PRIVACY

MAY 2019

Part X of the *Child, Youth and Family Services Act*: A Guide to Access and Privacy for Service Providers

Disclaimer: This guide is about Part X of the *Child, Youth and Family Services Act, 2017*, and its regulations.

The guide should not be relied on as a substitute for the legislation itself, or legal advice. It is not an official legal interpretation of Part X and does not bind the Office of the Information and Privacy Commissioner of Ontario (IPC). For the most up-to-date version of this guide, visit the IPC's website at **www.ipc.on.ca.**

Acknowledgements

The IPC gratefully acknowledges the contributions of representatives from the following organizations, who assisted with the preparation of this guide:

- Association of Native Child and Family Service Agencies of Ontario
- Ministry of Children, Community and Social Services
- Ontario Association of Children's Aid Societies
- Ontario Association of Residences Treating Youth
- Ontario Residential Care Association

CONTENTS

TERMS USED IN THIS GUIDE iv

INTRODUCTION 1

About the IPC 1

Overview of the *CYFSA* 2

DOES PART X OF THE *CYFSA* APPLY TO YOU? 3

Are you a service provider? 3

Are you subject to other privacy legislation? 3

What information does Part X apply to? 5

COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION 10

Collection of personal information 11

Use of personal information 13

Disclosure of personal information 16

CONSENT AND CAPACITY 20

Elements of consent 20

Conditional consent and withdrawal of consent 22

Capacity to consent 23

Substitute decision-makers 24

SAFEGUARDING AND MANAGING PERSONAL INFORMATION 27

Responding to privacy breaches 28

Retention, transfer and disposal 30

Public statement about information practices 31

ACCESS TO RECORDS OF PERSONAL INFORMATION 33

Individual's right of access 33

Service provider's response to access requests 36

CORRECTION OF RECORDS 40

Individual's right to correction 40

Service provider's response to correction requests 41

OFFENCES AND IMMUNITY 43

THE ROLE OF THE INFORMATION AND PRIVACY COMMISSIONER 44

IPC Complaint Process 44

Reporting annual statistics to the IPC 45

IPC's broader role 46

DEFINITIONS 47

ENDNOTES 50

TERMS USED IN THIS GUIDE

CYFSA – Child, Youth and Family Services Act

The *CYFSA* is an Ontario law that governs certain programs and services for children, youth, and families. The *CYFSA* is divided into parts, and it is **Part X** of the *CYFSA* that is the subject of this guide. Part X sets the rules that service providers must follow to protect privacy and enable access to records of personal information.

IPC – Information and Privacy Commissioner of Ontario

The Office of the Information and Privacy Commissioner is the oversight body for Part X of the *CYFSA*. The commissioner is appointed by and reports to the Legislative Assembly of Ontario and is independent of the government of the day. The IPC is the author of this guide. For more information about the IPC's role, see page one.

Other privacy legislation

FIPPA – Freedom of Information and Protection of Privacy Act

MFIPPA – Municipal Freedom of Information and Protection of Privacy Act

PHIPA – Personal Health Information Protection Act

These are three other Ontario privacy laws overseen by the IPC. These laws impact some service providers, and not others. They are not the subject of this guide but are discussed on pages three to five.

Personal information

Personal information means recorded information about an identifiable individual.

When a service provider is collecting information, personal information also includes information that is not recorded. See the full definition on page 48, and discussion on pages five and six.

Service provider

Part X of the *CYFSA* introduces requirements for "service providers," which are defined to include persons or entities that provide services funded under the *CYFSA*, or under the authority of a licence under the *CYFSA*. See page 49 for the full definition.

Introduction

INTRODUCTION

Part X of the *Child, Youth and Family Services Act* sets the rules that service providers must follow to protect privacy and enable access to personal information, effective January 1, 2020.

If you are a service provider seeking to understand your obligations under Part X, this guide is for you. It provides an overview of the core rules for collecting, using, disclosing, safeguarding and managing personal information, consent and capacity, and access to and correction of personal information. It also explains how these rules are enforced. Additional Part X requirements, such as those related to research and prescribed entities, are addressed only at a high level.

This guide is not a substitute for legal advice. If you are unsure of how to apply Part X in a given situation, you should contact the person in your organization responsible for ensuring compliance with Part X, or a lawyer.

If you have general questions about Part X, you can contact the Ministry of Children, Community and Social Services or the Office of the Information and Privacy Commissioner of Ontario (IPC).

You may find it helpful to read this guide with the *CYFSA* itself. If so, the guide's endnotes point you to the relevant sections of the legislation. You may also want to consult the definitions section on page 47. In addition to summarizing the requirements of Part X, this guide also presents some best practices and practical examples.

ABOUT THE IPC

The IPC provides oversight of Ontario's access and privacy laws, including Part X. These laws establish the rules for how Ontario's public institutions, health information custodians and service providers may collect, use, and disclose personal information.

As part of our mandate, we investigate privacy complaints related to personal information and ensure compliance with Ontario's access and privacy laws. Any person can file a complaint with the IPC about anyone who has or is about to break the rules of Part X. For more information about our complaints process, see pages 44.

Part of our mandate at the IPC is to provide information and education. We are available to consult with service providers to support their compliance with Part X.

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

OVERVIEW OF THE *CYFSA*

The *CYFSA* is an Ontario law that governs certain programs and services for children, youth, and families, including:

- child welfare
- residential care
- adoption
- youth justice
- children's mental health
- First Nations child and family services
- Inuit child and family services
- Métis child and family services

The **paramount purpose** of the *CYFSA* is to promote the best interests, protection and well-being of children.[1] One of several additional purposes is to recognize that appropriate sharing of information to plan and provide services is essential for creating successful outcomes for children and families.

Children and youth receiving services under the *CYFSA* have certain rights, including the right to:

- express their views freely and safely about matters that affect them
- be consulted on the nature of the services provided and participate in decisions about services provided to them
- raise concerns or recommend changes to their services, and to receive a response, without interference or fear of coercion, discrimination or reprisal[2]

Part X of the *CYFSA* sets out rules for service providers regarding privacy and access to personal information. With limited exceptions, service providers must have consent to collect, use or disclose personal information. They must also take steps to safeguard this information and must notify people if there is a breach of their privacy. Service providers must give individuals access to their records of personal information on request, subject to limited exceptions, and must respond to requests for correction of inaccurate or incomplete records.

DOES PART X OF THE *CYFSA* APPLY TO YOU?

Does Part X of the *CYFSA* apply to you?

Two questions will help determine whether and to what extent Part X applies to your organization: Are you a service provider? If so, are you already subject to other privacy laws?

ARE YOU A SERVICE PROVIDER?

A service provider[3] under Part X of the *CYFSA* is:

a) a person or entity that provides a service funded under the *CYFSA* (children's aid societies, including Indigenous child well-being societies, are one example)

b) a licensee, meaning the holder of a licence under Part VIII of the *CYFSA* (Adoption Licensing) or Part IX (Residential Licensing)

c) a lead agency[4]

d) the Minister of Children, Community and Social Services[5]

e) any additional person or entity[6] prescribed through a regulation

While a licenced operator of foster homes is defined as a service provider, a foster **parent** is not.

ARE YOU SUBJECT TO OTHER PRIVACY LEGISLATION?

Once you have determined that you are a service provider, the next step is to consider whether you are already subject to privacy legislation. You are exempt from much of Part X if you are:

- a health information custodian under the *Personal Health Information Protection Act*, when collecting, using or disclosing personal health information
- an institution under the *Freedom of Information and Protection of Privacy Act* or its municipal counterpart, the *Municipal Freedom of Information and Protection of Privacy Act*

Are you a health information custodian under *PHIPA*?

PHIPA governs the collection, use and disclosure of **personal health information** by health information custodians. Section 3 of *PHIPA* sets out who is a custodian, while section 4 sets out what is personal health information.

If you are a service provider who is also a custodian under *PHIPA,* the core rules of Part X do not apply to your collection, use or disclosure of personal

health information (*PHIPA* would apply instead).[7] The only sections of Part X which **do** apply are:

- sections 283-284 (Minister's powers to collect, use and disclose personal information)
- section 285 (Application of Part X)
- section 293 (Disclosure for planning and managing services)
- section 294 (Records of mental disorders)

Note that if you are a health information custodian who collects, uses and discloses personal information that is **not** personal health information, then Part X may apply to that information.

> A multi-service organization operates a children's aid society. It also runs a children's mental health program, for which it collects information about its clients' health history and provides health care as its primary purpose.
>
> Both *PHIPA* and Part X of the *CYFSA* would apply to different parts of this organization. For example, if a client wanted to access their records of personal health information from the organization's mental health program, they could do so under *PHIPA.* If they wanted to access their records of personal information from the children's aid society, they would do so under Part X of the *CYFSA*.

Are you an institution under *FIPPA* or *MFIPPA*?

FIPPA is a law that applies to provincial public institutions including the Ministry of Children, Community and Social Services. *MFIPPA* is its municipal counterpart — it applies to school boards, municipalities and other municipal institutions.[8]

If you are a service provider and an institution under *FIPPA* or *MFIPPA*, the core rules of Part X do not apply to you.[9] The only sections of Part X which **do** apply are:

- sections 283-284 (Minister's powers to collect, use and disclose personal information)
- section 285 (Application of Part X)
- section 293 (Disclosure for planning and managing services)
- section 294 (Records of mental disorders)
- sections 295-305 (Consent, capacity and substitute decision-making)

A father wants access to his records of personal information from a program operated directly by the Ministry of Children, Community and Social Services. Can he make an access request?

Yes, but not under Part X of the *CYFSA.* Because the ministry is an institution under *FIPPA*, the core rules of Part X, including the rules about access to records of personal information, do not apply to the ministry. The father would need to make an access request under *FIPPA*.

WHAT INFORMATION DOES PART X APPLY TO?

Now that you have determined you are a service provider to whom Part X applies, the next step is to understand what **types** of information Part X covers.

Generally, Part X applies to **personal information**, which is in the **custody or control** of a service provider, and which relates to the provision of a **service**. However, there are exceptions for certain types of records (such as adoption records) to which Part X does not apply. We will now walk through each of these concepts in turn:

Part X applies to personal information, which is in the custody or control of a service provider, and which relates to the provision of a service.

a) What is personal information?

Part X applies to personal information, which means "recorded information about an **identifiable individual**."[10] It does not apply to records that contain no personal information. For example, this might include things like capital funding records, organizational policies, or building contracts.

Information is about an identifiable individual if:

- it is about the individual in a personal capacity
- the individual can be identified from the information (either alone or by combining it with other information)

Examples include a person's name when combined with other information about them, such as their address, sex, age, education, or medical history. This is not a complete list; many other kinds of information may still qualify as personal 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 records, such as written case notes
- electronic records, such as in a client information system
- photographs and video footage, including from security cameras

When a service provider is collecting information, the definition of "personal information" also includes information that is **not** recorded. This means that when a service provider collects personal information, they must follow the rules of Part X even if the information is collected verbally, for example through a phone call or intake interview.[11]

It doesn't matter whether a record was created **before or after** Part X came into force. Even if an individual's personal information was recorded many years before, they have a right to access their record and you must protect it against privacy breaches.[12]

b) What is "custody or control"?

