential for serious harm. How much and what kind of evidence is needed will depend on the circumstances and seriousness of the consequences.

Under Ontario's health privacy law, an individual requested access to his personal health information from a mental health facility. The operators of the facility denied access on the grounds that releasing the records would result in a risk of serious harm to the nurses who drafted the records.

The individual complained to the IPC and, in *PHIPA* Decision 34, the IPC upheld the decision to deny access. The IPC reviewed evidence provided by the operator of the facility, including notes from the treating psychiatrist, and found it demonstrated a reasonable expectation of serious harm to the nurses if access was granted.

A record may contain information that is potentially uncomfortable or distressing to the individual requesting access. This alone would not be sufficient basis on which to apply this exception — unless you reasonably expect that releasing the record could result in a risk of serious harm (for example, serious psychological harm to the individual). When evaluating what **may** be a risk of serious harm to the requester, consider whether there are supports you could offer that would lessen this risk. This might include advising the requester about the potentially distressing nature of the information in advance, and encouraging him or her to engage a support person when viewing the record.

In determining whether granting access could result in a risk of serious harm, you may choose to consult with staff at your organization who have direct experience with the individual requesting the information.

Additionally, you are permitted to consult with a member of the:

- College of Physicians and Surgeons of Ontario
- College of Psychologists of Ontario
- Ontario College of Social Workers and Social Service Workers

The college member you consult with does not need to work for your organization. Where necessary for the purposes of the consultation, you can share personal information of the requester or other individuals with the college member.

Consulting with one of these professionals may be helpful in deciding whether it is safe to release the records. However, the final determination lies with you.

> An individual sought access to his homecare records. Before providing access, the agency redacted the names of employees who had provided homecare, arguing they would be at risk of harm if their names were released to the individual.
>
> In *PHIPA* Decision 91, the IPC determined there was insufficient evidence that releasing the names could reasonably be expected to result in a risk of serious harm. Although the agency had documented incidents of verbal abuse by the individual towards staff, the IPC found the harm that could potentially result from releasing the employees' names was speculative, and not reasonably likely.

ACCESS EXCEPTION FIVE: IDENTIFYING SOMEONE WHO WAS REQUIRED BY LAW TO PROVIDE THE INFORMATION

Individuals do not have a right of access where 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 (section 312(1)(d)(ii)).

Where an individual was required by law to provide the information, this exception applies to any information that could reasonably be expected to identify them. This includes their name along with any other identifying information. This exception does not cover all information provided by the individual to the service provider — only that which could identify them.

A youth requests access to records containing information about how he was initially referred to a children's aid society several years prior.

The society reviews the records and finds information about a teacher who made the initial call to the society. As required under the "duty to report" (section 125 of the *CYFSA*), the teacher had reported to the society that the youth, who was then a 13-year-old child, may be in need of protection.

Before releasing records to the youth, the children's aid society removes any information that could lead to the identification of the specific teacher, such as the teacher's name, position title and classroom number.

ACCESS EXCEPTION SIX: IDENTIFYING A CONFIDENTIAL SOURCE

Individuals do not have a right of access where 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. This exception only applies if the service provider considers it appropriate that the individual's identity be kept confidential (section 312(1)(d)(iii)).

For example, your client's friend may speak with you and ask that you not reveal that they shared information about the client. Similarly, a professional may provide you with written information and indicate that it is private and confidential. In both cases you have the discretion to deny access to any information that could reasonably be expected to identify these individuals, if you consider it appropriate to do so.

This doesn't mean withholding all the information provided by these individuals — just information that might identify them. For example, if a professional prepares a report but marks it confidential, you have discretion to withhold the professional's name and other identifying information under this exception, but not the rest of the information in the record.

In order to apply this exception you must:

- establish that the information was provided in confidence, whether implicitly or explicitly
- establish that some of the information could reasonably be expected to lead to the identification of the individual who provided the information in confidence

Based on these factors, you must consider whether it is appropriate for you to keep their identity confidential. You should not simply adopt a fixed rule and apply it in all situations — for example, by applying this exception to any report stamped "confidential." Instead, you must consider the specific circumstances of an individual's request.

