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

***VIA ELECTRONIC MAIL***

July 13, 2023

Director Aly N. Alibhai
Ministry of Children, Community and Social Services
Child, Youth and Family Services Act Review Project
2 Bloor St West, 30th Floor
Toronto, Ontario M7A 2T2

Dear Aly N. Alibhai:

**RE: Written Submission to the Ministry of Children, Community and Social Services with Respect to the 2023 Review of the *Child, Youth and Family Services Act, 2017***

I am writing with respect to the first review of the *Child, Youth and Family Services Act, 2017* ("the ***CYFSA***"), since its proclamation in 2018.

As an Office of the Legislature, the Information and Privacy Commissioner of Ontario (IPC) has a statutory mandate to protect and promote the access and privacy rights of Ontarians. The IPC offers the following comments and recommendations with the goal of strengthening the access and privacy protections afforded to Ontarians under the *CYFSA* and its regulations. The comments and recommendations are consistent with previous submissions made with respect to Bill 89 and the proposed Regulation on Personal Information under Part X of the *CYFSA* (now O. Reg. 191/18).

In this submission, we focus on five crucial issues, largely related to child and youth rights, and accountability[1]:

1. The Ministry's[2] broad authority to collect, use and disclose personal information, including the authorization of data integration, without adequate safeguards;
2. The unclear requirements for service providers, including the Ministry, to protect personal information;
3. Inconsistent minimum research requirements applicable to the Ministry, service providers, prescribed entities, and other persons and entities who are not prescribed;
4. The unclear requirements respecting the collection, use and disclosure of the personal information of deceased individuals; and,

[1] These are two of the six focus areas of the current review. The other four key areas are: First Nations, Inuit, and Métis peoples; Equity and anti-racism; Prevention and community-based care; and, Quality services.
[2] It is recognized the *CYFSA* refers to the Minister in many of the statutory provisions, however for the sake of simplicity and readability, this submission will refer to the Minister as the Ministry.

5. The need to enhance the Information and Privacy Commissioner's ability to be as transparent as possible to the public.

The overarching basis for our comments and recommendations stem from the very broad authority that the Ministry has given itself under sections 283, 284 and 293 of the *CYFSA*. These provisions appear to authorize the Ministry to collect practically any type and amount of personal information, require others to collect and disclose nearly any type and amount of personal information, and subsequently use that personal information for almost any purpose it deems appropriate.

I believe our recommendations support the Ministry of Children, Community and Social Services ("the Ministry") in carrying out its mandate while also improving accountability and transparency, and better protecting the access and privacy rights and interests of children, youth, and their families. Our recommendations fully align with the Ministry's goal to promote the best interests and well-being of children, youth, and families.

## The 2023 Review of the *Child, Youth and Family Services Act, 2017*

Children, youth, and families share significant amounts of sensitive personal information with service providers when receiving a service under the *CYFSA.* Although these services are not always mandatory, service recipients may feel pressured to provide their sensitive personal information in order to receive a benefit or to avoid significant negative outcomes. All children and youth who receive services under the *CYFSA* are inherently vulnerable and many belong to disadvantaged populations. This places them and their families in a position of increased vulnerability, and puts them at greater risk of inequitable outcomes during service delivery.

Prior to the enactment of Part X of the *CYFSA* in January 2020, children, youth, and family service providers in Ontario, including children's aid societies, were not subject to privacy legislation or oversight. The lack of a legislative privacy framework led to inconsistent policies and wide variation in the interpretation of an individual's right to access personal information in the custody and control of service providers.

Part X was modelled after the *Personal Health Information Protection Act* ("*PHIPA*") and sets the rules that service providers must follow to protect privacy and enable access to personal information. It also grants the IPC regulatory powers to ensure service providers' compliance with the access and privacy provisions of the *CYFSA*.

The addition of these privacy provisions to the *CYFSA* was an important step towards closing the legislative gap regarding access and privacy rights in a sector that receives significant public funding and provides services for some of the most vulnerable Ontarians, specifically children and youth. However, we believe further amendments are necessary to strengthen privacy, transparency and accountability as a counterbalance to the unparalleled powers of service providers providing services under the *CYFSA*.

The IPC's comments and recommendations largely relate to the review's key focus areas of child and youth rights and accountability. More specifically, on strengthening

the privacy and access rights of children and youth receiving services under the *CYFSA*, and calling for the Ministry to be more accountable when collecting, using, and disclosing the personal information of vulnerable Ontarians.

## Issue 1: The Powers of the Ministry to Collect, Use and Disclose Personal Information

The *CYFSA* gives the Ministry expansive powers to collect personal information, and then to use the personal information for a broad range of purposes, including sharing with other Ministries.[3] The Ministry is also exempt from vital privacy protective provisions that apply to other service providers under the *CYFSA.*[4] On their own, each of these broad capabilities could be considered to have significant privacy implications for vulnerable children, youth and families. When combined, however, as they are under Part X, it greatly expands the risk even more.

