Information and Privacy Commissioner of Ontario

Comments of the Information and Privacy Commissioner of Ontario on the Proposed Regulation under Part X of the *Child, Youth and Family Services Act, 2017*

Brian Beamish
Commissioner
January 22, 2018

The Ministry of Children and Youth Services (the Ministry) has posted the first phase of the proposed regulation to support the implementation of the *Child, Youth and Family Services Act, 2017* (the *Act*). This includes the proposed regulation under Part X of the *Act* (the draft regulation), which governs personal information.

The Office of the Information and Privacy Commissioner of Ontario (IPC) has reviewed the draft regulation and proposes six recommendations which are necessary to protect the privacy of Ontarians. These recommendations generally relate to:

- strengthening privacy breach notification and reporting requirements;
- placing requirements and restrictions on persons and entities that are not prescribed;
- enhancing the research requirements imposed on prescribed entities, the Minister, service providers, researchers and persons or entities that are not prescribed; and
- clarifying the requirements on service providers concerning the handling, retention and transfer of records.

For ease of reference, the draft regulation with the IPC's proposed amendments is set out in its entirety at Appendix A.

1. NOTIFICATION OF PRIVACY BREACH TO SERVICE PROVIDERS AND INDIVIDUALS

The *Act* and the draft regulation authorize service providers to disclose personal information to prescribed entities, and to persons and entities that are not prescribed. While section 308(1) of the *Act* requires service providers to notify affected individuals if personal information collected for the purpose of providing a service is stolen, lost or used or disclosed without authority, this requirement only applies to personal information that is in the service provider's custody or control. This same limitation applies in section 308(2) of the *Act*, which requires service providers to notify the IPC and the Minister if the circumstances surrounding the breach meet prescribed requirements. These limitations result in a gap. Individuals might not be notified when their personal information has been disclosed to a person or entity and is subsequently stolen, lost or used or disclosed without authority.

When a breach occurs in relation to personal information that has been disclosed to a person or entity, the service provider from whom the information was disclosed must be informed in order to notify the individual. While the IPC hopes that all persons or entities that receive personal information from a service provider will implement sufficient safeguards to protect the information they receive, the IPC understands that breaches do occur. In the event of a

breach, timely notification to the individual is essential to containing the potential impact of a breach. *The Personal Health Information Protection Act* (*PHIPA*) and other modern privacy legislation include requirements to notify individuals affected by a privacy breach.

(a) Require prescribed entities to notify service provider

The IPC recommends that the regulation require prescribed entities to notify service providers if personal information they received from a service provider has been stolen, lost or used or disclosed without authority.

The *Act* provides the authority to prescribe these requirements. Section 293(1) allows service providers to disclose personal information to prescribed entities for the purposes of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of services, and the allocation of resources to or planning for those services, including their delivery. Section 293(9) prohibits a prescribed entity that receives personal information from a service provider under sections 293(1) and (3) from using the information for purposes other than those for which it received the information, and prohibits disclosure of the information except as required by law, subject to any prescribed exceptions and additional requirements. Clause 11 of section 348 of the *Act* confirms this authority. Accordingly, the government has the authority to prescribe additional requirements, such as breach notification, for uses and disclosures that fall outside section 293(1). Any theft, loss or unauthorized use or disclosure would be outside section 293(1).

Additionally, section 293(3) of the *Act* authorizes the Minister to require service providers to disclose information, including personal information, to a prescribed entity for the purposes described in section 293(1). A prescribed entity receiving information under section 293(3) must comply with any prescribed requirements with respect to the use, security, disclosure, return or disposal of the information. Clause 8 of section 348 of the *Act* confirms this regulation-making authority. Therefore, the government has authority to prescribe requirements, such as breach notification, for prescribed entities receiving personal information under section 293(3).