Part X applies to records held by a service provider. More specifically, it applies to records "in the custody or under the control" of a service provider.

"Custody" and "control" are not defined in the *CYFSA* and must be determined on a case-by-case basis. Part X applies to records that are either in the custody **or** under the control of the service provider. It doesn't have to be both.

- **Custody**: You usually have custody of a record if it's in your **possession** — in your electronic database or paper files, for example. However, simply possessing the record is not enough to determine the question of custody. To have custody of a record, you must also have some right to deal with the record and some responsibility for its care and protection.[13] For example, your employee's personal journal, unrelated to work, would not be in your custody even if it is 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 you physically possess it. A record held by your consultant, for example, could be in your control in some circumstances.

The IPC and the courts have reviewed complaints and appeals under other privacy legislation involving this matter,[14] and have tended to take a broad and liberal approach to determining whether a record is in an organization's custody or control. The IPC has developed a list of factors to consider in

determining whether a record is in the custody or control of an institution, including:

- Did an officer or employee of the institution create the record?
- Does the content of the record relate to the institution's mandate and functions?
- Does the institution have a right to possession of the record?
- Does the institution 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 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.

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

c) What does collected for or relating to the provision of a service mean?

For Part X to apply, the personal information must be collected for or related to the provision of a **service**. Part X defines service as a program or service that is provided or funded under the *CYFSA* or provided under the authority of a licence.[15] It includes services for children and their families related to:

- child protection
- residential care
- community support and prevention
- physical or mental disabilities
- mental health
- adoption
- services or programs under the *Youth Criminal Justice Act* or *Provincial Offences Act*[16]

Generally speaking, personal information that is **not** collected for or related to the provision of a service under the *CYFSA* is not covered by the core Part X rules for collection, use, disclosure, access, and correction. For example, this could include certain human resources records or records related to programs that are not provided or funded under the *CYFSA*.

A community organization is funded by the Ministry of Children, Community and Social Services to offer youth support services under the *CYFSA*. The agency also offers other programs including social programs for seniors. To what extent does Part X apply?

- Because it provides a service funded under the *CYFSA,* the organization fits the definition of a "servicer provider," and Part X will apply to some of its records.
- However, the agency's seniors' programs are not provided or funded under the *CYFSA*. Part X will not apply to the organization's collection, use and disclosure of information for its seniors' programs, because Part X only applies to records related to the provision of a **service under the *CYFSA***.

d) Exceptions:

In general, Part X applies to personal information in the custody or control of a service provider that relates to the provision of a service under the *CYFSA*. However, there are exceptions.[17] Most of Part X does not apply to:

- the use or disclosure of **adoption** information by a licensee or children's aid society, once the adoption is finalized[18]
- records in the Child Abuse Register[19]
- records subject to court-ordered production to a children's aid society[20]
- court-ordered assessment reports related to potential admission of a child to secure treatment, where the court has made an order to withhold all or part of the report from the child[21]

Service providers should also be aware of **confidentiality provisions** in other parts of the *CYFSA* which prevail over Part X, including rules against publicly identifying children and families who participate in child protection hearings.[22]

Finally, it is important to note that where federal laws such as the *Criminal Code* or *Youth Criminal Justice Act* prohibit disclosure of personal information, they prevail over Part X. This means that service providers cannot disclose information under Part X if the *YCJA* or another federal law prohibits the disclosure.

An adoption practitioner is licensed by the Ministry of Children, Community and Social Services to provide private adoption services under the *CYFSA*, including assessing potential adoptive parents. Does Part X apply to this practitioner?

- Yes, as a licensee under the CYFSA, the practitioner is a "service provider" covered by Part X.
- However, the *CYFSA* establishes rules for the confidentiality of adoption information after an adoption order is made and these rules prevail over most of Part X. This means that if a person wanted access to information about their finalized adoption, it would be other legislation, and not Part X, which would guide this process.

Collection, use and disclosure of personal information

COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION

Part X protects privacy by setting rules for how service providers collect, use and disclose personal information. In this section, we look at a few overarching rules for collection, use and disclosure, before focusing on each of these three activities in turn.

These rules apply when you are collecting personal information from **any individual** for the purpose of providing a service, or using or disclosing that information. If you are providing services to a child, for example, these rules apply to how you collect, use and disclose the personal information not only of the child, but also of other individuals who may be involved in the services, such as her parents.

As a service provider, you must have an individual's **consent** to collect, use or disclose personal information **unless** the *CYFSA* authorizes you to do so without consent.[23]

Consent — including who can give consent and what makes a consent valid — is explained on pages 20-23 of this guide. Permitted collection, use and disclosure *without* consent is explained on pages 12-18.

Even when you have consent, there are three **limits** on when and how much personal information you can collect, use or disclose**:**[24]

1. You must ensure, to the best of your knowledge, that the collection, use or disclosure is **necessary for a lawful purpose**. For example, even if a client gave consent for you to use their personal information "in any way you please," you may only use it where necessary for a lawful purpose.

2. You must only collect, use or disclose as much personal information as is **reasonably necessary** to provide a service. For example, even with consent it would not be appropriate to collect information about clients' political affiliations, unless you somehow need this information to provide service.

3. You must not collect, use or disclose personal information where **non-personal** information will serve the same purpose. For example, if you are applying for a grant and are asked to give evidence of successful client outcomes, you could provide de-identified or statistical information. In this case, there would be no need to disclose clients' personal information in the application.

Note that these limitations do not apply to personal information that you are **required by law** to collect, use or disclose.

COLLECTION OF PERSONAL INFORMATION

You must have an individual's **consent** to collect, use or disclose personal information **unless** the *CYFSA* authorizes you to do so without consent.

While Part X does not define what it means to "collect" personal information, collecting information is generally understood to mean gathering or obtaining it from any source and in any manner (including verbally or in written or electronic format).

For example, when you conduct an intake interview, receive a report from a concerned teacher about a child who may be in need of protection, or ask a parent to fill out a needs assessment form, you are collecting personal information.

Collection of personal information can be either **direct** or **indirect**.

A collection is **direct** when the information comes from the person to whom the information relates (or their substitute decision-maker[25]). For example, during an intake interview between a worker and a youth, the worker is directly collecting the youth's personal information.

A collection is **indirect** when the information comes from a third party, and not from the individual or their substitute decision-maker. For example, if a teacher phones a children's aid society about a child who may be in need of protection, the society would indirectly collect the child's personal information from the teacher.

Direct collection

When service providers collect information directly, they usually do so with **consent**. This consent may be implied or you can choose to seek explicit consent.[26]

Implied consent is consent that is not given specifically, but which can be inferred based on the individual's actions and the facts of a particular situation. For example, if a young person expresses interest in a program and volunteers their personal information to enroll, their consent for the collection of their information may be implied.

In this guide, we use the term **explicit consent** to refer to consent that is more than just implied. It must be stated explicitly, either verbally or in writing. For example, although explicit consent is not required for direct collections of personal information, you may decide it is a good practice to ask all new clients to sign a consent form before you collect their information.

Under Part X, when you directly collect personal information from any person, you must give them **notice** that you may use or disclose their information in accordance with Part X.[27] There are various ways you could give this notice. For example, you could advise the individual that their information may be used or disclosed in accordance with Part X and answer any questions they may have. You could also direct the person to a written statement about your information practices under Part X. For more information, see "Public statement about information practices," page 31.

Sometimes you may need to collect information directly from an individual who is **not capable** of giving consent.[28] For example, a children's aid society conducting a protection investigation may need to interview a toddler separately from his parents. Service providers may directly collect personal information from an incapable person without consent in three situations. The collection must be **reasonably necessary** either to:

- provide a service, where it is not possible to obtain consent (for example, from a substitute decision-maker) in a timely manner
- assess, reduce or eliminate a risk of **serious harm** to any person or group
- assess, reduce or eliminate a risk of **harm** to a child (if you are a children's aid society)

Some of the rules for collection, use and disclosure of personal information are based on whether something is "**reasonably necessary."** What does this mean?

- Part X does not define the term "reasonably necessary." It is context-specific.
- In general, for something to be **necessary**, it must be more than merely helpful.
- The standard here is one of reasonableness. For example, even if you don't know for sure, is it **reasonable** to believe that the collection of information is necessary to assess, reduce or eliminate a risk of serious harm to a person or group?

Indirect Collection

Service providers may also collect information indirectly. Sometimes they do so with **consent.**[29] For example, a parent may consent to the service provider obtaining information from a specialist who has assessed their child. In this case, the provider would need the parent's explicit consent for the indirect collection, and cannot rely on implied consent.

As a service provider, there may be times when you need to indirectly collect information, **without consent.** Part X permits you to do so only in the following situations:

First, you can indirectly collect information without consent if it is **permitted or required by law.**[30] For example, when a children's aid society receives a call from a teacher about a child who may be in need of protection, the society can collect this information from the teacher without consent.

Receiving reports about children in need of protection is part of the society's mandate under the *CYFSA* and is permitted by law.

Second, service providers may indirectly collect personal information without consent if:

- the information is **reasonably necessary** to provide a service or to assess, reduce or eliminate a risk of **serious harm** to a person or group *and*
- it is not possible to collect personal information directly that can reasonably be relied on as **accurate and complete**, or in a **timely** manner.[31]

> A community service provider is working with a youth who is struggling in school. The service provider wants to speak directly with the teenager's teacher to help understand his classroom challenges.
>
> Speaking with the teacher to gather information would be an indirect collection of the teenager's personal information. In this case, the information would be helpful – but **not reasonably necessary** – to provide services or reduce a risk of serious harm. The provider must therefore get the youth's consent before speaking with his teacher.

Finally, children's aid societies can collect personal information from one another (or from child welfare authorities outside Ontario) if the information is reasonably necessary to assess, reduce or eliminate a **risk of harm to a child**.[32] A children's aid society would not require consent in this situation.

In summary, service providers may only collect personal information with consent, or in situations where collection without consent is specifically permitted by Part X.[33] Any other collection is unauthorized and contravenes the *CYFSA*. Providers must take reasonable steps to prevent unauthorized collection of personal information.[34] These steps might include developing clear policies and procedures for collecting information, and regularly training staff.

USE OF PERSONAL INFORMATION

Once you have collected personal information for the purpose of providing a service, Part X governs the ways you may **use** this information.

There is no definition of "use" in Part X. Generally, using personal information means viewing or dealing with the information in a manner that does not include disclosing it. For example, when a social worker prepares for a

meeting with a family by reviewing their team's case notes from a previous meeting with the family, they are "using" the information in the case notes.