While these concerns have been raised by the IPC since before the passage of Part X, the IPC is making a renewed call to repeal sections 283 and 284 of the *CYFSA* for the reasons set out below. The need to repeal these sections has become even more pronounced since the adoption of the Part III.1: Data Integration in the *Freedom of Information and Protection of Privacy Act* ("*FIPPA*") in 2019, which now provides a more balanced and privacy protective approach to conducting the planning, management, analysis and research functions provided for in the *CYFSA.*

### Recommendation 1.1: Require the Ministry to be Subject to the Same Privacy Rules as other Service Providers

*Under Part X of the CYFSA, the Ministry is subject to different, less stringent, privacy rules than other service providers subject to the Act. In other words, the law does not adequately protect the sensitive personal information of vulnerable children, youth and families collected, used and disclosed directly by the Ministry or subject it to sufficient governance and oversight. Further to previous submissions, the IPC continues to urge the government to amend the CYFSA to make the Ministry subject to the same privacy rules as other service providers when the Ministry is acting in this capacity.*

Part X of the *CYFSA*, sets out rules for the collection, use and disclosure of personal information by service providers that are subject to the *CYFSA*. However, Part X is structured so that the vast majority of the rules do not apply to a service provider that is already subject to *FIPPA*.[5] Because the Ministry is already subject to *FIPPA* when providing services under the *CYFSA*, it is not subject to the collection, use and disclosure requirements, and the safeguarding, access, and enforcement provisions, among others, under Part X of the *CYFSA*; rather, the Ministry is subject to *FIPPA's* Part III: Protection of Individual Privacy. Part III of *FIPPA* has not been substantially updated since it was enacted more than 35 years ago in a largely paper-based world. It

[3] See section 283 of the *Child, Youth and Family Services Act*
[4] See section 285 of the *Child, Youth and Family Services Act*
[5] See sections 2(1) and 285 (2) of the *Child, Youth and Family Services Act*

does not contemplate today's digital context in which massive amounts of personal data can be easily created and shared, nor does it incorporate many of the common features built into modern privacy laws, such as mandatory breach notification, consent and accountability requirements, and strong independent oversight. Given the scope of information-sharing enabled by the C*YFSA*, Part III of *FIPPA* is insufficient to address the data protection concerns of today's Ontarians.

The Ministry's exemption from following the stricter rules for the collection, use and disclosure of personal information as service providers when delivering services under the *CYFSA* should be of serious concern to Ontarians. The IPC believes the Ministry must be subject to a greater degree of accountability and oversight than that which is currently provided under Part III of *FIPPA*. It is our view that when the Ministry is acting as a service provider itself, its collection of personal information should be subject to the stronger privacy protections and safeguards available under Part X of the *CYFSA*. This would be consistent with the Ministry of Health's status under *PHIPA*, where it is subject to the same rules applicable to health information custodians. As a result, the IPC continues to urge the government to amend the *CYFSA* to make the Ministry subject to the same privacy rules as other service providers when acting in that capacity. The IPC would be pleased to consult with the Ministry on making these important amendments.

**Recommendation 1.2: Limit the Ministry's Powers to Require Service Providers to Collect and Disclose Information to the Ministry**

*Section 284 of the CYFSA gives the Ministry the power to direct service providers to collect a very broadly defined array of personal information from children, youth and families, even if it is not related to the services being provided, and share it with the Ministry. This allows for the circumvention of data minimization provisions and enables circumstances where personal information is not adequately safeguarded and protected. Further to previous submissions, the IPC continues to urge the government to repeal section 284 of the CYFSA.*

As previously mentioned, children, youth and families share significant amounts of sensitive personal information with service providers when receiving a service under the *CYFSA*. Section 286 of the *CYFSA* sets rules for service providers to protect vulnerable children, youth and families from the overcollection of their sensitive personal information. This provision requires that a service provider shall only collect personal information about an individual for the purpose of providing a service, or use or disclose the information if: 1) the service provider has the individual's consent and the collection, use or disclosure is necessary for a lawful purpose, or 2) collection, use or disclosure without consent is permitted or required by the *CYFSA*. The *CYFSA* also includes security and data minimization provisions to limit the collection, use or disclosure of personal information collected for the purposes of providing a service.[6] These restrictions and requirements for service providers properly limit the collection of personal information and require appropriate safeguards and privacy protections.

[6] See section 287 of the *Child, Youth and Family Services Act*

Despite these limits, section 284 of the *CYFSA* gives the Ministry powers to require a service provider to directly collect more personal information than what is required to provide a service to children, youth and families under the *CYFSA.* When the Ministry exercises its broad power under section 284, there is a risk that the security and data minimization provisions within Part X of the *CYFSA* may not be applicable, since the personal information in question would be collected for the ministry's purposes, not for the purposes of providing a service. The Ministry's powers to require service providers to disclose personal information should not compromise the safeguarding of personal information, and should be limited to information that has been collected by the service provider in accordance with section 286 of the *CYFSA*.