Although paragraph 13 of section 4(2) of the draft regulation requires a prescribed entity's research plan to include a description of how the entity will, at the earliest reasonable opportunity, notify the service provider from whom the personal information was received of any theft, loss or unauthorized use or disclosure of the personal information, this does not create a legal obligation on the prescribed entity to notify. Further, this would only apply to circumstances where the prescribed entity is using the personal information for research purposes.

The IPC recommends that the following provision be added to section 4 of the draft regulation:

> 4. (3) If a prescribed entity has received personal information from a service provider under subsection 293 (1) or (3) of the Act and the personal information

is stolen, lost or used or disclosed without authority, the prescribed entity shall notify the service provider at the first reasonable opportunity.

(b) Require persons or entities that are not prescribed to notify service provider

The IPC recommends that the regulation require persons and entities that are not prescribed to notify service providers that disclose personal information to them if the information has been stolen, lost or used or disclosed without authority.

The *Act* provides the authority to prescribe these requirements. Section 293(2) allows service providers to disclose personal information to persons and entities that are not prescribed for the purposes of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of services, and the allocation of resources to or planning for those services, including their delivery. Section 293(3) authorizes the Minister to require service providers to disclose information, including personal information, to a person or entity that is not prescribed, for those same purposes.

Sections 293(2) and (3) of the *Act* require a person or entity receiving personal information from a service provider to comply with "any prescribed requirements and restrictions with respect to the use, security, disclosure, return or disposal of the information." Accordingly, a person or entity that is not prescribed that receives information under those sections must comply with any prescribed requirements with respect to the use, security, disclosure, return or disposal of the information. Clause 8 of section 348 of the *Act* confirms this authority. Therefore, the government has authority to prescribe requirements, such as breach notification, for persons and entities that are not prescribed that are receiving personal information under sections 293(2) and (3).

Persons and entities that are not prescribed are also required by paragraph 13 of section 4(2) of the draft regulation to include a description of how the person or entity will, at the earliest reasonable opportunity, notify the service provider from whom the personal information was received of any theft, loss or unauthorized use or disclosure of the personal information. As noted above, this requirement does not create a legal obligation requiring the person or entity to notify the service provider. Further, this would only apply to circumstances where the person or entity is using the personal information for research purposes.

The IPC recommends that the following provision be added to section 4 of the draft regulation:

> 4. (4) If a person or entity that is not a prescribed entity has received personal information from a service provider under subsection 293 (2) or (3) of the Act and the personal information is stolen, lost or used or disclosed without authority, the person or entity shall notify the service provider at the first reasonable opportunity.

(c) Require prescribed entities receiving information from a prescribed entity or a person or entity that is not prescribed to notify the person or entity that disclosed the information

Section 6 of the draft regulation permits a prescribed entity or a person or entity that is not prescribed to disclose personal information received under sections 293(1), (2) or (3) of the *Act* to another prescribed entity who meets specified requirements. However, the draft regulation does not contain a corresponding obligation on these entities to notify the person or entity that disclosed the personal information if the information has been stolen, lost or used or disclosed without authority.

The IPC recommends that the proposed regulation be amended to add the following provisions to section 6:

> 6. (2) If a prescribed entity has received personal information under this section and the personal information is stolen, lost or used or disclosed without authority, the prescribed entity shall notify the person or entity that disclosed the personal information at the first reasonable opportunity.
>
> (3) If a prescribed entity or a person or entity that is not a prescribed entity receives notice that personal information that the person or entity disclosed under this section has been lost, stolen or used or disclosed without authority, the person or entity shall notify the service provider that disclosed the personal information at the first reasonable opportunity.

(d) Require service providers to notify the individual

Service providers should be required to notify individuals when they receive notice of a privacy breach from prescribed entities or persons or entities that are not prescribed. This notice should further advise individuals of their right to make a complaint to the IPC.