An individual complained to the IPC following an access request to a health unit under Ontario's health privacy legislation. The health unit had denied access to some of her information, on the grounds it would reveal the identity of confidential sources.

In *PHIPA* Decision 24, the IPC reviewed the withheld information, and was satisfied that granting access would lead to the identification of several individuals who provided information. For the most part, the IPC was also satisfied the information had been provided in confidence. However, the IPC found insufficient evidence that the information from one particular source had been given in confidence, and ordered that information to be released.

ADDITIONAL CONSIDERATIONS

We began with a scenario where a former client requested access to a record from your organization.

To determine whether the former client has a right to access some or all of the information in the record, we outlined three considerations:

1. Is the requested record:
    - a record of the individual's **personal information**,
    - related to the provision of a *CYFSA* **service** to her, and
    - in your custody or control?
2. Is the record **dedicated primarily** to the provision of a service to the individual?
3. Do any of the six **access exceptions** apply to information in the record?

By considering these three questions, you will determine what information the former client has a right to access. You can then issue a decision and prepare the records for release, as outlined in part two of this guide.

PROVIDING REASONS FOR A REFUSAL OF ACCESS

You have determined that the former client has a right to access some, but not all, of the information in the record, in this case, because one of the access exceptions applies. You must now redact the information which the former client is not entitled to access and then release the remainder of the record to her.

When denying access to some or all of a record, you must provide a written explanation to the requester. The requirements for how to do so depend on which access exception applies:

- you must inform the requester when access exception 1 or 2 applies (information is subject to a legal privilege, or another law or court order prohibits its disclosure).
- you have a choice about how to inform the requester when the other access exceptions (exception 3, 4, 5 or 6 — sections 312(1)(c) and (d) of the *CYFSA*) apply. You can choose to:
    - specifically indicate the access exception that applies
    - indicate that one of these exceptions applies, without specifying which one, or
    - refuse to confirm or deny the existence of any record subject to these exceptions

The latter options may be used where specifically naming the access exception could itself cause harm or reveal confidential information. For example, if an individual suspects that his sister had provided information about him in confidence, he may choose to make an access request for "any information about me provided by my sister." If you indicate that access exception six applies (identifying a confidential source), this would **in itself** identify the sister as a source of information. In such cases, you may choose to refuse to confirm or deny the existence of the record.

REFUSING A FRIVOLOUS OR VEXATIOUS REQUEST

Service providers may refuse an access request if it is frivolous or vexatious, or made in bad faith. When refusing a request on these grounds, you must inform the requester.

Refusing an access request on these grounds should not be a routine matter. It is your responsibility to demonstrate that the request is frivolous or vexatious or made in bad faith. There is a high threshold for making this determination.

The IPC has determined, under other privacy legislation, that a request is frivolous or vexatious if it is:

- part of a pattern of conduct (for example, an excessive number of access requests by the same person) that amounts to an abuse of the right of access or interferes with the operations of the institution, or
- made for a purpose other than to obtain access — such as to annoy or harass the institution or to purposefully burden the system

The IPC has described "bad faith" as implying an intent to mislead or deceive someone; or a neglect or refusal to fulfil some duty. Bad faith is not simply bad judgement or negligence — it implies the conscious doing of a wrong for a dishonest purpose.

Service providers may only deny access if they have reasonable grounds for believing the individual's **request for access** is frivolous or vexatious or is made in bad faith. The question is not whether the individual has otherwise engaged in acts of bad faith, outside of their access request.

SUBSTITUTE DECISION-MAKERS CAN REQUEST ACCESS

A substitute decision-maker can request access to an individual's record on their behalf. For example, the custodial parent of a child under 16 years of age who is receiving services from your organization may request access to the child's records with some exceptions.

When a substitute decision-maker requests access on behalf of a capable child, the decision of the capable child prevails if there is a conflict. For example, a custodial parent requests access to her 14-year-old daughter's records, but the daughter indicates that she does not want her mother to have access. Provided the youth is capable, her decision prevails, and the mother's access request must be refused.

PART TWO – HOW TO PROCESS AN ACCESS REQUEST

Part one of this guide focused on an individual's right of access and the exceptions to that right. In part two, we explain requirements and best practices for how to process access requests.