For the reasons outlined above and given significant concerns regarding the risks associated with the overcollection of personal information, especially from vulnerable populations, the IPC continues to urge the government to repeal section 284 of the *CYFSA*. Limiting the Ministry's collection of personal information, especially without consent, would be more respectful of the rights of children and youth receiving services and would strengthen principles of accountability and transparency.

**Recommendation 1.3: Limit the Ministry's Powers for Indirect Collection and Data Integration as a Funder, Planner and Manager of Service Delivery**

*Under the CYFSA, the Ministry has expansive powers to indirectly collect and share personal information, allowing for the overcollection and integration of considerable amounts of sensitive personal information from vulnerable individuals without adequate privacy protections. The IPC continues to urge the government to remove all data integration powers in the CYFSA, repeal section 283, and rely on Part III.1 of FIPPA instead.*

Section 283(1) of the *CYFSA* gives the Ministry expansive powers to collect the sensitive personal information of children, youth, and families, both directly from individuals and indirectly through service providers, for a broad range of purposes. The language within this provision of the *CYFSA* conflates three distinct privacy concepts, namely direct collection, indirect collection, and subsequent use of that personal information, into a single authority. It is important to note that *PHIPA*, which Part X is modeled after, clearly differentiates these concepts and does not grant powers under a single authority.

One of the key purposes of public-sector privacy law is to place limits on government collection and use of personal information. One way in which these laws achieve this end is by articulating limits on when, why and how the government may collect personal information and then subsequently use it. By amalgamating collection and use of personal information into a single provision, the *CYFSA* blurs these lines. This substantially broadens the ministry's powers to collect and use the sensitive personal information of children, youth, and families beyond what is reasonably necessary. The combination of authorities for collection and use raises substantial privacy concerns, including the potential overcollection of personal information, and the integration of data without adequate privacy protections. This should be a significant concern to both the

Ministry and Ontarians and one that merits serious attention as part of this 5-year review. To ensure that the Ministry's power to collect and use personal information is as limited and specific as possible, it is important to separate out the Ministry's authority to collect personal information directly from the individual; the Ministry's authority to collect personal information indirectly; and the Ministry's authority to use personal information.

Further, section 283(5) of the *CYFSA* provides the Ministry and other prescribed ministries with the authority to share personal information with each other for the broad purposes of planning, managing, or delivering services and conducting research and analysis. The IPC is concerned that this provision risks allowing large-scale, integrated databases of personal information across multiple institutions without necessary safeguards or appropriate limits.

In the recent past, the Ontario government has identified the need to protect Ontarians' privacy rights in the context of large-scale government data sharing. In 2019 the government established Ontario's Data Integration Framework amending *FIPPA* to include Part III.1, Data Integration. Part III.1 provides a robust, privacy-protective framework for a government-wide approach to the practice of integrating data from various sources. This framework enables prescribed data integration units to collect personal information for the purpose of compiling information, including statistical information, to enable analysis in relation to the management or allocation of resources, the planning for the delivery of services and the evaluation of those programs and services. Critically, Part III.1 provides a consistent and privacy protective government-wide approach, which includes requirements to create records with the minimal amount of personal information necessary, to de-identify the personal information, and to promptly and securely destroy records of personal information after de-identification and linking have occurred.[7] Part III.1 also requires IPC review of data integration practices and procedures to help ensure public trust and transparency related to the management of government data assets.

As the IPC has stated previously, purpose-built, standalone data integration provisions, like the ones within the *CYFSA* should not exist separately from the suite of protections and controls provided for under Part III.1 of *FIPPA*.[8] The Ministry's authority under section 283 of the *CYFSA* significantly undermines the well-thought-out privacy framework of Part III.1 of *FIPPA*.

Accordingly, the IPC urges the government to remove from the *CYFSA* all data integration authorities that are already authorized under Part III.1. of *FIPPA* under a much more protective framework and repeal section 283 of the *CYFSA*. If the Ministry believes that there remain additional requirements for the collection and use of personal information beyond those authorized under Part III.1 and the service provider provisions of the *CYFSA*, the IPC would welcome an opportunity to discuss additional limited

[7] See section 49.6 of the *Freedom of Information and Protection of Privacy Act*
[8] See Letter to the Ministry of the Solicitor General regarding the regulatory proposals under the Community Safety and Policing Act, 2019, the IPC's 2018 Annual Report (pg. 2) and the IPC's Bill 102 Submission

authorities, including with appropriate safeguards, for the Ministry's collection of personal information under the *CYFSA*.

## Issue 2: The Requirements of Service Providers, including the Ministry, to Protect Personal Information

### Recommendation 2.1: Enhance Service Providers' Transparency and Accountability with respect to the Retention of Records

*The CYFSA does not establish requirements for common retention periods of records of personal information held by service providers. The lack of guidance contributes to a risk that records of personal information are kept for longer than necessary and does not facilitate consistent and transparent retention processes across child, youth and family services sectors. The IPC continues to urge the government to amend the CYFSA to require service providers to make their records retention policies publicly available, and to develop common retention schedules that limit the storage of personal information for only as long as necessary prior to its secure disposal.*

The *CYFSA* imposes requirements on service providers for the handling, retention, transfer, and disposal of records. Specifically, each service provider is required to develop and maintain a records retention policy that identifies each type of record, the sensitivity of the personal information contained in the record and the manner of use or disclosure, how long the record will be kept, and the method of disposal, transfer, and storage.[9] Although the *CYFSA* requires service providers to consider certain factors in determining how long to keep each type of record, it does not stipulate the minimum or maximum length of time that a record of personal information must be kept, nor does it establish baseline expectations with respect to common retention periods.