The IPC recommends that the following provision be added to the proposed regulation:

> 12. If a service provider receives notice under subsection 4 (3), 4 (4) or 6 (3) that personal information it disclosed to a prescribed entity or a person or entity that is not a prescribed entity under subsection 293 (1), (2) or (3) of the Act has been stolen, lost or used or disclosed without authority, the service provider shall,
>
> (a) notify the individual to whom the information relates at the first reasonable opportunity of the theft, loss or unauthorized use or disclosure; and
>
> (b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under section 316 of the Act.

2. NOTIFICATION AND REPORTING OF BREACH TO THE MINISTER AND THE IPC

Section 9 of the draft regulation sets out the circumstances in which a service provider is required to notify the IPC and the Minister of the theft, loss or unauthorized use or disclosure of personal information under section 308(3) of the *Act*. The IPC recommends three amendments to the draft regulation to ensure that privacy breaches are properly reported to the IPC and the Minister.

(a) Reference personal information in the service provider's "custody or control"

The circumstances set out in section 9 of the draft regulation do not specify what personal information is at issue, with the exception of paragraph 4. Paragraph 4 specifies that the personal information must be "in the custody or control of the service provider." However, the other paragraphs lack this specification.

The IPC recommends that the section be amended to clarify that service providers' notification requirements are triggered only where personal information in their custody or control is stolen, lost or subject to unauthorized use or disclosure, except in the circumstances described in paragraph 5 of section 9 of the draft regulation. This amendment will ensure consistency across the *Act* and its regulation, as well as with section 6.3(1) of O. Reg. 329/04 under *PHIPA*.

The IPC recommends that paragraphs 1, 2, 3, and 6 of section 9 of the draft regulation be amended to reference personal information in the service provider's custody or control, as set out in Appendix A.

(b) Require reporting breaches where disciplinary action was taken

Section 9 of the draft regulation addresses the circumstances in which the IPC and the Minister must be notified of a privacy breach. This section should be expanded to include a requirement that service providers report a privacy breach to the IPC and the Minister where an employee or any other person acting on behalf of the service provider has been terminated, suspended or subject to disciplinary action as a result of a privacy breach, or has resigned for reasons related to a breach.

Although many breaches which result in employee discipline, termination or resignation would likely be captured under another paragraph of section 9, adding these circumstances to the regulation would provide important clarification by making it absolutely clear to service providers that breaches of this nature must be reported. Additionally, these amendments would provide consistency with the circumstances in which privacy breaches must be reported under paragraphs 5 and 6 of section 6.3(1) of O. Reg 329/04 under *PHIPA*.

Accordingly, the IPC recommends that the following paragraphs be added to section 9 of the draft regulation:

> 7. An employee of the service provider or any other person acting on behalf of the service provider is terminated, suspended or subjected to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal of personal information by the employee or other person.
>
> 8. An employee of the service provider or any other person acting on behalf of the service provider resigns and the service provider has reasonable grounds to believe that the resignation is related to an investigation or other action by the service provider with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of personal information by the employee or other person.

(c) Clarify reporting obligations of service providers who are also health information custodians under *PHIPA*

Section 11 of the draft regulation requires service providers to annually report statistics to the IPC about access and correction requests and privacy breaches. The IPC is unclear whether and how these reporting requirements will apply to service providers that are also health information custodians as defined under section 3 of *PHIPA*.

Section 285(3) of the *Act* exempts health information custodians from a number of sections of Part X of the *Act*, including the requirements with respect to the collection, use, or disclosure of personal health information. However, because section 11 of the draft regulation does not refer back to a specific section of Part X, it is unclear whether it applies to health information custodians.

The IPC recommends that the Ministry clarify whether and how the reporting requirements in section 11 will apply to service providers that are also health information custodians. The IPC notes that health information custodians are already bound by obligations with respect to the annual reporting of privacy breaches under O. Reg 329/04 under *PHIPA*.