There are six main steps for processing an access request:

1. Receiving the request
2. Searching for records
3. Calculating the timeline for a response
4. Reviewing and preparing the records
5. Issuing a final decision and releasing records
6. Closing the request file

These steps apply to any written request for access to personal information under the *CYFSA*. Note that you may also receive informal requests for access made orally instead of in writing. You may choose to respond to informal requests. However you should advise the individual that an informal request is not subject to the procedural requirements of the *CYFSA*, such as the 30-day response deadline or the right to appeal to the IPC.

STEP ONE: RECEIVING A REQUEST

When you receive a written request for access to personal information, review it as soon as possible to ensure you understand what the requester is looking for. The request should contain enough information to allow you to find the requested records with reasonable effort.

CLARIFYING THE REQUEST

If the request is unclear and does not contain sufficient information to enable you to find the records, you must work with the individual to clarify their request.

When working with a requester to clarify, you can assist them by explaining the types of records your organization holds. The goal is to ensure that you and the requester have a clear understanding about the nature of the records they seek. Once a request has been clarified, you should confirm this in writing.

Sometimes you may receive a request written as a question and it may be unclear if the individual is seeking access to a record. For example, a parent may email you to ask about the dates you met with their child last year. You may be unsure whether the parent is seeking access to a record with the service dates or simply wants a reply to their question.

In such cases, you should clarify with them the nature of their request. If they indicate they would like to make an access request, you should work with them to reformulate the request so you can conduct a search for the appropriate records.

A request should contain enough information to enable you to find the requested records with reasonable effort.

NARROWING THE REQUEST

Individuals may not know how to describe the specific records they seek. As a result, they may word their request broadly, such as a "request for my file." To ensure you provide them with the specific information they are seeking and avoid unnecessary search and review time, it may be helpful to have a discussion with the requester about narrowing their request.

For example, an individual asking for access to their file may only be interested in records related to recent services and they may be open to narrowing the request to a particular time period. However, if the individual does not wish to narrow the request, you must respond to the original broadly-worded request.

Discussions about narrowing a request should take place early in the process, if possible.

ACKNOWLEDGING RECEIPT

It is a best practice to acknowledge having received the access request. You can do this by sending a letter or email to the requester. It should include:

- the date the request was received
- your organization's file or reference number
- details of the request, especially if it was clarified or narrowed
- contact information for someone who can answer additional questions about your organization's information management practices

VERIFYING THE IDENTITY OF THE REQUESTER

You must take reasonable steps to verify the identity of the requester before you can release any personal information to them. It may be helpful to consider this requirement at the start of the process to avoid delays.

In some cases, you may already be satisfied that the requester is who they claim to be, for example because you currently provide services to them. In such cases, there is no need to take additional steps to satisfy yourself of the requester's identity.

If you do need to take additional steps to verify the identity of a requester, you can do so in different ways. For example, you may ask them to sign a form confirming their identity or to produce a piece of identification. You do not have to confirm the authenticity of identification documents provided, unless you have reason to doubt their authenticity.

If a substitute decision-maker makes an access request on behalf of an individual, you can generally rely on their assertion that they have the authority to act as a substitute decision-maker and to make the access request. But if you have reason to believe otherwise, you may request a copy of a power of attorney, custody order, or other document establishing their authority to act as a substitute decision maker. Note it is an offence under the *CYFSA* to make an access request under false pretences.

As a best practice, staff should document steps that have been taken to verify the identity of a requester before records are released.

PRIVACY AND CONFIDENTIALITY REQUIREMENTS

You should treat information about an access request and the requester's identity like any other personal information in your custody or control. This means taking reasonable steps to protect the information from privacy breaches. You should not identify the individual or the nature of the request to other employees within your organization, except where necessary to process the request.

DETERMINING METHOD OF ACCESS

Providing access to records under Part X of the *CYFSA* means making the record available for examination or, if asked, providing the requester with a copy. To ensure there are no delays in processing the request, it may be helpful to clarify with the requester their preferred method of access near the start of the process.

For example, if the individual says they would like to receive a copy of the records, you can send them along with the final decision letter. If the requester prefers to come in person to view the records, you can save the time spent photocopying or scanning records and schedule a visit in advance.