The IPC is concerned that the existing provisions do not facilitate consistent and transparent retention processes across the sector, and they allow for the potential storage of personal information for longer than necessary. This has a direct impact on individuals' access to their own personal information and the protection of their privacy. For example, individuals who spent time in the care of a Children's Aid Society may be uncertain as to whether their records still exist, and may have concerns about how long their personal information may be retained and how it may be used once they have aged out of the system or they are no longer receiving services under the *CYFSA*. Retention schedules support the protection of personal information by ensuring that records are only collected and kept for as long as necessary.

To address the concerns regarding lack of transparency, the IPC recommends that section 10 of O. Reg. 191/18: Personal Information ("O. Reg. 191/18") be amended to require service providers to make their records retention policies publicly available. Service providers are already required by section 311 (1) of the *CYFSA* to make a general description of their information practices available to the public. A specific

[9] See section 309 (1)(b) of the *Child, Youth and Family Services Act* and section 10 (5) and (6) of O. Reg., 191/18

requirement to make retention policies publicly available would complement this general requirement and support access to information by providing clarity to individuals about what records are kept and for how long. Additionally, publicly available policies allow for improved oversight of service providers' compliance with the requirements to develop and maintain such policies. Accordingly, the IPC recommends a provision be added to section 10 of O. Reg. 191/18 as detailed in Appendix A.

Furthermore, to address the concerns regarding inconsistency across service providers and the storage of personal information for longer than necessary, the IPC continues to urge the Ministry to work together with interested parties and subject matter experts in the sector, as well as the Archives of Ontario, to develop common retention requirements, especially for children's aid societies, and to support the sector to comply with these requirements, including through changes to related information management systems, such as the Ministry's Child Protection Information Network (CPIN).

Developing common and transparent records retention requirements or guidelines would also help to ensure that legal requirements regarding the retention or secure destruction of specific classes of sensitive records, such as records under the *Youth Criminal Justice Act*, are appropriately dealt with across the child protection sector. Examining current information system functionality and retention practices, and then implementing any necessary changes, supports the rights of children, youth and families receiving services by limiting the overcollection and storage of their personal information, and by making it simpler to understand what types of records are kept across service providers and for how long.

**Recommendation 2.3: Define the Meaning and Regulate the Activities of an Agent**

*The lack of a definition of the meaning of an "agent" within the CYFSA creates a risk that sensitive personal information could be shared, without the direct knowledge of an individual, to an inappropriate person or entity. Additionally, the absence of provisions that more clearly and directly set out the responsibilities and obligations of an agent, risks undermining privacy protections for personal information once in the hands of the agent. The IPC recommends the CYFSA be amended to clearly define the meaning of "agent" and more clearly and directly regulate their activities.*

Part X of the *CYFSA* allows a service provider to share information with an "agent" in specific circumstances. For example, under s. 291(1)(a) a service provider may use personal information collected for the purpose of providing a service for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, including providing the information to an officer, employee, consultant, or agent of the service provider.

While *PHIPA* also allows for the sharing of personal health information with an "agent", under that legislation, "agent" is clearly defined.[10] *PHIPA* also clearly regulates the activities of an "agent" and, among other things, clearly and directly limits what agents

[10] See section 2 of the *Personal Health Information Protection Act*

can do with personal health information (see, for example, s. 17 of *PHIPA*). Under PHIPA, the IPC has seen many instances of agents acting without authorization, and has also seen the importance of imposing clear and direct statutory obligations on those agents for addressing these bad actors.

To strengthen the protection of personal information under the *CYFSA*, the IPC recommends the Ministry work together with subject matter experts to clarify and define the meaning of an "agent", and more clearly and directly regulate their activities to more closely align with the framework for regulating agents as prescribed in *PHIPA.*

**Recommendation 2.3: Further Enhance the Protection of Personal Information when it is Disclosed to Persons and Entities who are not Prescribed**

*The CYFSA lacks adequate safeguards for personal information disclosed for analytical and statistical purposes to a person or entity not prescribed. The IPC commends the Ministry for adopting some of my office's previous recommendations to strengthen minimum standards for these disclosures, however, the IPC continues to urge the government to make additional amendments specifically to oblige persons or entities not prescribed to comply with the terms of the agreement required under the regulation, by prescribing breach notification timelines, and by extending the regulatory requirements to disclosures required by the Ministry.*

Section 293 of the *CYFSA* allows service providers to disclose personal information to two categories of entities: 1) prescribed entities and 2) persons and entities who are not prescribed. These disclosures are permitted for the purposes of analysis and compiling statistics for planning, managing, and evaluating services, provided certain conditions are met.