3. REQUIREMENTS AND RESTRICTIONS APPLICABLE TO PERSONS OR ENTITIES THAT ARE NOT PRESCRIBED

Section 2 of the draft regulation permits service providers to disclose personal information to a person or entity that is not prescribed under section 293(2) of the *Act*. This section applies if the person or entity to which the information will be disclosed identifies as a First Nations, Inuit or Métis person or entity, and the service provider and the person or entity have entered

into an agreement with respect to the use, security, disclosure, return or disposal of the information. However, there are no minimum requirements for the agreement, nor is there a requirement for the person or entity to comply with the agreement.

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 safeguards must be implemented to ensure that the privacy and confidentiality of Ontarians' personal information is protected, regardless of whether it is held by a prescribed entity or a person or entity that is not prescribed.

Any person or entity that receives personal information for the purpose of analysis or compiling statistical information without the knowledge or consent of the individual must be transparent and accountable. To this end, the IPC strongly recommends setting minimum standards in the regulation for persons or entities that are not prescribed who are receiving personal information under sections 293(2) and (3). In addition, the regulation should be strengthened by establishing minimum requirements for the agreements between service providers and persons or entities receiving personal information under section 293(2) and (3). For example, the agreements should include limitations on further disclosures, contact with the individual, and notification in the event of a breach.

As discussed above, the authority to prescribe such requirements is found in sections 293(2) and (3) of the *Act*, which permit service providers to disclose personal information to a person or entity that is not prescribed for the purposes of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of services, and the allocation of resources to or planning for services, including their delivery. These provisions specifically contemplate that a person or entity that receives personal information under these sections must comply with "any prescribed requirements and restrictions with respect to the use, security, disclosure, return or disposal of the information." Clause 8 of section 348 of the *Act* confirms this regulation-making authority.

Accordingly, the IPC recommends amending section 2 of the draft regulation as follows:

Prescribed requirements and restrictions, ss. 293 (2) and (3) of the Act

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 subsections 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, and

ii. the service provider and the person or entity have entered into an agreement ~~with respect to~~ addressing the use, security, disclosure, and return or disposal of the 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,

(a) comply with the conditions or restrictions, if any, that the service provider imposes in the agreement described in subclause ii of paragraph 1 of subsection 2 (1); and

(b) notify the service provider from whom the information was collected immediately in writing if the person or entity becomes aware of any breach of section 293 of the Act or the agreement described in subclause ii of paragraph 1 of subsection 2 (1).

4. ENHANCING THE REQUIREMENTS APPLICABLE TO PARTIES USING PERSONAL INFORMATION FOR RESEARCH

The IPC urges that the draft regulation be amended with respect to the research requirements imposed on prescribed entities, the Minister, service providers, researchers and persons and entities that are not prescribed in order to protect the privacy rights of Ontarians as well as to ensure consistency and transparency within the sector.

(a) Prescribed Entities and Persons and Entities that are Not Prescribed Using Personal Information for Research

As noted above, section 293(9) of the *Act* prohibits a prescribed entity or a person or entity that is not prescribed that receives personal information under section 293(1), (2) or (3) from using the information except for the purposes for which it was received, or disclosing the information except as required by law, subject to the exceptions and additional requirements that are prescribed. The authority to prescribe such requirements is outlined above in Part 1(a) of this submission.

Section 4 of the draft regulation creates an exception to the prohibition at section 293(9) of the *Act,* as it permits a prescribed entity or a person or entity that is not prescribed to use personal information received under section 293(1), (2) or (3) for a purpose other than for which it was received, subject to three requirements:

1. the person or entity submits a research plan respecting the use of the personal information to a research ethics board that meets certain criteria;

2. the person or entity has received written confirmation from each member of the research ethics board confirming that there is no conflict of interest; and

3. the research ethics board has approved the plan.

The draft regulation mirrors elements of the research requirements set out in sections 44(1) and (2) of *PHIPA*. However, key components of sections 44(3), (4) and (6) of *PHIPA* are missing.

Sections 44(3), (4) and (6) of *PHIPA* set out widely accepted, essential elements of the framework for using personal 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. These provisions provide consistency in the research ethics board approval process and ensure researchers are respecting the privacy of the individuals. The omission of these types of provisions from the draft regulation is concerning, as it creates a gap in the privacy protections individuals can expect depending on who is holding the personal information.