Some service providers may want to design a standard form to be used by individuals requesting access. If so, consider adding a question about method of access. For example, the form could ask requesters to indicate whether they would like to come in to view the records, or if they would prefer to receive a copy of the records in paper or electronic format.

Note that you cannot charge the requester a fee for processing the access request.

STEP TWO: SEARCHING FOR RECORDS

Once you've received an access request, you are required to conduct a reasonable search for the requested records.

A reasonable search occurs when an experienced employee who is knowledgeable in the subject matter of the request makes a reasonable effort to locate records related to the request. For more information about this topic, consult the *Reasonable Search* factsheet available at www.ipc.on.ca.

> A reasonable search occurs when an experienced employee who is knowledgeable in the subject matter of the request makes a reasonable effort to locate records related to a request.

In some cases, such as when only a single record is requested, your search may be simple and straightforward. But in other cases, searching can be more complex. To help ensure that your organization conducts a reasonable search:

- notify staff who may have been involved in providing services and direct them to retrieve or secure records in their possession that may be related to the request
- search all areas where paper and electronic records may be held, including email accounts and archives

Every person involved in the search should document the steps taken during the search and the results. This can help later on if you need to respond to any concerns or appeals about the adequacy of the search.

Documentation should include the:

- name of the person or people who carried out the search
- date the search was conducted
- time taken to complete the search
- locations searched
- records found at each location

Consider developing a worksheet or checklist for staff to use when carrying out searches for records. It is important that your organization has a clear process in place, with step-by-step instructions for staff on how to conduct a proper search.

You should document all steps taken during a search so that you can respond to any concerns or complaints regarding the adequacy of the search.

STEP THREE: CALCULATING THE TIMELINE FOR A RESPONSE

You must respond to an access request within 30 calendar days. If you do not, you are deemed to have refused the request. The requester may then file a complaint with the IPC about your failure to respond.

The day you receive the request is generally considered to be "day zero." When calculating the due date for a request, you should count the 30 days starting from the next calendar day. If you receive the request outside of regular business hours, or on a holiday, the 30 days will start the next day your office is open.

If the 30 day period expires on a day when your office is closed, the deadline to respond to the request falls on the next business day.

REQUESTS THAT REQUIRE CLARIFICATION

Despite the above, if the request needs clarification, the 30-day period does not start until the request has been clarified with the requester. Once the request contains sufficient detail, your 30-day timeline for response begins. You should review the request as soon as possible to determine if it needs clarification.

This only applies when a request lacks sufficient detail to allow you to identify and locate the records. Narrowing the request does not extend the 30-day timeline for response.

TIME EXTENSIONS

At the earliest opportunity, you should assess the time needed to respond to the request. If you are not able to respond within 30 days, you may be able to extend the time to respond by up to an additional 90 days.

A time extension is **only** permissible if:

- responding within 30 days would unreasonably interfere with your operations because the request involves numerous pieces of information or requires a lengthy search, or
- an assessment of the individual's right of access is not possible within the 30 days

In deciding whether an extension is permissible you may consider:

- the scope of the request and the volume of records that must be searched for and reviewed
- the number and nature of the record locations to be searched (e.g., databases and paper record storage facilities)
- the age and complexity of the records
- the impact of completing the request on your organization's other daily functions
- the need for consultation with a professional about a potential risk of harm

If you determine that a time extension is necessary, you must inform the requester in writing within 30 days of receipt of the request. The written notice of extension must clearly state the length of the extension and the reason for it.

You may be entitled to extend the time for fully responding to a request by up to 90 days. If so, you must notify the requester within 30 days of receiving their request.

EXPEDITED ACCESS

In some situations, an individual may need access to their records urgently. If you are satisfied that their request is urgent, you must make a reasonable effort to provide the records within their specified time frame.

STEP FOUR: REVIEWING AND PREPARING THE RECORDS

After the search is complete and all responsive records have been gathered, you must review them to determine the requester's right of access. For more information about determining the right of access, see part one of this guide.

If you determine the requester is not entitled to access some of the information in the record, that information must be redacted before the record can be released. This requires a complete blackout of the information to which the requester does not have a right of access, so that it cannot be read in any form.