When you use personal information, you must take reasonable steps to ensure it is as **accurate**, complete and as up-to-date as necessary for the purposes for which it is used.[35] You must exercise judgment about how accurate the information needs to be. For example, personal information used to deliver certain services may in some cases require a higher degree of accuracy than information used solely for administrative purposes.

Service providers can use information with the **consent** of the individual (provided that, to the best of the service provider's knowledge, the use is necessary for a lawful purpose).[36] Service providers can also use personal information **without consent** if certain conditions are met.

As a service provider, you can use personal information without consent for the purpose it was collected or created. You can also use it for all the functions reasonably necessary for carrying out that purpose, including providing the information to an **officer, employee, consultant or agent** of your organization.

> A group home requests that all staff arriving to their shift review the log written by their coworkers from the previous shift. The purpose of the log is to improve continuity between shifts and ensure staff are aware of any important issues.
>
> When staff members arrive at work and review the log, they are "using" the information. This use is necessary for ensuring continuity of services which is the purpose of maintaining the log.

In some cases, an individual may instruct you **not** to use their information.[37] For example, a parent may consent to their information being used for a single point-in-time service, but not for any other purpose. The service provider is responsible for complying with the individual's instruction. However, there are exceptions:[38]

- Even if an individual has explicitly instructed otherwise, you can still use the information if reasonably necessary to assess, reduce or eliminate a risk of **serious harm** to any person or group.
- If you are a children's aid society, you can also use the information if reasonably necessary to assess, reduce or eliminate a risk of **harm** to a child.[39]

You may also use personal information, without consent, for the following purposes:[40]

- where permitted or required by law
- for planning, managing and delivering services that you provide or fund (including resource allocation, evaluation, monitoring and preventing fraud)
- for risk and error management, or quality assurance
- to seek consent (in this case you must use only their name and contact information)
- to dispose of or de-identify the information
- for research conducted by the service provider, subject to certain requirements[41]
- for a proceeding (or contemplated proceeding) where the service provider is or is expected to be a party or witness and the information relates to a matter at issue
- if you believe on reasonable grounds that the use is reasonably necessary to assess, reduce or eliminate a risk of serious harm to a person or group

In summary, if you collect personal information to provide a service, you can **only** use it for that purpose or for one of the additional purposes set out in Part X or with the individual's consent. Any other use of the information is not authorized and contravenes the *CYFSA*.

An example of an unauthorized use of information is **snooping**. Employees reading records for reasons not related to the performance of their duties, such as curiosity or financial gain, is an unauthorized use of information not permitted under Part X.[42]

> An employee is searching through the service provider's case management system and notices an intake record under a familiar name. Although the record is not relevant to their job, the employee is curious and reads the record to confirm that it involves one of their neighbours.
>
> This represents an **unauthorized use** of the neighbour's personal information and is not allowed under Part X.

DISCLOSURE OF PERSONAL INFORMATION

In the course of providing services, you may sometimes need to **disclose** personal information. There is no definition of "disclose" in Part X. Generally, it means releasing or making the information available to another person or organization.

Note that sharing information with an officer, employee, consultant or agent of your own service provider is considered a use, and not a disclosure when it is for the purpose for which the information was collected, or for one of the other purposes set out in the "use" section of the legislation.[43]

When you are disclosing personal information, you need consent, unless Part X permits the disclosure without consent.

While implied consent is acceptable for collection and use of information in some cases, consent for disclosure must be explicit.

Disclosure with consent

You may disclose personal information with the explicit consent of the individual to whom the information relates as long as the disclosure is for a lawful purpose. While implied consent is acceptable for collection and use of information in some cases, consent for disclosure must be explicit. This explicit consent may be written or verbal, but verbal consent is only valid if you make a written record of it. See Consent, pages 20-23.

> A service provider has directly collected an individual's personal information to register them for a literacy program at their request.
>
> When intake staff share this information with their colleague who leads the literacy program, this is a "**use**" of information. The service provider can rely on the implied consent of the individual to use their information to deliver the literacy program.
>
> Later, the literacy program leader concludes that the individual needs parenting support. She wants to share their information with another organization that provides parenting classes. This is a "**disclosure**" of the information, requiring explicit consent from the individual.

Disclosure without consent

You may disclose personal information **without consent** in certain situations that are set out in Part X.[44] This includes where the disclosure is **permitted or required by law**. For example:

- All individuals are required to report to a children's aid society if they reasonably suspect that a child may be in need of protection.[45] Part X is not a barrier to this disclosure.

- Children's aid societies are required by the *CYFSA* to consult with a representative chosen by each of a child's bands and First Nation, Métis or Inuit communities whenever they are proposing to provide certain services to the child, such as developing a safety plan. With one exception, consent is not required in these situations.[46]

Other examples of where you may disclose personal information without consent:

- if there are reasonable grounds to believe that the disclosure is necessary to assess, reduce or eliminate a **risk of serious harm** to a person or group
- to a law enforcement agency in Canada to aid an investigation[47]
- to a legal representative or litigation guardian, for certain purposes, such as to represent the individual in a proceeding
- to comply with a summons, order or procedural rule relating to the production of information in a proceeding, such as a proceeding before a court or tribunal[48]
- to contact a relative, friend or potential substitute decision-maker in certain instances, such as where the individual is injured or incapacitated

Children's aid societies can disclose personal information to one another (and to child welfare authorities outside Ontario) if it is reasonably necessary to assess, reduce or eliminate a risk of harm to a child.[49] The consent of the individual to whom the information relates is not required.

> A youth tells a drop-in program worker about her plans to harm herself, but instructs the worker not to tell anyone else. The worker consults with their supervisor. After considering the situation — including the level of risk and degree of urgency — and weighing various options for responding, they decide to disclose the information to the group home where the youth lives.
>
> This type of disclosure is permitted under Part X, which allows for disclosure without consent if necessary to assess, reduce or eliminate a **risk of serious harm** to a person or group.

Disclosure to successors and for planning and managing services

There are special rules for disclosing personal information to a **successor**, such as another service provider that is taking over the delivery of services to your clients.[50] These rules might apply, for example, when two children's aid societies are amalgamating or when a new Indigenous child well-being

society is designated to serve Indigenous children within an area currently served by another society. They might also apply when a community organization is ceasing operations and another service provider plans to take over some of its services.

After entering into an agreement with a potential successor to keep the personal information confidential and secure and not to retain it longer than necessary, you may disclose personal information to them, without consent, to allow them to assess and evaluate your operations.

Before you transfer records to your successor, you must make reasonable efforts to notify the individuals whose records will be transferred.[51]

Note that a singular transfer of a specific file, such as where a client moves and their file is transferred from one service provider to another, would likely not fall within the successor provisions. In such instances, the file could be disclosed with consent or where permitted by Part X.[52]

Finally, service providers can disclose personal information for purposes such as planning services, managing services, and research. Service providers may disclose personal information to:

- the **Minister of Children, Community and Social Services** for certain purposes, including determining compliance with the *CYFSA*, and improving the quality of services[53]
- **prescribed entities** for analysis or compiling statistics for planning, managing and evaluating services, if certain conditions are met[54]
    - Two entities that are currently prescribed for this purpose are the Canadian Institute for Health Information and the Institute for Clinical Evaluative Sciences.
- a **First Nations, Inuit or Métis person or entity**, for analysis or compiling statistics for planning, managing and evaluating services.[55] Certain conditions apply, including that the personal information to be disclosed must relate to First Nations, Inuit or Métis individuals.

Accuracy and documentation

For any disclosure of personal information, you must take reasonable steps to ensure the information is as accurate, complete and as up-to-date as necessary for the purpose of the disclosure. Alternatively, you must inform recipients of any limitations on the accuracy, completeness, or up-to-date character of the information.[56]

A family you worked with five years ago requests that you forward their records to their new service provider.

Before sending the records, you make a note on the records identifying them as out of date, and specifying when they were last updated.

Service providers should document disclosures of personal information. For example, if you believe a disclosure without consent is reasonably necessary to reduce a risk of serious harm, you should record what information you disclosed, when and to whom, along with the reason for doing so.[57]

Consent and Capacity

CONSENT AND CAPACITY

As a service provider, you must get **consent** before collecting, using or disclosing personal information unless the *CYFSA* authorizes you to do so without consent. In this section, we explain the requirements for getting consent, the meaning of capacity to consent and the rules for substitute decision-makers.

ELEMENTS OF CONSENT

If you require consent to collect, use or disclose personal information, the consent must:[58]

- be provided **by the individual** or their substitute decision-maker (the individual cannot provide a valid consent if they are not capable)
- not be obtained through **deception or coercion**—the individual must give the consent freely and voluntarily
- **relate to the information** that you are collecting, using or disclosing *and*
- be **knowledgeable**

A consent is considered knowledgeable if it is reasonable to believe that the individual knows the **purposes** of the collection, use or disclosure and knows that they have the right to give, withhold or withdraw consent.[59] It is generally reasonable to believe that an individual knows the purposes for the collection, use or disclosure if you:

- post a notice describing the purposes, where it is likely to come to the individual's attention
- make the notice readily available to the individual
- give the individual a copy of the notice *or*
- otherwise communicate the content of the notice to the individual

This notice can be given in the form of your public statement of information practices if the statement describes the purposes of the collection, use or disclosure and explains that an individual may give, withhold or withdraw consent. For more information, see "Public statement about information practices," page 31.

It is not always reasonable to believe that a written notice or statement of information practices will sufficiently inform someone of the purposes of

a collection, use or disclosure. For example, when low literacy skills or a language barrier prevent someone from understanding your notice, you must find another way to communicate the relevant information.

Consent may be implied in some cases

When you directly collect personal information to provide a service, an individual's consent may be **implied**.[60] Implied consent is consent that is not given explicitly, but which can be inferred based on the individual's actions and the facts of a particular situation. You may imply consent for the use of personal information if you collected it directly and to provide a service. For example, if a parent gives you their personal information directly so that you can provide a service, you may imply their consent to use the information for this purpose.

In other cases, consent must be **explicit** and not merely implied. This includes any consent required for:

- an indirect collection (see page 12)
- a collection other than to provide a service
- a use of personal information, if the information had been collected indirectly, or was collected for a purpose other than providing a service
- a disclosure (see page 16)

Consent may be written or verbal

An explicit consent can be given in writing or verbally.[61] However, you can only rely on a verbal consent if you make a written record of:

- the name of the individual who gave the consent
- the information to which the consent relates *and*
- how you notified the individual about the purposes of the collection, use or disclosure

Presumption of consent's validity

You may presume that a consent is valid and has not been withdrawn, unless it is unreasonable to do so.[62] This applies whether you directly obtain an individual's consent, or receive a document claiming to be a record of their consent.

You can also rely on a person's claim they have authority to consent on someone else's behalf — for example, as a substitute decision-maker — except where it is unreasonable to do so.[63] For example, it would be unreasonable to rely on a person's claim that they have authority to consent as a child's custodial parent if you are aware that they no longer have custody of the child.