While the IPC will review the practices and procedures of prescribed entities every three years to ensure that adequate privacy and confidentiality protections are in place, a person or entity that is not prescribed is not subject to any review process or oversight. Accordingly, other strong safeguards must exist to ensure that the privacy and confidentiality of Ontarians' personal information is protected, regardless of whether it is received by a prescribed entity or an entity that is not prescribed.

Existing provisions within section 2 of O. Reg. 191/18 place some requirements and restrictions on the disclosure of personal information to persons and entities who are not prescribed, including a requirement for service providers to enter into an agreement with respect to the use, security, disclosure, return or disposal of the information.[11] However, there is no requirement within the regulation for the person or entity that is not prescribed to comply with any conditions or restrictions within the agreement, or any prescribed timeline for notification of privacy breaches. Also, the restrictions and requirements within section 2 do not extend to circumstances where the Ministry exercises its powers under section 293(3) to require service providers to disclose information, including personal information, to a person or entity not prescribed.

[11] See section 2(1) of O. Reg., 191/18

In the IPC's view, any person or entity that receives sensitive personal information of vulnerable children and youth or their families without their direct knowledge, must be subject to clear transparency and accountability requirements. This could be achieved by strengthening the contractual obligation arising from the agreement required under section 2 of O. Reg. 191/18 into a clear statutory one, by prescribing breach notification timelines, and by extending the regulatory restrictions and requirements to disclosures required by the Ministry.

## Issue 3: Insufficient Research Requirements

### Recommendation 3.1: Enhance the Research Requirements for Service Providers, including the Ministry

*Under the CYFSA, the Ministry and service providers are subject to different, less stringent research rules than prescribed entities and persons and entities that are not prescribed. The IPC continues to urge the government to strengthen the research plan requirements for the Ministry and service providers when using the sensitive personal information of vulnerable children and youth for research purposes.*

Section 5 of O. Reg. 191/18 establishes requirements and restrictions applicable to the Ministry and a service provider when using personal information for the purposes described within the *CYFSA,* including for research.[12]

Under the regulation, the Ministry, service providers, prescribed entities, and persons and entities who are not prescribed are required to prepare a research plan that meets prescribed criteria.[13] However, the Ministry and service providers under the *CYFSA* are exempt from some of the research plan requirements, including the requirement to include information in the research plan about how and when personal information will be disposed of or returned to the service provider. The Ministry is also exempt from the requirement to include its research funding source in the research plan.

In our view, the Ministry and service providers should be required to document how and when personal information used for research will be returned or disposed of. This will ensure transparency and increase public confidence that the Ministry and service providers are handling personal information appropriately, in accordance with the purposes of the *CYFSA*. Similarly, requiring the Ministry to disclose its research funding source would provide for more transparency and enhance public trust.

The research plan scheme under the *CYFSA* is modeled after the research plan requirements set out in *PHIPA* and O. Reg. 329/04. However, under *PHIPA*, health information custodians conducting their own research are not exempt from any of the requirements for a research plan. In the spirit of accountability and transparency, the scheme created under the *CYFSA* should be consistent with *PHIPA*. The Ministry and

[12] See paragraph 6 of section 283 (1) and section 291(1)(j) of the *Child, Youth and Family Services Act*
[13] See section 5(1) and 4(2) of O. Reg., 191/18

service providers should not be exempt from requirements meant to protect the privacy of Ontarian's personal information. Accordingly, the IPC continues to urge the government to amend section 5 of O. Reg. 191/18 to remove the exemptions, and strengthen the minimum requirements for the use of personal information by the Ministry and service providers, as detailed in Appendix A.

### Recommendation 3.2: Enhance the Research Requirements for Prescribed Entities and Persons and Entities who are not Prescribed

*The CYFSA lacks adequate privacy protections for personal information that is used for research purposes by prescribed entities and persons and entities that are not prescribed. Further to previous submissions, the IPC continues to urge the government to amend the CYFSA to strengthen the protection of personal information used for research purposes.*

As previously mentioned, the *CYFSA* allows service providers to disclose personal information to two categories of entities: 1) prescribed entities and 2) persons and entities that are not prescribed. These disclosures are permitted for the purposes of analysis and compiling statistics for planning, managing, and evaluating services, provided certain conditions are met.

When conducting research, O. Reg. 191/18 requires both categories of entities to submit a written research plan, including minimum required content, to a research ethics board for approval. The regulations mirror elements of *PHIPA.* However, key privacy elements are missing.[14]

*PHIPA* sets out widely accepted, essential elements of the framework for using personal health information for research, namely, the matters a research ethics board must consider, the minimum requirements for a research ethics board's decision, and the minimum requirements applicable to researchers receiving the personal information.[15] Such provisions provide consistency in the research ethics board approval process and ensure researchers are respecting the privacy of individuals.