There are several ways in which you can redact a record, including:

- using a black marker to conceal the exempted information and then photocopying the record to ensure the information cannot be seen through the black ink
- using computer software to redact information on an electronic copy of the record

When reviewing responsive records, consider how best to preserve the original record. For example, make a photocopy of a paper record and use the copy to do any necessary redacting.

An individual has a right to access personal information that can "reasonably" be severed from the part of a record to which they do not have a right of access. In decisions made under other access and privacy laws, the IPC has found that a record cannot be reasonably severed if it would result in disconnected snippets of words or phrases with no coherent meaning or value.

If a record is withheld in full, you do not need to release fully redacted pages to the requester. Instead, you can provide a decision letter or index of records to advise them of the record or pages being withheld.

The review process can take time. If you are reviewing unfamiliar records, you may find it helpful to consult with a staff member who is more knowledgeable about them.

> Redacting records requires a complete blackout of the exempted information so that it cannot be read in any form.

INDEX OF RECORDS

When you have made a decision to withhold or sever a large number of records, consider creating an **index** of the records, and be sure to number the documents and/or pages. An index can provide the requester with details about what information the records contain and why certain exceptions may apply. If a complaint is made to the IPC, the index can also be useful for parties involved in the complaint process to refer back to.

The index should not include any personal information or any information that would reveal the contents of the records that are being withheld.

It should include a numbered list of all responsive records as well as:

- corresponding page numbers for each record
- date of the record
- a general description of the record
- whether access was denied, or granted in full or in part
- an explanation for why access was denied, where applicable

For more information on how to create an index of records, refer to the sample index in the appendices of this guide.

STEP FIVE: FINAL DECISION AND RELEASING RECORDS

Once you have completed your review of all the records, you must provide a final decision in writing to the requester. The final decision letter should include:

- the reasons for the final decision
- a description of the records being released in full or in part
- any exceptions that were applied to deny access in whole or in part, as appropriate (see "providing reasons for a refusal of access" in part one of this guide,)

- if the requested records do not exist, an explanation that the records could not be located after a reasonable search
- if Part X does not apply to the requested records, an explanation to this effect (for example, see "exclusions" in part one of this guide)
- information about the requester's right to file a complaint to the IPC within six months, along with contact details for the IPC
- the name of the decision maker and contact details for someone who can answer any additional questions about your organization's information management processes

If the requester has asked for a copy of the records, you can mail them with the final decision letter, along with an index of records where appropriate. If the requester has asked to view the records, then you must schedule a time for them to visit.

At the request of the individual, you must provide an explanation of the purpose and nature of the record and any term, code or abbreviation used in the record, as long as you are reasonably able to do so.

For more information on how to write a final decision letter, refer to the sample letter in the appendices of this guide.

Note that you cannot charge the requester a fee for processing the access request.

STEP SIX: CLOSING A REQUEST FILE

Once the final decision has been issued and the records have been released to the individual, the request file can be closed. Before doing so, ensure that all relevant information about the request has been recorded, including:

- details of the search
- the time taken to respond to the request
- any time extension that was applied
- any external consultations that were required
- whether access was denied, or granted in full or in part
- any access exceptions that were applied to the records

All steps that were taken during the process should be documented in detail. This information may be helpful for your own analysis and will assist you in submitting your organization's annual access request statistics to the IPC. For more information refer to the IPC's *Guidelines for Submitting Annual Statistics to the IPC*.

Once the file is closed, it should be kept with the records in an accessible location for at least six months to ensure a faster response in the event the requester files a complaint with the IPC. Once the six-month complaint period has passed, the file can be kept in accordance with your agency's applicable records retention schedules and policies.

COMPLAINTS TO THE IPC

Individuals have a right to complain to the IPC about your response to their access request (or lack of response) within six months.

Where possible, the IPC promotes informal and early resolution of complaints, often through mediation.

If a complaint is not resolved at an early stage, the IPC may decide to conduct a formal review. During a review, the burden of proof to justify the denial of access lies with the service provider. For example, if your organization denied access to a record based on one of the access exceptions, the IPC adjudicator would ask you to provide reasons and evidence for why the exception applies to the requested information.