Accordingly, the IPC recommends that section 4 of the draft regulation be amended as follows:

Restrictions on use, s. 293 (9) of the Act

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 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 approved the plan.~~ 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.

(b) Minister and Service Providers Using Personal Information for Research

Section 5 of the draft regulation establishes requirements and restrictions applicable to the Minister's use of personal information for the purposes described in paragraph 6 of section 283(1) of the *Act* and service providers' use of personal information for the purpose set out in section 291(1)(j) of the *Act*. This section similarly omits the research requirements in sections 44(3), (4) and (6) of *PHIPA*.

Paragraph 1 of section 5 of the draft regulation requires that the Minister or service provider prepare a research plan that meets the requirements in section 4(2) of the draft regulation, subject to two exceptions. The Minister is exempt from including the requirements in paragraphs 12 and 14 of section 4(2) in its research plan. Similarly, the requirement in paragraph 12 does not apply to service providers. The basis for these exceptions is not clear.

Paragraph 12 requires that the research plan include information about how and when personal information will be disposed of or returned to the service provider. This requirement is similar to paragraph 9 of the research plan requirements in section 16 of O. Reg 329/04 under *PHIPA*. While the Minister and service providers may not need to return personal information when conducting their own research, both should be required to document how and when personal information used for research will be disposed of. This will ensure transparency and increase public confidence that the Minister and service providers are handling personal information appropriately, in accordance with the purposes of the *Act*.

Paragraph 14 requires that the funding source of the research be included in the research plan. This requirement is identical to paragraph 10 of the research plan requirements in section 16 of O. Reg 329/04 under *PHIPA*. While the Ministry may often fund its own research, there may be circumstances in which the Ministry is working with other institutions or organizations that are also providing funding. Clarifying the source of funding in the research plan will provide for more transparency.

This scheme is modeled after the research plan requirements set out in *PHIPA* and O. Reg 329/04. Under *PHIPA*, health information custodians conducting their own research are not exempt from any of the requirements for a research plan. The scheme created under the *Act* should be consistent with *PHIPA*. Accordingly, the IPC recommends that the proposed exemptions be removed from the draft regulation.

For the reasons outlined above, the IPC recommends that section 5 of the draft regulation be amended as follows:

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.~~ 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.

(c) Researchers Using Personal Information for Research

Section 6 of the draft regulation creates another exception to the prohibition at section 293(9) of the *Act,* as it permits a prescribed entity or a person or entity that is not prescribed to disclose personal information received under sections 293(1), (2) or (3) to another prescribed entity for the purposes described in section 293(1) of the *Act,* or to a researcher who meets the same general requirements set out in section 4. Again, the research requirements in sections 44(3), (4) and (6) of *PHIPA* are not included.

In addition, the IPC recommends that the agreement between a researcher and a person or entity that discloses personal information to the researcher should require the researcher to notify the person or entity if personal information they receive is stolen, lost or used or disclosed without authority. This requirement would address a gap in breach notification similar to that described in Part 1 of this submission regarding notification to service providers disclosing personal information to persons and entities.

The IPC recommends that section 6 of the draft regulation be amended as follows:

Exception to restriction on disclosure by prescribed entity

6. (1) Despite subsection 293 (9) of the Act, a prescribed entity, or a person or entity that is not a prescribed entity, may disclose personal information disclosed to it under subsection 293 (1), (2) or (3) of the Act to,

(a) another prescribed entity, if the disclosure is for the purposes described in subsection 293 (1) of the Act; or