You receive a letter from a social worker at another organization, requesting certain information about a youth you have served. The letter includes a consent for disclosure form with the youth's signature. Can you disclose the information?

Yes, you may disclose the information to the social worker. You may presume the consent is valid and has not been withdrawn unless it is not reasonable to do so (for example, if you are aware of a more recent document from the individual withdrawing consent).

CONDITIONAL CONSENT AND WITHDRAWAL OF CONSENT

Individuals may choose to place a **condition** or limit on their consent. For example, they may consent to have some records of personal information disclosed to a third party, but not others.

You must respect these conditions **unless** they restrict or prevent a service provider from recording personal information where required by law or by an established standard of professional or institutional practice.[64] For example, an individual providing information about a child who may be in need of protection cannot restrict a child protection worker from documenting this information.

A youth would like to receive ongoing support from an Indigenous child well-being society. However, she tells the society she doesn't want them to document or store any of her personal information, because she knows an employee of the society and is worried they could read the record.

The society worker explains that legislation and professional standards require them to document certain information in order to provide the service. They speak with the youth about other ways her concerns may be addressed. For example, this could include options for restricting that employee's access to the record.

An individual may also choose to **withdraw** their consent at any time by providing notice to the service provider.[65] If an individual notifies you verbally that they are withdrawing consent, you should record the direction, the date you received it, and how you became aware of their direction. Ensure that other employees within your organization who are providing services to the individual are aware that consent has been withdrawn.

Note that a withdrawal of consent does not apply in situations where consent is not required to collect, use, or disclose personal information. For example, if the law requires disclosure, you can disclose even if an individual has not provided consent or has withdrawn their consent.

CAPACITY TO CONSENT

Individuals must be **capable** of providing consent for the collection, use or disclosure of personal information. Capable means they are able to:

- understand the information that is relevant to deciding whether to consent *and*
- appreciate the reasonably foreseeable consequences of giving, withholding or withdrawing the consent[66]

When determining someone's capacity to consent, you can **presume** that an individual of any age is capable, **unless** you have reasonable grounds to believe they are not. For example, while Part X does not link capacity to age or provide a minimum age for consent, it would be reasonable to conclude that an infant is incapable of providing consent.

When determining someone's capacity to consent, you can **presume** that an individual of any age is capable, **unless** you have reasonable grounds to believe they are not.

Note that a person can be capable of consenting at one time, but incapable at another.[67] For example, a traumatic event or a new medication might temporarily affect an individual's capacity to provide consent.

Individuals can also be capable of providing consent for some parts of their personal information, but not others.[68] For example, a child may be capable of consenting to the disclosure of most of her record to another service provider, but incapable of appreciating the consequences of disclosing or not disclosing a particularly sensitive part of the record.

When assessing if an individual is capable:

- provide them with all the relevant information, including the purpose for the proposed collection, use or disclosure. When you are collecting the information directly, advise them that it may be used or disclosed in accordance with Part X
- consider asking the individual to repeat the relevant information back to you — it may help you to assess their level of understanding
- ensure that language barriers, speech impairments or cultural differences do not influence your assessment of capacity

Determining an individual is incapable

When you determine that someone is incapable, it affects their right to make some or all decisions about their personal information. You must give the individual information about the consequences of this determination if it is reasonable to do so.[69]

The determination of incapacity is specific to an individual's rights **under Part X** — it does not impact their right to make decisions about other matters unrelated to their personal information.

Service providers are responsible for determining capacity under Part X. However, people have a right to challenge determinations of incapacity through an application to the Consent and Capacity Board.[70] You should make them aware of this right. More information about Ontario's Consent and Capacity Board is available at **www.ccboard.on.ca**.

SUBSTITUTE DECISION-MAKERS

Substitute decision-makers can consent on behalf of an individual to the collection, use or disclosure of the individual's personal information. They can also act on behalf of the individual to make any request, give any instruction, or take any step that Part X allows an individual to take — including an access request.[71]

As described below, certain persons may act as a substitute decision-maker on behalf of:

- an **incapable** person (of any age)
- a **child** under the age of 16 — whether capable or incapable — subject to the exceptions below
- a **capable** person over the age of 16 who has authorized the substitute decision-maker in writing

Substitute decision-makers for incapable individuals

If an individual of any age is not capable of consenting, the *CYFSA* sets out who can be their substitute decision-maker for Part X.[72] These persons, ranked in order, are the incapable individual's:

1. substitute decision-maker under the *Health Care Consent Act,* for specified purposes[73]
2. guardian of the person or property
3. attorney for personal care or property
4. representative appointed by the Consent and Capacity Board[74]
5. spouse or partner
6. parent (not including access parent), **or** a children's aid society or other person who is lawfully entitled to consent in the place of the parent[75]
7. access parent (i.e., a non-custodial parent with only a right of access to the child)

8. sibling
9. other relative

A person lower on the list (for example, an access parent) may be the individual's substitute decision-maker only if no one higher on the list (for example, a custodial parent) exists and meets the criteria for consenting on behalf of the individual.[76] Substitute decision-makers must be 16 years of age or older, available, willing, and capable. [77]

Substitute decision-makers for children under the age of 16

For a child **under the age of 16,** the custodial parent, children's aid society or other person authorized to give, withhold or withdraw consent on the parent's behalf can act as the child's substitute decision-maker.[78] They can consent on behalf of the child for the collection, use or disclosure of the child's information **except** where the information relates to:

- counselling which the child consented to on their own under the *CYFSA* (or the previous *Child and Family Services Act*) or
- treatment about which the child made a decision under the *Health Care Consent Act*

Subject to these exceptions, a custodial parent or children's aid society can act as substitute decision-maker for a child under the age of 16, whether the child is capable or incapable. However, if the child is capable, then a decision to give, withhold or withdraw consent by the **capable child prevails** over a conflicting decision by the custodial parent or society.[79]

A decision to give, withhold or withdraw consent by the capable child prevails over a conflicting decision by the custodial parent or children's aid society.

A mother phones a service provider to register her ten-year-old for a voluntary community program. She provides the intake worker with her son's personal information, and consents on his behalf for its collection and use. If the mother is a custodial parent, the intake worker can rely on this consent, because a custodial parent may consent on behalf of a child younger than 16-years-old.

Later, the mother and son are visiting the service provider's office together. The son informs the worker that he doesn't want to be part of the program and doesn't want the provider to have any of his information. The mother disagrees. At this point, the service provider must determine whether the son is capable. If so, his decision to withdraw consent **prevails** over his mother's decision, and the provider can no longer collect or use his information.

Substitute decision-makers for capable individuals over the age of 16

Any capable individual, age 16 or older, may choose to authorize another capable individual, age 16 or older, to be their substitute decision-maker for the purposes of Part X.[80] For example, a 17-year-old working with an advocate could make this advocate her substitute decision-maker, by presenting a written, signed statement to the service provider. The advocate could then consent on her behalf for a collection, use or disclosure of her personal information.

Considerations for substitute decision-makers

When a substitute decision-maker gives, withholds or withdraws consent or provides an instruction on behalf of an individual, they must consider:

- the wishes, values and beliefs they know, or believe, the individual holds or would want reflected in decisions about their personal information[81]
- if the benefits of the collection, use or disclosure outweigh the risk of any negative consequences
- if the purpose of the collection, use or disclosure can be otherwise achieved
- if the collection, use or disclosure is required to satisfy a legal obligation

If you believe that a substitute decision-maker has **not complied** with their obligation to consider these factors, you may apply to Ontario's Consent and Capacity Board for a determination.[82]

SAFEGUARDING AND MANAGING PERSONAL INFORMATION

Safeguarding and managing personal information

Whether in paper, electronic or any other format, records of personal information must be safeguarded at all times.

As a service provider, you must take **reasonable steps** to protect personal information in your custody or control against theft, loss or unauthorized collection, use, disclosure, copying, modification or disposal.[83] There is no precise definition of a "reasonable step." What is reasonable depends on the circumstances. It will change as you use new technologies, and as new threats or vulnerabilities emerge.

When determining how to protect personal information, you should assess the nature of the records, including:

- the sensitivity and amount of personal information in the record
- the number and nature of people with access to the information
- any threats and risks associated with the manner in which the information is kept

Based on this assessment, you should put in place measures to safeguard privacy. These measures should be regularly reviewed to ensure they continue to be reasonable. In many cases, reasonable measures will include the following safeguards:

Administrative Safeguards	Technical Safeguards to Protect Electronic Data	Physical Safeguards
• privacy and security policies and procedures • staff training on privacy and security • confidentiality agreements • privacy impact assessments	• strong authentication and access controls • logging, auditing and monitoring • strong passwords and encryption • maintaining up-to-date software by applying the latest security patches • firewalls, hardened servers, intrusion detection and prevention, anti-virus, anti-spam, and/or anti-spyware software • protection against malicious and mobile code • threat risk assessments	• controlled access to locations where personal information is stored • locked cabinets • access cards and keys • identification, screening and supervision of visitors

Under Ontario's health privacy law, the IPC reviewed a privacy breach involving a hospital clerk who viewed hundreds of patients' records without authorization. The hospital discovered the privacy breach during a proactive audit and reported it to the IPC.

In *PHIPA* Decision 64, the IPC reviewed and summarized the hospital's privacy policies, confidentiality agreements, privacy warnings, staff training and auditing policies. The IPC concluded that although the employee's use of information was unauthorized, in the circumstances of the breach and the hospital's response to and investigation of it, the hospital had taken **reasonable steps** to protect the information.

A privacy breach occurs when personal information is stolen or lost or is collected, used or disclosed without authority.

RESPONDING TO PRIVACY BREACHES

A **privacy breach** occurs when personal information is stolen or lost or is collected, used or disclosed without authority.

In the event of a privacy breach, you should immediately notify the relevant staff in your organization and then identify the scope of the breach and take the steps necessary to contain it. We recommend that you have a privacy breach protocol in place detailing the steps to take in response to a breach, in what order, and by whom. Additional information about responding to privacy breaches is available at **www.ipc.on.ca**.

You should take the following steps to **contain** a privacy breach:

- retrieve and secure any personal information that has been collected, used or disclosed without authority
- ensure that no copies, including digital copies, have been made or retained by the individual who was not authorized to receive or use the information
- determine whether the breach would allow unauthorized access to any other personal information — for example on an electronic information system — and take necessary steps to prevent a further breach, such as changing passwords or temporarily shutting down your system

You must **notify individuals** at the first reasonable opportunity of any breach in which their personal information in your custody or control was lost, stolen or used or disclosed without authority.[84] This notice must:

- provide a general description of the breach in easy-to-understand language
- inform the individual of any steps you have taken to:
    - mitigate adverse effects on the individual and
    - prevent a similar breach from happening
- provide contact information for one of your employees who can provide additional information *and*
- advise the individual of their right to complain to the IPC

You must also **notify the IPC** and the Minister of Children, Community and Social Services of any privacy breach that meets certain criteria.[85] This includes any breach you determine to be significant based on the sensitivity and volume of the information breached, the number of service providers involved and the number of people affected.