CONCLUSION

To help you develop policies on how to process a request, please refer to the attached checklist and other appendices.

Visit www.ipc.on.ca for the latest guidance, including frequently asked questions about Part X, and recent orders or decisions made by the IPC.

APPENDICES

CHECKLIST FOR RESPONDING TO AN ACCESS REQUEST UNDER THE *CYFSA*

- ☐ Is the request written or oral? If the request is made orally, let the requester know that the procedural rules of Part X only apply to written requests.
- ☐ Review the request to make sure you understand it and that it is detailed enough to do a search.
- ☐ If the request doesn't have enough information or detail, contact the requester to clarify the request.
- ☐ Once the request has been clarified, confirm the request in writing with the requester.
- ☐ Confirm with the individual how they would like to access the information. Would they like to view the records in person or receive a copy in paper or electronic format?
- ☐ Do you need to confirm the identity of the individual requesting the information or their substitute decision-maker? If yes, document the steps taken to confirm the identity.
- ☐ Identify all physical locations, record repositories, and databases to search for records.
- ☐ Begin search for records.
- ☐ Notify all appropriate staff of the request and instruct them to retrieve and preserve all responsive records. Give staff a deadline to provide you with all responsive records.
- ☐ If the request results in a large number of records, consider contacting the requester to discuss possible options for narrowing the request. The requester is not obligated to narrow their request.
- ☐ If the requester wants to narrow the request, confirm the new scope of the request with them in writing.
- ☐ If a time extension is needed to complete the request, inform the requester in writing of the extension and the amount of extra time required. This must be done as soon as possible and no later than 30 days after receiving the request.
- ☐ Review all responsive records to determine the requester's right of access, including whether any of the access exceptions apply. Where appropriate, consult with other professionals regarding the risk of harm from the release of the records.
- ☐ Redact any information to which the requester does not have a right of access.
- ☐ When you are withholding or severing a large number of records, prepare an index of the records and include information about any exceptions applied.

- [ ] Create a final decision letter and send it to the requester within 30 days (or within the extended timeline of not more than 90 additional days that you previously specified to the requester).
- [ ] If the records are being disclosed (partially or in full), schedule a time for the requester to come in and view them. If the requester wants a copy of the records, you can send it with the final decision letter.
- [ ] After records have been released, close the file. Keep the request file, and any records associated with it, for at least six months in case the requester files a complaint with the IPC.
- [ ] Record relevant information about the request, including the information required for annual statistical reporting to the IPC.
- [ ] After the six month complaint period ends, you may store the request file according to your organization's retention schedule.

SAMPLE DECISION LETTER – FULL ACCESS

January 28, 2020

PERSONAL AND CONFIDENTIAL

Name
123 Main Street
Main Town, Ontario
A1A 2B2

Dear Name:

Re: Request No. 2020-001

Thank you for your letter dated January 1, 2020, which we received on January 3, 2020. We understand from your letter that you are seeking access to records of your personal information under the *Child, Youth and Family Services Act, 2017* (the *CYFSA*).

You requested the following: _____

We thoroughly searched our records and found approximately ___ pages of records in response to your request.

These records are _____ *(e.g., case notes, service plans)*. They were used by our office for the purposes of _____.

Attached please find a copy of the records you requested. We are granting you access to all of these records in full. If you have any questions or concerns, please contact *[person at your organization]* at (123) 456-7890 or email@service.provider.ca.

If you are not satisfied with the results of your access request, you may make a complaint to the Office of the Information and Privacy Commissioner of Ontario (IPC). Your complaint must be filed within six months of receiving this letter.

Complaints to the IPC can be filed online at www.ipc.on.ca, or mailed to the IPC registrar at 2 Bloor Street East, Suite 1400, Toronto, ON, M4W 1A8. The IPC can be reached at 416-326-3333 or toll free at 1-800-387-0073.

Should you wish to make a complaint to the IPC, you should provide them with:

- a copy of the access request you made to us
- a copy of this final decision letter, including the request number at the top of the letter
- the reason why you are not satisfied with the response

Sincerely,

Name
Position
Name of Service Provider

Encl.