To ensure that research is conducted in an accountable, transparent and privacy protective manner by all persons or entities, the IPC continues to urge the government to amend section 4 (1) of O. Reg. 191/18 to strengthen the requirements for the use of personal information for research purposes by mirroring the similar requirements under *PHIPA*, as detailed by Appendix A.

## Issue 4: The Collection, Use and Disclosure of the Personal Information of Deceased Individuals

### Recommendation 4.1: Clarify who can Act as Substitute Decision-Maker for a Deceased Individual

[14] See section 44 of the *Personal Health Information Protection Act*
[15] See sections 44 (3), (4) and (6) of the *Personal Health Information Protection Act*

*A lack of clarity within the CYFSA regarding who may consent to the collection, use or disclosure of personal information on behalf of a deceased individual limits access to and the protection of a deceased person's personal information. The IPC recommends amending Part X of the CYFSA to clarify who may consent, withhold, or withdraw consent on behalf of a deceased individual in relation to the personal information of the deceased individual.*

While the *CYFSA* provides that a substitute decision-maker must take into consideration the wishes, values and beliefs of an individual who is incapable or deceased,[16] it does not identify who may consent on behalf of a deceased individual. This lack of clarity within the *CYFSA* leads to a risk that there will be no statutory substitute decision-maker for deceased individuals, with the result that the personal information of deceased individuals may be rendered inaccessible under the *CYFSA*.

*PHIPA* provides that where an individual is deceased, the deceased's estate trustee or the person who has assumed responsibility for the administration of the deceased's estate (if the estate does not have an estate trustee) may give, withhold, or withdraw consent on behalf of the individual.[17] This provision within *PHIPA* makes it clear who can act as a substitute decision-maker for a deceased individual and allows for access to the personal information of a deceased individual even in the absence of an estate trustee.

In order to protect the personal information of deceased individuals while also ensuring that it can be accessed and used for appropriate purposes, such as the administration of the deceased's estate, the IPC recommends amending the *CYFSA* to add a provision specifying who may consent, withhold or withdraw consent in such cases.

**Recommendation 4.2: Clarify Service Providers' Authority to Disclose Personal Information in Compassionate Circumstances, where the Individual is Deceased**

*The CYFSA is also unclear regarding the amount of personal information that can be shared with family members and friends when an individual is deceased. The IPC recommends amending Part X of the CYFSA to clarify service providers' authority to disclose personal information without consent in compassionate circumstances, where the individual is deceased.*

Section 292(1)(e) of the *CYFSA* provides that a service provider may, without the consent of the individual, disclose the personal information of a deceased individual for the purposes of contacting a relative, member of the extended family, or friend of the individual if the individual is deceased. While this provision provides authority to contact a relative or friend of a deceased individual, unlike section 38(4)(b) of *PHIPA*, it does not clarify what, if any, personal information can be disclosed.

[16] See section 302 (1) of the *Child, Youth and Family Services Act*
[17] See section 23 (1) 4 of the *Personal Health Information Protection Act*

*PHIPA* provides that a health information custodian may disclose personal health information about an individual who is deceased (or is reasonably suspected to be deceased) for several purposes, including: for the purposes of identifying the individual, for informing any person whom it is reasonable to inform in the circumstances of the fact that the individual is deceased or reasonably suspected to be deceased and the circumstances of the death where appropriate, or the spouse, partner sibling or child of the individual if the recipients reasonably require the information to make decisions about their own health care or their children's health care.[18]

To provide clarity regarding the amount of personal information that can be shared in compassionate circumstances, while also ensuring the protection of deceased individuals' personal information, the IPC recommends repealing s. 292 (1)(e) of the *CYFSA* and replacing it with language more consistent with the equivalent more detailed provision within *PHIPA*, for example:

**Disclosure without Consent, s. 292 (1)**

(e) if the individual is deceased, or is reasonably expected to be deceased,

(i) for the purpose of identifying the individual

(ii) for the purpose of informing any person whom it is reasonable to inform in the circumstances of

(a) The fact that the individual is deceased or reasonably suspected to be deceased, and
(b) The circumstances of death, where appropriate;

## Issue 5: The Powers of the Information and Privacy Commissioner of Ontario

### Recommendation 5.1: Allow the Commissioner to be as Transparent as Possible

As part of being a modern and effective regulator, the IPC embraces transparency and promoting public trust in our public institutions. The IPC strives to ensure that Ontarians understand their access and privacy rights and the important work the IPC does to support those rights by being as transparent as possible.

Currently, the IPC is subject to confidentiality provisions under the *CYFSA*[19] which mirror those within s. 68(3) of *PHIPA.* Broadly speaking, these sections require the IPC to keep information confidential subject to some exceptions. While the IPC appreciates the importance of maintaining some degree of confidentiality where necessary and required, the IPC believes that the *CYFSA* should explicitly afford the IPC with greater discretion and flexibility to disclose or make public more information about the work we do.