These types of privacy breaches must also be reported to the IPC:

- those involving stolen personal information
- breaches in which personal information was used or disclosed by someone who knew or should have known they were doing so without authority
- breaches where it is likely personal information has or will be further used or disclosed again without authority
- a privacy breach that is part of a pattern of similar breaches
- a breach that results in an employee being terminated, suspended or disciplined, or resigning

Breach reports can be submitted to the IPC by mail, or online at **www.ipc.on.ca**. The IPC will review the information you provide, including a description of the breach and your response to it and may, in some cases, decide to conduct an investigation.

To minimize the risk of further breaches, you should review your existing policies, procedures, training programs and safeguards and consider whether you need to make changes. You should also keep a record of all breaches. Statistics about breaches involving a theft, loss, or unauthorized use or disclosure of personal information must be submitted to the IPC as part of your annual statistical report. For more information, see pages 45-46.

A youth worker informs their supervisor that they mistakenly sent correspondence containing a client's personal information to the wrong person.

The supervisor notifies the organization's privacy officer, and together with the worker they take the following steps:

- contain the breach by ensuring the person who received the letter in error has returned it or disposed of it securely
- notify the individual whose privacy was breached (including the required information in the notice)
- make a record of the breach
- take action to prevent similar breaches – in this case, by sending all staff a reminder of privacy policies and tips for avoiding a similar mistake

If the breach was accidental, isolated, and limited in scope, they are not required to report it to the Minister of Children, Community and Social Services or IPC.

RETENTION, TRANSFER AND DISPOSAL

You must have safeguards in place to ensure you are retaining, transferring and disposing of personal information appropriately and securely.[86]

Part X requires that you take reasonable steps to ensure records of personal information in your custody or control are retained, transferred and disposed of in a secure manner. In addition, you must comply with the requirements in the *CYFSA* and its regulations, as described below.

You must have a **retention policy** that sets out the types and classifications of records of personal information you hold, how long you will retain them, and how you will dispose of or transfer them. Part X does not dictate how long you must retain records, but it does require you to consider certain factors in deciding your retention periods.[87] For example, you must consider whether another service provider has custody or control of the record or requires it to provide services. You must also consider whether the *CYFSA* or another law includes requirements for retention of the record.[88]

Regardless of your retention periods, if an individual requests **access** to a record, you must retain it for as long as it takes to fulfil the request and allow for any recourse the individual has (including complaints to the IPC and any

subsequent appeals or reviews). For more information about individuals requesting access to personal information, see pages 33-39.

To securely **dispose** of records, you must protect against their theft, loss, and unauthorized use or disclosure.[89] You must also ensure that the personal information in the record cannot be reconstructed or retrieved after disposal. For this reason, recycling records of personal information or leaving intact documents for garbage pick-up are unacceptable methods of disposal.

To securely dispose of records, you should:

- Develop a secure destruction policy to complement your retention policy that determines what records should be destroyed, by whom, and when.
- Ensure that any agreement you enter into with an external service provider, such as a shredding company, to dispose of records addresses the issue of secure disposal.
- When disposing of electronic records, either physically destroy the storage media or overwrite the information stored on the media. The best method will vary depending on the type of media.[90]

You must also document which records you have disposed of — in a way that does not include the personal information contained in the record.

You must make a written statement about your information practices available to the public.

PUBLIC STATEMENT ABOUT INFORMATION PRACTICES

You must make a written statement about your information practices available to the public. This could be included on your website or on posters or brochures in your workplace.[91]

Your public statement must include an easy-to-understand description of:

- your **information practices** (This means 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[92])
- how an individual may obtain access to or request correction of a record of personal information held by your organization
- how to contact your organization
- how to make a complaint to your organization and to the IPC

It is good practice to write clear, concise statements describing the information practices of your organization, taking care to avoid technical and legal language. You can consider providing additional details through a separate document. For example, a poster in your waiting room could

provide a high-level statement about your information practices, which directs readers seeking more detail to a brochure or website.

If you use or disclose personal information **outside the scope** of your publicly stated information practices, and without consent, you are required to inform the individual at the first reasonable opportunity. You are also required to make a note about the use or disclosure and attach it to the individual's record.[93] This might apply, for example, if you use personal information for research after stating in your description of information practice that you will only use personal information for direct service delivery.

ACCESS TO RECORDS OF PERSONAL INFORMATION

Access to records of personal information

Individuals have a right under Part X to access their records of personal information from service providers, subject to limited exceptions. Service providers must respond to access requests within 30 calendar days and are not permitted to charge fees. In the following section, we review individuals' access rights, exceptions, and detailed rules for how you must respond.

INDIVIDUAL'S RIGHT OF ACCESS

All individuals, regardless of age, have a right to access records of their personal information in your custody or control that relate to providing them with a service.

The general right of access in Part X applies to all records of personal information in the service provider's custody or control, regardless of where the information originated. The right of access is not limited to records in the custody or control of a service provider that were **created by** that service provider.

> A youth requests access to all records in his case file at a group home. One of the records was authored by another service provider. Can the group home release this record to the youth even though it was not created by group home staff?
>
> If the group home has **custody or control** of the record, the youth **would** have a right to access the record from the group home, subject to any applicable access exceptions. For a discussion of "custody or control," see pages 6-7.

Access exceptions

There are a few exceptions to the right of access. Individuals do **not** have a right to access their record of personal information if:

- it is subject to a legal privilege restricting its disclosure to the individual
- another act or a court order prohibits its disclosure to the individual *or*
- the information was collected or created primarily in anticipation of or for use in a legal proceeding which has not concluded

Additionally, individuals do not have a right to access their record of personal information if granting access could reasonably be expected to:

- result in a risk of serious harm to any individual[94]
- lead to the identification of an individual who was required by law to provide information in the record to the service provider *or*
- lead to the identification of an individual who provided the information either explicitly or implicitly in confidence — if the service provider considers it appropriate to keep their identity confidential

If one of these exceptions applies, the individual does not have a right of access to that information in the record. However, you would still be required to grant access to the remainder of the record of personal information if you can **sever** or redact the information to which the exception applies.[95]

> A children's aid society receives an access request from a youth looking for records related to a society investigation.
>
> The society reviews the records and finds information about a neighbour who made the initial call to the society to report that the family's children may be in need of protection, as required by the "duty to report."
>
> Before releasing records to the youth, the children's aid society removes or redacts any information which could lead to the identification of the neighbour, who was required by law to provide this information to the society.

In addition to these exceptions, Part X also allows service providers to refuse access if a request is **frivolous or vexatious** or made in bad faith.[96] The IPC has found, 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)

There is a high threshold for deciding that a request is frivolous or vexatious. Refusing an access or correction request on these grounds is not a routine matter and should not be undertaken lightly.

Is the record dedicated primarily to the provision of service to the individual?

Service providers must ask themselves whether the record is dedicated primarily to the provision of service to the individual requesting access:

- If so, the individual has a right of access to the **entire record** — subject to the exceptions previously noted — even if it incidentally contains information about other individuals and other matters.
- If not, the individual only has a right to their own **personal information** that can reasonably be severed from the rest of the record.

> A youth who was in the care of a children's aid society wants to access their old service plan. The society reviews the plan, which contains limited personal information about the youth's parents and former foster parent. Nevertheless, the society determines that the record is **dedicated primarily** to the provision of services to the youth.
>
> After ensuring that none of the access exceptions apply to any information in the record (for example, there is no risk of serious harm to the parents, foster parents, or any individual), the society grants the youth full access to the record, without removing or redacting the personal information of the other individuals.

Determining whether a record is dedicated primarily to providing services to the individual is important because it dictates the access the individual has to a record. Deciding this issue under other legislation, the IPC has considered whether:

- the provision of a service to the individual is central to the purpose for which the record exists
- the record would exist "but for" the provision of a service to the individual
- the record is qualitatively related to other matters, for example, legal advice
- the record would typically be found in an individual's file
- the record contains information about many individuals to whom service has been provided (such as a schedule)
- the record arises indirectly and several steps removed from the actual service experience[97]

It may not always be the case that every record filed under an individual's name is dedicated primarily to providing services to that person. Determining whether a record is dedicated primarily to the provision of service to the person requesting access to it should be done on a record-by-record basis.

How are access requests made?

While you can choose to respond to verbal or informal requests for access, the request must be in writing for the procedural access rules of Part X to apply.[98] There is no requirement in the *CYFSA* for individuals to use a certain form or to submit the request in a certain way. Even if you'd prefer for individuals to make access requests by filling out a designated form, you must still respond to requests that come in other formats, such as email.

In addition, there is no requirement for a person requesting access to a record to specify that they are seeking access **under Part X of the *CYFSA***. However, it may be helpful to clarify this with the requester in certain circumstances, such as where more than one privacy and access law could apply.

Access requests must include enough detail to enable you to identify and locate the record with reasonable effort. If a request does not contain enough detail, you must **offer to assist** the requester in clarifying the request.[99] You should do so as soon as you receive a request that is not sufficiently detailed. Once the request contains sufficient detail, your 30-day timeline for response begins.

> A former client emails you to request a copy of her complete file. She provides her first and last name, but no other identifying details. You check your case management system and see three people with the same name. This means you are unable to identify which are the requester's records.
>
> You **assist** the requester in clarifying her request by replying the following day to advise that you require additional information, such as her date of birth, to locate the records. One week later, you receive a reply containing the necessary information. At this point, the access request has been made, and you have 30 days in which to respond.

SERVICE PROVIDER'S RESPONSE TO ACCESS REQUESTS

When you receive an access request, you must conduct a reasonable search to locate the responsive record(s). A reasonable search means an experienced employee made a reasonable effort to locate the records.

For more information on how to conduct a reasonable search see our fact sheet on this topic, available at **www.ipc.on.ca**.

You must respond to an access request as soon as possible and no later than **30 calendar days** after receiving the request.[100] A service provider that does not respond within 30 days is deemed to have refused the request.[101] The individual may then make a complaint to the IPC.[102]

In some cases, an individual may request expedited access – for example, they may explain that they need the information within two weeks to meet an application deadline for a specific program or service. If you are satisfied with the evidence that they require access in an expedited period, you must provide access within that period, if you are reasonably able to do so.[103]

Outside of expedited access requests, your response is due within 30 calendar days. The response must do one or more of the following:

- **grant access** to some or all of the requested information
- **refuse or decline access** to some or all of the information, with a written explanation
- **extend the deadline** for fully responding by up to 90 days, with a written explanation (this option is **only** available if the criteria outlined on pages 38-39 are met)

These responses are not mutually exclusive. For example, your response might grant access to some information, while refusing access to other information.