SAMPLE DECISION LETTER – REFUSING ACCESS TO SOME INFORMATION

January 29, 2020

PERSONAL AND CONFIDENTIAL

Name
124 Main Street
Main Town, Ontario
A1A 2B2

Dear Name:

Re: Request No. 2020-002

Thank you for your email sent on January 2, 2020. As confirmed in our phone call on January 3, 2020, you are seeking access to records under the *Child, Youth and Family Services Act, 2017* (the *CYFSA*).

You requested the following: _____

We thoroughly searched our records and located approximately ___ pages of records in response to your request.

These records are *[e.g., case notes, service plans]* and were used by our office for the purposes of _____.

After reviewing these records, we have decided to grant you access to these records, with two exceptions:

- One paragraph on page 4 of the first record has been redacted. It is subject to a legal privilege and cannot be released in accordance with section 312(1)(a) of the *CYFSA*.
- We have determined that the second record is not dedicated primarily to the provision of a service to you. This means your right of access is limited to your own personal information from the record. We have therefore redacted information from the record that is about other people and/or other matters, in accordance with section 312(3) of the *CYFSA*.

Enclosed please find a copy of the records to which you have been granted access.

If you are not satisfied with the results of your access request, you may make a complaint to the Office of the Information and Privacy Commissioner of Ontario (IPC). Your complaint must be filed within six months of receiving this letter.

Complaints to the IPC can be filed online at www.ipc.on.ca, or mailed to the IPC registrar at 2 Bloor Street East, Suite 1400, Toronto, ON, M4W 1A8. The IPC can be reached at 416-326-3333 or toll free at 1-800-387-0073.

Should you wish to make a complaint to the IPC, you should provide them with:

- a copy of the access request you made to us
- a copy of this final decision letter, including the request number at the top of the letter
- the reason why you are not satisfied with the response

If you have any questions or concerns about your request or about the enclosed records, please contact *[person at your organization]* at (123) 456-7890 or email@service.provider.ca.

Sincerely,

Name
Position
Name of Service Provider

Encl.

SAMPLE DECISION LETTER – NO RECORDS FOUND/PART X DOESN'T APPLY

January 30, 2020

PERSONAL AND CONFIDENTIAL

Name
125 Main Street
Main Town, Ontario
A1A 2B2

Dear Name

Re: Request No. 2020-003

Thank you for your letter dated January 3, 2020, which we received on January 6, 2020. We understand that you are seeking access to records under the *Child, Youth and Family Services Act, 2017* (the *CYFSA*).

You requested the following: _____

Option 1: After a thorough search of our records, we were unable to find any records that relate to your request.

Option 2: We have determined that the *CYFSA* (Part X) does not apply to the records you have requested. *[If possible, provide information about how the individual could obtain access to the records]*.

If you are not satisfied with the results of your access request, you may make a complaint to the Office of the Information and Privacy Commissioner of Ontario (IPC). Your complaint must be filed within six months of receiving this letter.

Complaints to the IPC can be filed online at www.ipc.on.ca, or mailed to the IPC registrar at 2 Bloor Street East, Suite 1400, Toronto, ON, M4W 1A8. The IPC can be reached at 416-326-3333 or toll free at 1-800-387-0073.

Should you wish to make a complaint to the IPC, you should provide them with:

- a copy of the access request you made to us
- a copy of this final decision letter, including the request number at the top of the letter
- the reason why you are not satisfied with the response

If you have any questions or concerns, please contact *[person at your organization]* at (123) 456-7890 or email@service.provider.ca.

Sincerely,

Name
Position
Name of Service Provider

SAMPLE INDEX OF RECORDS

1	Summary of case officer notes	5, 7	Partial	312(1)(d)(iii)	Denied in part, information could reveal the identity of another individual who provided information in confidence
2	Interview with a third party	9-12	No	312(1)(c)	Denied in full, information is part of a current court proceeding
3	Interview with requester	13-16	Yes	n/a	n/a
4	Email between internal staff	20	Partial	312(1)(d)(i)	Denied in part, information could cause serious harm to an individual
5	Handwritten staff notes	22-25	Yes	n/a	n/a

Providing Access to Personal Information under the *Child, Youth and Family Services Act*

A Guide for Service Providers

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

November 2019