[18] See section 38 (4) of the *Personal Health Information Protection Act*
[19] See section 328(3) of the *Child, Youth and Family Services Act*

Given the era of transparency and the importance of accountability, the IPC recommends that section 328(3) of the *CYFSA* be amended and relaxed to allow for greater public transparency. For consistency, any changes and amendments should also be made to *PHIPA*. The IPC would be pleased to discuss this issue further with the Ministry.

## Conclusion

The IPC recommends that:

1. The *CYFSA* be amended to make the Ministry subject to the same privacy rules as other service providers;
2. The *CYFSA* be amended to limit the Ministry's powers to require service providers to collect and disclose information to the Ministry;
3. The *CYFSA* be amended to limit the Ministry's powers for indirect collection and data integration as a funder, planner and manager of service delivery;
4. The *CYFSA* be amended to enhance service providers' transparency and accountability with respect to the retention of records;
5. The Ministry consider defining the meaning and regulating the activities of an agent under the *CYFSA;*
6. O. Reg. 191/18 be amended to further enhance the protection of personal information when it is disclosed to persons and entities who are not prescribed;
7. O. Reg. 191/18 be amended to enhance the research requirements for service providers, including the Ministry;
8. O. Reg. 191/18 be amended to enhance the research requirements for prescribed entities and persons and entities who are not prescribed;
9. The *CYFSA* be amended to clarify who can act as a Substitute Decision-Maker for a deceased individual;
10. The *CYFSA* be amended to clarify service providers' authority to disclose personal information without consent in compassionate circumstances, where the individual is deceased;
11. The *CYFSA* be amended to allow the Commissioner to be as transparent as possible; and
12. The Ministry consult with my office on the access and privacy implications of these, and any other, recommendations being considered prior to the publication of the Ministry's report.

As previously stated, children, youth and families share significant amounts of sensitive personal information with service providers when receiving a service under the *CYFSA.* All children and youth who receive services under the *CYFSA* are inherently vulnerable and many belong to disadvantaged populations, which places them and their families in a position of not only increased vulnerability, but at greater risk of inequitable outcomes during service delivery. Therefore, it is imperative to ensure that legislation requires service providers and the Ministry to be highly accountable and transparent with respect to the collection, use and disclosure of personal information.

The recommended amendments are necessary to enhance the protection of the personal information and the privacy and access rights of Ontarians who receive child, youth, and family services under the *CYFSA*, while still enabling the Ministry, services providers, prescribed entities, and persons and entities who are not prescribed to carry out their mandated functions.

Thank you for receiving my comments and recommendations with respect to the first review of the *CYFSA* since its proclamation in 2018.

In the spirit of openness and transparency, I will be posting this submission on the IPC website.

Sincerely,

Patricia Kosseim
Commissioner

CC: Deputy Minister Denise Allyson Cole, Ministry of Children, Community and Social Services
Assistant Deputy Minister Rupert Gordon, Ministry of Children, Community and Social Services
Associate Deputy Minister John Roberts, Ministry of Public and Business Service Delivery

# Appendix A: Proposed Amendments to O. Reg. 191/18: Personal Information

## Prescribed requirements and restrictions, ss. 293 (2) and (3)

2. (1) The following requirements and restrictions apply to the disclosure of personal information by a service provider to a person or entity that is not a prescribed entity under subsection 293 (2) and (3) of the Act:

1. A service provider may only disclose the personal information if,

i. the person or entity to which the information will be disclosed identifies as a First Nations, Inuit or Métis person or entity,

ii. the information relates to First Nations, Inuit or Métis individuals,

iii. the service provider and the person or entity to which the information will be disclosed have entered into an agreement ~~with respect to~~ addressing the use, security, disclosure, and return or disposal of the information,

iv. the agreement referred to in subparagraph iii,

A. requires the person or entity to whom the information is disclosed to notify the service provider who disclosed it of any loss or theft of the personal information or of any unauthorized use or disclosure of the information at the first reasonable opportunity, and

B. sets out how the person or entity will notify the service provider,

v. the service provider has received written acknowledgement from each of the bands or First Nations, Inuit or Métis communities whose member's personal information will be disclosed, indicating that the band or community approves of the fact that the person or entity will receive the personal information, and

vi. the service provider has received written acknowledgement from each of the bands or First Nations, Inuit or Métis communities with which an individual whose personal information will be disclosed identifies, indicating that the band or community approves of the fact that the person or entity will receive the personal information.

(2) A person or entity that is not a prescribed entity who receives personal information from a service provider under subsection 293 (2) or (3) of the Act shall comply with the conditions or restrictions, if any, that the service provider imposes in the agreement described in subclauses iii and iv. of paragraph 1 of subsection 2(1).

…

**Restrictions on use, s. 293 (9)**

**4.** (1) Despite subsection 293 (9) of the Act, a prescribed entity, or a person or entity that is not a prescribed entity, may use personal information received under subsection 293 (1), (2) or (3) of the Act for a purpose other than for which it was received if the following requirements are met:

1. The person or entity shall submit a research plan that meets the requirements of subsection (2) respecting the use of that personal information to a research ethics board that meets the following criteria:

    i. It has at least five members.

    ii. At least one member has no affiliation with the person or persons that established the research ethics board.

    iii. At least one member is knowledgeable in research ethics, either as a result of formal training in research ethics or practical or academic experience in research ethics.

    iv. At least two members have expertise in the methods or in the areas of research being considered.

    v. At least one member is knowledgeable in privacy issues but does not provide legal advice to a service provider.