You must respond to an access request as soon as possible and no later than **30 calendar days** after receiving the request.

Granting access

Granting access means giving the person requesting access to a record the opportunity to examine it and, at their request, giving them a copy of it. It is not sufficient to provide a summary of the record.

If it is practical to do so, you must explain the purpose and nature of the record and any terms, codes or abbreviations used.

You may not charge a fee for providing access to a record.[104] This rule applies to all of the activities associated with processing an access request. For example, you cannot charge requesters for filing the request, photocopying, postage or the staff time required to process the request.

Before you provide access, you must take reasonable steps to satisfy yourself of the requester's identity.[105] In some cases, this might include the requester signing a confirmation form or showing official identification.

Refusing or declining access

Your written response may also indicate that you are **not** providing access to some or all of the requested records.

If you cannot locate a record after a reasonable search — or if you have concluded that the record doesn't exist, can't be found or that Part X doesn't apply to it — you must clearly indicate this in your response to the requester. You should also notify the requester of their right to file a complaint the IPC.

If you are refusing all or part of the request based on one of the **access exceptions,** you must give written notice to the requester that you are refusing access and that they are entitled to complain to the IPC. In most cases you are also required to inform the requester of any exceptions that apply, as follows:

You **must** inform the requester when one of the following applies:

- the information is subject to a legal privilege
- another act or a court order prohibits its disclosure to the individual
- the request is frivolous or vexatious or made in bad faith

You have **discretion** about how to inform the requester when one of the following access exceptions apply. You can choose to specifically indicate the exception that applies — or to indicate that one of them applies, without specifying which one. You can also **refuse to confirm or deny** the existence of any record subject to these exceptions[106]:

- the information was collected or created primarily in anticipation of or for use in a legal proceeding which has not concluded, or
- granting access could reasonably be expected to:
    - result in a risk of serious harm to any individual[107]
    - lead to the identification of an individual who was required by law to provide information in the record to the service provider or
    - lead to the identification of an individual who provided the information either explicitly or implicitly in confidence, if you consider it appropriate to keep their identity confidential

Extending the deadline

In limited circumstances, a service provider may advise the individual they are extending the deadline for responding to an access request by not more than **90 calendar days.**

An extension is allowed only 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 feasible within the 30 days[108]

If you plan to extend the deadline, you must give the individual **written notice** of the length of the extension and the reason for it — no later than 30 days after receiving the original request.[109] You must then provide a full response, granting and/or refusing access, within the extended time limit. Otherwise, you are deemed to have refused the request.[110] People are entitled to file a complaint with the IPC for any refusal of an access request, including a deemed refusal. They can also complain about the time extension itself. For example, if they don't agree their access request meets the criteria for an extension under Part X.[111]

If you plan to extend the deadline, you must give the individual **written notice** of the length of the extension and the reason for it – no later than 30 days after receiving the original request.

SUBSTITUTE DECISION-MAKERS CAN REQUEST ACCESS

A substitute decision-maker can request access to an individual's record on their behalf.[112] For example, the custodial parent of a child under 16-years-old who is receiving services from your organization may request access to the child's records. In these cases, the custodial parent would "stand in the shoes of" the child to make the request. This would be an access request (sections 312-314 of the *CYFSA*), rather than a disclosure. Any reference to the individual in Part X would be read as a reference to the substitute decision-maker. For example, the requirement to respond to the individual within 30 days would be read as a requirement to respond to the **substitute decision-maker** within that timeframe.

You can rely on a person's assertion that they have authority to request access as a substitute decision-maker unless it is unreasonable to do so.[113] Note that it is an offence under the *CYFSA* to make an access or correction request under false pretences.[114] For more information, see Substitute Decision-Makers, pages 24-26.

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.[115] 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 will be refused.

Correction of records

CORRECTION OF RECORDS

Under Part X, individuals have the right to request correction to records of their personal information, with limited exceptions. As with access requests, service providers must respond to correction requests within 30 calendar days and are not permitted to charge fees. In the following section, we review individuals' correction rights, exceptions, and detailed rules for how you must respond.

INDIVIDUAL'S RIGHT TO CORRECTION

Individuals can request that a service provider correct a record of their personal information if they believe it is inaccurate or incomplete.[116] A substitute decision-maker may also request a correction to an individual's record on their behalf.

A correction refers not only to striking out incorrect information but also to adding information to make a record complete.

There is no age requirement for making a correction request. Note that the right to request a correction from a service provider only applies if the service provider has previously given the individual **access** to the record.

Individuals must submit correction requests to the service provider **in writing**.[117] The law does not require them to use a certain form or submit the written request in a certain manner. This means that even if you prefer for individuals to make correction requests using a designated form, you must still respond to requests that come in other formats, such as through email.

Service provider's duty to correct, and exceptions

You must grant a correction request if the individual demonstrates, to your satisfaction, that the record is inaccurate or incomplete and gives you the information you need to correct the record.

There are two exceptions. You are **not** required to correct a record if:

- it consists of a professional opinion or observation that was made in good faith *or*
- your organization did not create it, and you do not have sufficient knowledge, expertise or authority to correct it

You are also permitted to refuse a correction request if you have reasonable grounds to believe the request is frivolous or vexatious or made in bad faith. For more information about what makes a request "frivolous or vexatious," see access exceptions, page 34.

An individual complained to the IPC under Ontario's health privacy law after a health information custodian refused to correct a social worker's report.

In *PHIPA* Decision 67, the IPC found that the custodian was not obligated to make the requested corrections — because the information in dispute consisted of the social worker's professional opinions and observations, made in good faith.

SERVICE PROVIDER'S RESPONSE TO CORRECTION REQUESTS

The timelines and other rules for responding to a correction request are very similar to those for access requests. You must respond to a correction request as soon as possible, and no later than **30 calendar days** after receiving the request.[118] A service provider that does not respond within 30 days is deemed to have refused the request.[119] The individual may then make a complaint to the IPC.

Your response within 30 days must be in writing and must explain that you are doing one or more of the following:

- **granting** the correction request in whole or in part
- **refusing** the correction request, in whole or in part, with a written explanation
- **extending** the deadline for fully responding by up to 90 days, with a written explanation

Granting the correction

When you grant a correction request, you must provide written notice of how you corrected it. Correcting means:

- **recording** the correct information in the record or, if that's not possible, by ensuring a system is in place to inform those who access the record that it is incorrect or incomplete, and to direct them to the correct information *and*
- **striking out** the incorrect information without obliterating it or, if that's not possible, by labelling it incorrect, severing it, storing it separately and maintaining a link to trace the incorrect information

At the request of the individual, you must give written notice of the correction to the people to whom you have disclosed the information, to the extent it is reasonably possible. An exception to this requirement is where providing notice cannot reasonably be expected to affect the ongoing provision of services.

You may not charge a fee for granting a correction. This applies to all activities associated with processing a correction request.

Refusing the correction request

Your written response may indicate that you are **not** making some or all of the requested corrections. In this case, you must explain why you are refusing the request and must inform the individual of their rights, including the right to file a complaint with the IPC.

Additionally, you must inform the individual of their right to prepare a concise **statement of disagreement** regarding the correction that you are refusing to make, and their right to require you to:

- attach this statement to the record, and disclose it whenever you disclose the related information
- make reasonable efforts to provide the statement to any person to whom you previously disclosed the information — unless the statement cannot be expected to affect the ongoing provision of services

Extending the deadline

In limited circumstances, you may extend the deadline for responding to a correction request by no more than **90 calendar days.** You may only extend the deadline if:

- responding within 30 days would unreasonably interfere with your operations *or*
- it is not reasonably practical to respond within the 30 days, given the time required to complete the necessary consultations[120]

If you plan to extend the deadline, you must give the individual **written notice** of the length of the extension and the reason for it within 30 days of receiving the request. You must then provide a full response, granting and/or refusing the correction, within the extended time limit. Otherwise, you are deemed to have refused the request. For any refusal of a correction request, including a deemed refusal, the individual may file a complaint with the IPC. They may also complain about the time extension itself if they don't agree their request meets the criteria where an extension is permitted by Part X.

OFFENCES AND IMMUNITY

Offences and immunity

In this section, you'll find information about how the rules for privacy and access to personal information are enforced. This includes an overview of offences under Part X, protections against liability and the role of the IPC.

OFFENCES

Under Part X of the *CYFSA,* it is an offence to:[121]

- wilfully collect, use or disclose personal information in contravention of Part X or the regulations
- wilfully dispose of a record in a manner that is not secure or with the intent to evade an access request
- willfully fail to notify an individual, at the first reasonable opportunity, of the theft, loss or unauthorized use or disclosure of their personal information
- wilfully obstruct the IPC or make a false statement to the IPC
- wilfully fail to comply with an order of the IPC
- retaliate against a whistleblower, such as by demoting or firing an employee because they reported a privacy breach to the IPC
- request access or correction of a record under false pretenses
- knowingly make certain false statements about the authority to access a record or to consent on behalf of someone for a collection, use or disclosure of personal information

A prosecution for offences under Part X of the *CYFSA* cannot be initiated without the consent of the Attorney General of Ontario. There is no time limit for commencing these prosecutions. If a person is found guilty, they may be fined up to $5000. If a corporation commits one of these offences, every officer, member, employee or agent found to have authorized the offence, or who knowingly refrained from using their authority to prevent it, can be found guilty and held personally liable for the fine.

However, service providers are not subject to actions or proceedings for damages resulting from an act or omission related to the execution of their duties under Part X that is made reasonably and in good faith.[122]

No person can be fired, suspended, demoted, disciplined or otherwise disadvantaged for:

- refusing to contravene Part X
- preventing any person from contravening Part X
- reporting a contravention or future contravention to the IPC[123]

The role of the Information and Privacy Commissioner

THE ROLE OF THE INFORMATION AND PRIVACY COMMISSIONER

The Office of the Information and Privacy Commissioner provides oversight of Ontario's access and privacy laws, including Part X. The commissioner is appointed by and reports to the Legislative Assembly of Ontario and is independent of the government of the day.

Any person may file a complaint with the IPC about another person who has or is about to contravene Part X. This could include complaints about:

- refusal of an access or correction request, or failure to respond
- privacy breaches
- failure to comply with any Part X requirement

In response to complaints, or on its own initiative, the IPC may choose to conduct a review of any matter involving a possible contravention of Part X. Where possible, the IPC promotes informal and early resolution of complaints, and often does this through mediation.

IPC COMPLAINT PROCESS

Any person who believes that another person has or is about to contravene Part X can file a complaint, in writing, with the IPC. Complaints about access and correction decisions must be filed within **six months** after the service provider refused the request (or failed to respond). All other complaints must be filed within **one year** after the subject of the complaint first came or should have come to the complainant's attention.[124]

The following description of the IPC complaint process is subject to change. Please ensure that you consult **www.ipc.on.ca** for more information about these processes:

Intake

The IPC registrar reviews the complaint to determine how it should be processed. The registrar or an intake analyst may attempt to resolve the complaint informally. They may also dismiss the complaint if it is clearly outside the IPC's jurisdiction, they are satisfied with your response to the complaint, or for other reasons.