(b) a researcher who has ~~had a research plan that meets the requirements of subsection 4 (2) approved by a research ethics board that meets the criteria set out in paragraph 1 of subsection 4 (1).~~,

i. met the requirements of paragraphs 2, 3 and 4 of subsection 4 (1);

ii. had a research plan that meets the requirements of subsection 4 (2) approved by a research ethics board that meets the criteria set out in paragraph 1 of subsection 4 (1);

iii. entered into an agreement with the prescribed entity or person or entity that is not a prescribed entity addressing the use, security, disclosure, and return or disposal of the information, in which the researcher agrees to, at minimum,

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

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

C. comply with the conditions and restrictions, if any, that the person or entity imposes with respect to the use, security, disclosure, return or disposal of the information;

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

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

F. 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;

G. notify the person or entity from whom the information was collected immediately in writing if the researcher becomes aware of any breach of the agreement; and

H. notify the person or entity from whom the information was collected at the first reasonable opportunity if personal information that was collected has been stolen, lost or used or disclosed without authority.

5. CLARIFYING REQUIREMENTS CONCERNING THE HANDLING, RETENTION AND TRANSFER OF RECORDS

The *Act* and draft regulation impose requirements on service providers with respect to the handling, retention and transfer of records. While these efforts are laudable, the draft regulation should be strengthened to ensure consistency and transparency in retention practices across the sector, and to protect Ontarians' access and privacy rights with respect to personal information held by service providers.

(a) Retention of Records

Section 10 of the draft regulation sets out requirements for the retention of records by service providers. Specifically, each service provider is required to develop and maintain a records retention policy. The draft regulation dictates what must be contained in such a policy, including identifying each type of record and how long it will be kept. The draft regulation also requires that certain factors be considered by service providers in determining how long

to keep each type of record. However, the regulation does not stipulate the minimum 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 draft regulation does not facilitate consistent and transparent retention practices across child, youth and family services sectors. This is important because retention and record management practices have a direct impact on both access to personal information and the privacy of individuals with respect to their personal information. The IPC recommends the following amendments.

(i) Require service providers to make retention policies public

The IPC recommends that the draft regulation be amended to require service providers to make their records retention policies publicly available. Service providers are required by section 311 of the *Act* to make a general description of their information practices available to the public. A specific requirement to make retention policies publicly available would complement this general requirement.

One benefit of publicly available retention policies would be to support access to information, by providing clarity to individuals about what records are kept and for how long. For example, individuals wishing to know more about their time in the care of a Children's Aid Society (CAS) many years prior may be uncertain as to whether their records still exist. By providing clarity about what records are kept by the service provider and for how long, publicly available retention policies can support individuals in deciding whether and when to seek access to their personal information. Additionally, publicly available retention policies could allow for improved oversight of service providers' compliance with the requirements to develop and maintain such policies.

Accordingly, the IPC recommends that the following provision be added to section 10 of the draft regulation:

(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).

(ii) Develop common records retention requirements for children's aid societies (CASs) and other sectors

The IPC recognizes that diversity among service providers may make it impractical for the Ministry to dictate common retention timelines for all service providers. However, there are certain sectors, most notably child welfare, for which common retention requirements should be developed.

Common retention requirements for the child welfare sector would support access to information, by making it simpler to understand what types of records are kept by all CASs, and for how long. Many individuals are served by more than one CAS, and may be seeking access to information held by several different CASs. It would be cumbersome for individuals to have to grapple with different retention schedules for each of Ontario's 48 CASs.

It would also be impractical for each CAS to have its own retention policy, especially because an increasing number of records are shared by CASs through the Child Protection Information Network (CPIN). Because CASs routinely share information with one another as part of child protection investigations and for screening of alternate caregivers, they require certainty about how long various types of records are retained by other CASs. This certainty would be facilitated by common retention requirements for the child welfare sector as a whole.

Developing appropriate retention schedules can be challenging. The IPC recommends that the Ministry work together with subject matter experts in the child welfare sector to develop common retention requirements for CASs, and support the sector to comply with these requirements, including through any necessary changes to CPIN.