2. The person or entity has received written confirmation from each member of the research ethics board that the member's personal interest in the use of the personal information or the performance of the research does not conflict or appear to conflict with the member's ability to objectively review the research plan.

3. ~~The research ethics board has approved the plan.~~ The person or entity has received written confirmation from the research ethics board that, when deciding whether to approve the research plan that the person or entity submitted to it, the research ethics board considered the relevant matters, including,

    i. whether the objectives of the research can reasonably be accomplished without using the personal information that is to be collected;

    ii. whether, at the time the research is conducted, adequate safeguards will be in place to protect the privacy of the individuals whose personal information is being collected or used and to preserve the confidentiality of the information;

iii. the public interest in conducting the research and the public interest in protecting the privacy of the individuals whose personal information is being collected or used; and

iv. whether obtaining the consent of the individuals whose personal information is being collected or used would be impractical.

4. The research ethics board has provided the person or entity with a decision, in writing, approving the research plan and setting out whether the approval is subject to any conditions.

5. When using personal information about an individual under this section, the person or entity shall,

i. comply with the conditions, if any, specified by the research ethics board in respect of the research plan;

ii. use the information only for the purposes set out in the research plan as approved by the research ethics board;

iii. not publish the information in a form that could reasonably enable a person to ascertain the identity of the individual;

iv. not disclose the information except as permitted or required by law;

v. not make contact or attempt to make contact with the individual, directly or indirectly, unless the service provider from whom the information was collected first obtains the individual's consent to being contacted; and

vi. notify the service provider from whom the information was collected immediately in writing if the person or entity becomes aware of any breach of this subsection.

**Restrictions on use of personal information by Minister and service provider**

**5**. The Minister shall not use personal information for the purposes described in paragraph 6 of subsection 283 (1) of the Act and a service provider shall not use personal information collected for the purposes of providing a service for the purpose set out in clause 291 (1) (j) of the Act unless the following requirements are met:

1. The Minister or service provider, as the case may be, prepares a research plan that meets the requirements of subsection 4 (2) ~~with the exception of those requirements set out in,~~

~~i. paragraphs 12 and 14 of that subsection, in the case of the Minister, or~~

~~ii. paragraph 12 of that subsection, in the case of a service provider.~~

2. The Minister or service provider, as the case may be, submits the research plan to a research ethics board that meets the criteria set out in paragraph 1 of subsection 4 (1).

3. The Minister or service provider, as the case may be, has received written confirmation from each member of the research ethics board that the member's personal interest in the use of the personal information or the performance of the research does not conflict or appear to conflict with the member's ability to objectively review the research plan.

~~4. The research ethics board has approved the plan.~~

4. The Minister or service provider, as the case may be, has received written confirmation from the research ethics board that, when deciding whether to approve the research plan that the Minister or service provider submitted to it, the research ethics board considered the relevant matters, including,

    i. whether the objectives of the research can reasonably be accomplished without using the personal information that is to be collected;
    ii. whether, at the time the research is conducted, adequate safeguards will be in place to protect the privacy of the individuals whose personal information is being collected or used and to preserve the confidentiality of the information;
    iii. the public interest in conducting the research and the public interest in protecting the privacy of the individuals whose personal information is being collected or used; and
    iv. whether obtaining the consent of the individuals whose personal information is being collected or used would be impractical.

5. ~~The research ethics board has approved the plan.~~ The research ethics board has provided the Minister or service provider, as the case may be, with a decision, in writing, approving the research plan and setting out whether the approval is subject to any conditions.

6. When using personal information about an individual under this section, the Minister or service provider, as the case may be, shall,

    i. comply with the conditions, if any, specified by the research ethics board in respect of the research plan;
    ii. use the information only for the purposes set out in the research plan as approved by the research ethics board;
    iii. not publish the information in a form that could reasonably enable a person to ascertain the identity of the individual;
    iv. not disclose the information except as permitted or required by law;

v. if the information was collected indirectly, not make contact or attempt to make contact with the individual, directly or indirectly, unless the person that collected the information first obtains the individual's consent to being contacted; and

vi. if the information was collected indirectly from a service provider, prescribed entity, or person or entity that is not a prescribed entity, notify the service provider, person or entity from whom the information was collected immediately in writing if the Minister or service provider becomes aware of any breach of this subsection

…

**Prescribed requirements, s. 309 (1) (b) of the Act**

**10.** (1) For the purposes of clause 309 (1) (b) of the Act, this section prescribes requirements in respect of the retention, transfer and disposal of records.

(8) A service provider shall, in a manner that is practical in the circumstances, make available to the public the records retention policy described in subsection (5).

…