Mediation

Complaints that are not resolved or dismissed at intake may be sent to mediation or further investigation. During mediation, the IPC will investigate the circumstances of the complaint and try to help all parties either reach a full settlement or simplify the complaint.

An IPC mediator acts as a neutral third party. Their main role is to offer guidance to help the parties understand one another and to come to a suitable resolution. Mediation is usually conducted by telephone, with the IPC mediator speaking separately with each party.

Mediation can succeed in settling some or all of the issues, clarifying the issues, and helping the parties to better understand the law. The majority of complaints received by the IPC are resolved at the intake or mediation stage.

The majority of complaints received by the IPC are resolved at the intake or mediation stage.

In some cases, such as a privacy breach, the IPC will appoint an investigator to gather and clarify the facts relating to a contravention or potential contravention of the *CYFSA*.

Adjudication

If a complaint is not resolved at an early stage, the IPC may decide to conduct a formal review. In this situation, an IPC adjudicator will prepare a notice and send it to the parties in turn, including the service provider and complainant. The notice sets out the issues to be addressed and summarizes applicable laws and IPC decisions.

The IPC typically conducts reviews in writing, by asking the parties to submit written representations on the facts and issues described in the notice. The notice includes a deadline for all written representations (arguments and information to support the parties' positions).

The representations will generally be shared with the other parties unless there is an overriding confidentiality concern. Once the adjudicator has considered all representations and, where applicable, reviewed the records, they will then decide how each issue should be resolved. The IPC has the power to make **orders** and issue recommendations for service providers, their agents or employees. For example, the adjudicator may order that a service provider grant the individual access to the requested record. The IPC may also decide not to issue an order. The IPC's decisions are publicly available on our website.

A person affected by an IPC order or by conduct giving rise to a conviction for an offence under Part X can sue for damages for actual harm caused by the contravention or offence.[125]

REPORTING ANNUAL STATISTICS TO THE IPC

All service providers must keep track of certain statistics regarding Part X and report them annually to the IPC.[126] Reports for each calendar year will be due in March of the following year. The IPC provides an electronic form and guidance for submitting the report on our website.

The annual statistical report will ask you to provide the number of:

- **access requests** you received in the previous year – and the number of times you:

- responded within 30 calendar days
- extended the deadline to respond by up to 90 days
- refused access to all or part of a record
- refused the request based on each of the access exceptions (under s. 312(1))

- **correction requests** you received – and the number of times you:
  - responded within 30 calendar days
  - extended the deadline to respond by up to 90 days
  - refused the request based on one of the exceptions (s. 315(6), (9) or (10)),
  - received a statement of disagreement
- **privacy breaches** of the personal information in your custody and control, of the following types:
  - theft
  - loss
  - unauthorized use
  - unauthorized disclosure
- times personal information was used or disclosed **outside the scope of your information practices**

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

IPC'S BROADER ROLE

In addition to resolving complaints and conducting reviews, the IPC also helps to educate service providers and all Ontarians about access and privacy laws and issues. Under the *CYFSA*, the IPC may also:

- offer comments on a service provider's information practices, at their request
- receive representations from the public about the operation of Part X
- engage in research about Part X
- authorize indirect collections of personal information
- provide information and public education about Part X and the IPC's role

Visit our website at **www.ipc.on.ca** for the latest guidance, including frequently asked questions about Part X, and recent orders or decisions made by the IPC. We're here to help. Email us at **info@ipc.on.ca** or call us at 416-326-3333 (in the Toronto area) or toll-free at 1-800-387-0073.

DEFINITIONS

"**capable**" means able to understand the information that is relevant to deciding whether to consent to the collection, use or disclosure of personal information and able to appreciate the reasonably foreseeable consequences of giving, withholding or withdrawing the consent. "Incapable" means not capable. "Capacity" and "incapacity" have corresponding meanings. (*CYFSA,* s. 281)

"commissioner" is used in the *CYFSA* to refer to the Information and Privacy Commissioner of Ontario, and "assistant commissioner" has a corresponding meaning (*CYFSA*, s. 281). In this guide, the acronym "IPC" refers to the Office of the Information and Privacy Commissioner of Ontario.

"information practices" means policies respecting the collection, use, modification, disclosure, retention or disposal of personal information and the administrative, technical and physical safeguards and practices that the service provider maintains with respect to the information. (*CYFSA*, s. 281)

"**law enforcement**" has the same meaning in s. 292 of the *CYFSA* as it does in s. 2(1) of the *Freedom of Information and Protection of Privacy Act*:

- policing,
- investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or
- the conduct of proceedings referred to in the clause above.

"minister" means the Minister of Children, Community and Social Services, who was designated in 2018 to administer the *CYFSA*. (*CYFSA,* s. 2(1))

"parent" means:

- the person who has lawful custody of the child, or
- if more than one person has lawful custody of the child, all persons who have lawful custody, excluding any person who is unavailable or unable to act, as the context requires. (*CYFSA,* s. 2(2))

Note that this definition applies to Part X but not to some other parts of the *CYFSA.* For example, Part V (Child Protection) includes a broader definition of parent.

"**personal information**" has the same meaning as in s. 2(1) of *FIPPA* (*CYFSA,* s. 2(1)), which provides that "personal information" means recorded information about an identifiable individual, including:

- information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- any identifying number, symbol or other particular assigned to the individual,
- the address, telephone number, fingerprints or blood type of the individual,
- the personal opinions or views of the individual except where they relate to another individual,
- correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- the views or opinions of another individual about the individual, and
- the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Note that personal information does not include information about an individual who has been dead for more than thirty years. (*FIPPA*, s. 2(2))

Personal information also does not include the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity. This applies even if an individual carries out business, professional or official responsibilities from their dwelling and the contact information for the individual relates to that dwelling. (*FIPPA*, s. 2(3-4))

Specific to the *collection* of personal information, the definition of personal information includes information that is not recorded. (*FIPPA,* s. 38(1))

"**potential successor**" and "**successor**" mean a potential successor or a successor that is a service provider, or that will be a service provider if it becomes a successor. (*CYFSA,* s. 310(3))

"proceeding" includes a proceeding held in, before or under the rules of a court, a tribunal, a commission, a justice of the peace, a coroner, a committee of a College within the meaning of the *Regulated Health Professions Act, 1991*, a committee of the Ontario College of Social Workers and Social Service Workers under the *Social Work and Social Service Work Act, 1998*, an arbitrator or a mediator. (*CYFSA*, s. 281)

"**service**" means a service or program that is provided or funded under the *CYFSA* or provided under the authority of a licence (*CYFSA,* s. 281). It includes,

- a service for a child with a developmental or physical disability or the child's family,
- a mental health service for a child or the child's family,
- a service related to residential care for a child,
- a service for a child who is or may be in need of protection or the child's family,
- a service related to adoption for a child, the child's family or others,
- counselling for a child or the child's family,
- a service for a child or the child's family that is in the nature of support or prevention and that is provided in the community,
- a service or program for or on behalf of a young person for the purposes of the *Youth Criminal Justice Act* or the *Provincial Offences Act*, or
- a prescribed service [currently, none are prescribed]. (*CYFSA,* s. 2(1))

"**service provider**" means,

- the minister,
- a licensee,
- a person or entity that provides a service funded under this act (e.g., children's aid societies), or
- a prescribed person or entity [currently, none are prescribed],
- but does *not* include a foster parent. (*CYFSA,* s. 2(1))

For the purposes of Part X, it also includes a lead agency designated under section 30 of the *CYFSA*. (*CYFSA,* s. 281)

"**substitute decision-maker**" means a person who is authorized under Part X to give, withhold or withdraw consent on behalf of an individual to the collection, use or disclosure of personal information about the individual. (*CYFSA,* s. 281)

ENDNOTES

1 *CYFSA,* s. 1

2 *CYFSA*, s. 3. This guide does not include a comprehensive list of a child's and young person's rights under the *CYFSA.* Please see Part II of the *CYFSA* for more information.

3 *CYFSA* s. 2(1) and 281

4 Lead agencies are designated by the minister under section 30 of the *CYFSA.* O. Reg. 155/18, ss. 24-25, establishes child and youth mental health as a category of lead agencies and sets out their functions.

5 "Minister" is defined by the *CYFSA* as "the Minister of Children and Youth Services or such other member of the Executive Council as may be designated under the *Executive Council Act* to administer this Act." In June 2018, an order in council under the *Executive Council Act* transferred the powers and duties of the Minister of MCYS to the new Minister of Children, Community and Social Services.

6 Currently, no additional service providers are prescribed.

7 *CYFSA*, s. 285(3)

8 *FIPPA* institutions are identified in section 2(1) of that act, or listed in Regulation 460. *MFIPPA* institutions are identified in section 2(1) of that act, or listed in O. Reg. 372/91.

9 *CYFSA,* s. 285(2)

10 The *CYFSA* defines "personal information" as having the same meaning as in *FIPPA* (*CYFSA*, s. 2(1)). Personal information is defined in s. 2(1) of *FIPPA,* as well as in s. 38(1) (specific to the collection of personal information).

11 *CYFSA*, s. 2(1), *FIPPA*, s. 38(1)

12 *CYFSA*, s. 285(6). Note that the rights and obligations of Part X do not apply retroactively. For example, an individual would not have a right under Part X to complain to the IPC about an access request made before Part X came into force.

13 See IPC Order P-239.

14 For example, see IPC order MO-3646-I for a discussion of "custody or control" under *MFIPPA*.

15 *CYFSA*, s. 281

16 *CYFSA*, s. 2(1)

17 *CYFSA*, s. 285 (4-5)

18 The collection, use, or disclosure of adoption information given to a designated custodian or other persons also falls outside of most of Part X. See *CYFSA*, ss. 224, 225, 227 and 285(4). The rules for disclosure of information about adoptions are found in O. Reg. 158/18 under the *CYFSA,* and the *Vital Statistics Act.*

19 See *CYFSA*, s. 133. Note that the Child Abuse Register is to be repealed on a date to be proclaimed.

20 See *CYFSA*, ss. 130(6) and (8)

21 See *CYFSA,* ss. 163(6) and 285(5)

22 *CYFSA*, s. 282; See *CYFSA* s. 87 (8-10)

23 *CYFSA*, s. 286

24 *CYFSA*, ss. 286-287

25 A "substitute decision-maker" means a person who is authorized under Part X to consent, withhold or withdraw consent on behalf of an individual to the collection, use or disclosure of personal information about the individual (*CYFSA*, s. 281).

26 *CYFSA*, s. 295(2)

27 *CYFSA*, s. 290

28 *CYFSA*, s. 289

29 *CYFSA*, s. 288(1)

30 *CYFSA*, s. 288(2)(e)

31 *CYFSA*, s. 288(2)(a)

32 *CYFSA*, s. 288(2)(b). Societies are also permitted to collect information from one another if necessary for prescribed purposes related to their functions (s. 288(2)(c)). However, no purposes are currently prescribed.

33 Service providers may also indirectly collect personal information if the indirect collection has been specifically authorized by the IPC. *CYFSA*, s. 288(2)(d).

34 *CYFSA*, s. 307

35 *CYFSA*, s. 306(1)

36 *CYFSA*, s. 286

37 An express instruction can be made where the information was collected with the consent of the individual; or the information was collected under clause 288(2)(a) of the *CYFSA*.

38 *CYFSA*, s. 291(2)

39 *CYFSA*, s. 291(2)(a)(i). Societies can also use the information for a "prescribed purpose" related to their functions. However, no purposes are currently prescribed.

40 See *CYFSA,* s. 291.

41 Part X regulation contains many requirements related to using information for research, including the need to have a research plan approved by a research ethics board. This guide does not provide detail on research-related requirements. See section 5 of Regulation 191/18 under the *CYFSA* for further information.

42 Guidance about how to detect and deter snooping is available on the IPC's **website**.

43 *CYFSA*, s. 291(1)

44 See *CYFSA,* s. 292.

45 *CYFSA*, s. 125

46 *CYFSA*, s. 73; O. Reg. 156/18, s. 29. This requirement also applies to persons or entities providing a prescribed service or power under the *CYFSA*. See also CYFSA, s. 72. Note that a child's consent **is** required before consulting with the child's bands or First Nation, Métis or Inuit communities if the consultation concerns a plan to transition the child from a society's care to living independently (O. Reg. 156/18, s. 29(4)).

47 "Law enforcement" has the same meaning as in s. 2(1) of *FIPPA* (*CYFSA*, s. 292(4)). For more information about disclosure to law enforcement, please see the IPC's fact sheet "Disclosure of Personal Information to Law Enforcement" available at **www.ipc.on.ca**.

48 *CYFSA,* s. 292(1)(f). Note that this is subject to section 294 of the *CYFSA*, which deals with the disclosure of records of mental disorders, including where a physician has issued a written statement that the disclosure is likely to be detrimental to treatment or result in bodily harm.

49 *CYFSA*, s. 292(2). Societies are also permitted to disclose information to one another if necessary for prescribed purposes related to their functions (s. 292(3)). However, no purposes are currently prescribed.

50 *CYFSA*, s. 310. See also O. Reg. 191/18, s. 10(4).

51 If providing notice before transferring records to a successor is not reasonably possible, you must do so soon as possible after transferring the records.

52 *CYFSA*, s. 292

53 *CYFSA*, ss. 283 and 284

54 *CYFSA*, s. 293(1); O. Reg. 191/18, ss. 1, 3, 4, 6

55 *CYFSA*, s. 293(2); O. Reg. 191/18, ss. 2, 3, 4, 6

56 *CYFSA*, s. 306(2)

57 Note that s. 306(3) of the *CYFSA* requires service provider to record disclosures made under the prescribed provisions in the prescribed manner. However, at this time, no such provisions/manners have been prescribed. Also note that recording disclosures is a best practice, given your obligations in the event of a request for a correction, under s. 315(11)(c) of the *CYFSA.*

58 *CYFSA*, s. 295(1)

59 *CYFSA*, s. 295(4)

60 *CYFSA*, s. 295(2)

61 *CYFSA*, s. 295(3)

62 *CYFSA*, s. 298. Note that you can rely on a consent given before Part X comes into force, as long as it meets the requirements of Part X (s. 295(6)). However, you may wish to obtain new consents given the new requirements of the *CYFSA*, including that a verbal consent be recorded and the individual know the purposes for which the information can be used/disclosed.

63 *CYFSA*, s. 331(4)

64 *CYFSA*, s. 297

65 *CYFSA*, s. 296

66 *CYFSA*, s. 281

67 *CYFSA*, s. 300(2)

68 *CYFSA,* s. 300(1)

69 *CYFSA*, s. 304(2). This section also requires you to provide the incapable person with prescribed information, while section 304(1) requires you to make determinations of incapacity in accordance with any prescribed requirements and restrictions. Nothing is currently prescribed under either of these subsections.

70 *CYFSA*, s. 304(3), O. Reg 191/18, s. 7

71 *CYFSA*, s. 303(1)

72 *CYFSA*, s. 301(4); *PHIPA* s. 26

73 Specifically, this refers to a substitute decision-maker within the meaning of sections 9, 39 and 56 of the *Health Care Consent Act*, if the purpose of the collection, use or disclosure is necessary for, or ancillary to, a decision about a treatment under Part II, admission to a care facility under Part III, or a personal assistance service under Part IV of the *Health Care Consent Act*, respectively.

74 *CYFSA*, s. 305(1-2). Incapable individuals 16 years of age and older can apply to the Board to appoint a representative to consent on their behalf or a prospective representative can themselves make an application to the Board. Such applications cannot be made if the individual already has a guardian of the person or of property, or an attorney for personal care or for property.

75 If a society is entitled to consent in the place of the parent, this paragraph does not include the parent. If the incapable person has a child who is over 16, the child is also included in this paragraph.

76 *CYFSA*, s. 301(4); *PHIPA*, s. 26(4). Note that the Public Guardian and Trustee may make the decision to consent if no other person meets the requirements.

77 The exception to this age restriction is where an individual's substitute decision-maker is their parent, in which case the parent could be under 16 and still be a substitute decision-maker. Substitute decision-makers must not be prohibited by court order or separation agreement from having access to the individual or from giving or refusing consent on their behalf (*CYFSA*, s. 301(4); *PHIPA*, s. 26(2)).

78 *CYFSA*, s. 301(2-3)

79 *CYFSA*, s. 301(3)

80 *CYFSA*, s. 301(1)

81 *CYFSA*, s. 302(1). If the individual is capable, this refers to the wishes, values and beliefs the substitute decision–maker knows the individual holds and believes would want reflected in decisions about their personal information. If the individual is incapable or deceased, this refers to the wishes, values and beliefs they know the individual held when capable or alive, and believe would want reflected in decisions about that individual's personal information.

82 *CYFSA*, s. 302(2)

83 *CYFSA*, ss. 307 and 308(1)

84 *CYFSA*, s. 308(2); O. Reg. 191/18, s. 8

85 While this guide provides a simplified summary, you should review the full list of criteria set out in section 9 of O. Reg. 191/18, to determine whether a specific privacy breach should be reported to the IPC and minister.

86 *CYFSA*, s. 309(1); O. Reg. 191/18. s. 10

87 These requirements are found in O. Reg. 191/18. s. 10. In developing retention policies, service providers should familiarize themselves with the requirements of subsections 10 (5-7) of this regulation.

88 For example, O. Reg. 156/18 under the *CYFSA*, s. 93(2), includes retention requirements for certain records maintained by licensees who operate children's residences.

89 O. Reg. 191/18, s. 10(3)

90 The IPC offers guidance on the topic of secure disposal of records, including electronic records, available at **www.ipc.on.ca.**

91 *CYFSA*, s. 311

92 *CYFSA*, s. 281

93 *CYFSA*, s. 311(2). Note that you would be required to notify the individual at the first reasonable opportunity, unless they do not have a right of access to the record under s. 312.

94 In determining whether granting access could result in a risk of serious harm, service providers may consult with a member of the College of Physicians and Surgeons of Ontario, the College of Psychologists of Ontario or the Ontario College of Social Workers and Social Service Workers (*CYFSA,* s. 312(4)).

95 *CYFSA*, s. 312(2). The individual has a right to access personal information that can "reasonably" be severed from the part of the record to which they do not have a right of access. The IPC has considered this question under other privacy legislation and found that personal information that would comprise only disconnected or meaningless snippets is not considered reasonably severable (see, for instance, IPC Orders PO-1663 and *PHIPA* Decision 73).

96 *CYFSA*, s. 314(6). Guidance about what constitutes a "frivolous or vexatious" request is available at **www.ipc.on.ca.**.

97 The IPC has not yet had occasion to consider this question under Part X of the *CYFSA*. Several IPC decisions under *PHIPA*, including *PHIPA* Decision 17, consider a similar provision in that act.

98 *CYFSA*, ss. 312(5) and 313. An individual making a verbal or informal request may only be granted access to a record of personal information to which they have a right of access (i.e., where there is nothing in the law that prohibits the release of the information).

99 Please see the IPC's website for guidance about offering assistance in clarifying access requests.

100 *CYFSA*, s. 314(3)

101 *CYFSA*, s. 314(7)

102 *CYFSA*, s. 314(8)

103 *CYFSA*, s. 314(5)

104 *CYFSA*, s. 314(10) states that fees may not be charged for providing access except in prescribed circumstances. Nothing has been prescribed under this section, meaning there are no circumstances where fees may be charged.

105 *CYFSA,* s. 314(9)

106 For example, this response may be appropriate where confirming that a record exists, even without granting access to it, could reveal confidential information.

107 In determining whether granting access could result in a risk of serious harm, service providers may consult with a member of the College of Physicians and Surgeons of Ontario, the College of Psychologists of Ontario or the Ontario College of Social Workers and Social Service Workers (*CYFSA,* s. 312(4)).

108 *CYFSA*, s. 314(3)

109 *CYFSA*, s. 314(4)

110 *CYFSA*, s. 314(7)

111 *CYFSA*, s. 314(3)

112 *CYFSA*, s. 303. Note that this section permits a substitute decision-maker to make requests on behalf of an individual, and that this is not limited to access requests (for example, it would apply to correction requests as well).

113 *CYFSA*, s. 331(4)

114 *CYFSA*, s. 332(1)(b)

115 *CYFSA*, s. 301(3)

116 *CYFSA,* s. 315(2)

117 While you can choose to respond to verbal or informal correction requests, the request must be in writing in order for the procedural rules of Part X to apply (*CYFSA*, s. 315(3)).

118 *CYFSA*, s. 315(4)

119 *CYFSA*, s. 315(7)

120 *CYFSA,* s. 315(4)

121 *CYFSA*, s. 332

122 *CYFSA,* s. 331

123 *CYFSA*, s. 330

124 *CYFSA*, s. 316. Note that the IPC has the power to permit a complaint to be submitted after a longer period of time, if the IPC is satisfied that this will not result in prejudice to any person. More information about IPC processes under Part X is available on our website.

125 *CYFSA*, s. 325. If the Superior Court of Justice determines the harm was caused by a contravention that the defendants engaged in willfully or recklessly, the Court may include in its award of damages an award for mental anguish.

126 O. Reg. 191/18, s. 11

Part X of the *Child, Youth and Family Services Act*: A Guide to Access and Privacy 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
Telephone: 416-326-3333
Email: info@ipc.on.ca

May 2019