The IPC recommends that common retention requirements for CASs be developed without delay and that the draft regulation be amended to require CASs to comply with these requirements. However, if the Ministry decides that regulation is not the appropriate vehicle for establishing common retention requirements for CASs, the Ministry should issue a binding directive to CASs under section 42(1) of the *Act*.

In addition to child welfare, the IPC recommends that the Ministry systematically review every sector providing services under the *Act*, and consider whether it requires the development or updating of common retention requirements.

(b) Reference Personal Information that has been "Collected, Used or Disclosed" in Sections 10(2) and 11(6)-(11)

Section 10(2) of the draft regulation prescribes requirements for the retention, transfer and disposal of records of personal information in the custody or control of a service provider that was "collected by the service provider for the purpose of providing a service." The IPC recommends that this section be amended to reference personal information that was collected, used or disclosed by the service provider for the purpose of providing a service.

This would capture personal information that has been collected for another purpose and then used or disclosed for the purpose of providing a service. For example, a service provider may collect personal information to provide a program that does not fall within the specific meaning of a "service" as defined in Part X of the *Act,* and later use that information for providing a service. The regulatory requirements about retention, transfer and disposal

should apply to such a record, and to any other record which is collected, used or disclosed for the purpose of providing a service.

The IPC recommends that section 10(2) be amended as follows:

> Prescribed requirements, s. 309 (1) (b) of the Act
>
> 10. (2) In this section, a reference to a record is a reference to a record that is in the service provider's custody or control and that contains personal information that was collected, used or disclosed by the service provider for the purpose of providing a service.

For the same reason, the IPC recommends that paragraphs 6 to 11 of section 11(1), which prescribe requirements for annual reporting to the IPC, be redrafted to reference personal information that was collected, used or disclosed for the purpose of providing a service, as set out in Appendix A.

6. CLARIFY WHETHER SECTION 10(4) REFERS TO A SUCCESSOR

Section 10(4) of the draft regulation requires that:

> [A] service provider that ceases to provide the service to which a record relates shall not transfer the record to another service provider for the purpose of allowing that service provider to continue to provide that service unless the service provider that will receive the record has in place a records retention policy under this section that addresses the retention of the type of record being transferred.

It is not clear whether this section refers to the transfer of records to a successor, as described under section 310 of the *Act*. If so, the IPC recommends that section 10(4) of the regulation be redrafted to use the term "successor", in order to clearly link the regulation to the requirements in the *Act* regarding the transfer of personal information to successors.

CONCLUSION

The IPC commends the Ministry for the safeguards set out in the proposed regulation in respect of Part X of the *Act*, which will enhance the protections afforded to Ontarians who receive child, youth and family services. The IPC urges the Ministry to amend the regulation in the manner outlined in this submission in order to ensure consistency, transparency and accountability throughout the sector, and to protect Ontarians' access and privacy rights.

We look forward to further consultations and to working together with the Ministry and stakeholders to achieve these ends.

APPENDIX A: DRAFT REGULATION WITH IPC PROPOSED AMENDMENTS

ONTARIO REGULATION

to be made under the

CHILD, YOUTH AND FAMILY SERVICES ACT, 2017

PERSONAL INFORMATION

Prescribed entities, s. 293 of the Act

1. The following entities are prescribed for the purposes of section 293 of the Act:

    1. The Canadian Institute for Health Information.

    2. The Institute of Clinical Evaluative Sciences.

Prescribed requirements and restrictions, ss. 293 (2) and (3) of the Act

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 subsections 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, and

        ii. the service provider and the person or entity have entered into an agreement ~~with respect to~~ addressing the use, security, disclosure, and return or disposal of the 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,

    (a) comply with the conditions or restrictions, if any, that the service provider imposes in the agreement described in subclause ii of paragraph 1 of subsection 2 (1); and

    (b) notify the service provider from whom the information was collected immediately in writing if the person or entity becomes aware of any breach

of section 293 of the Act or the agreement described in subclause ii of paragraph 1 of subsection 2 (1).

Prescribed excluded information, s. 293 (1), (2) and (3) of the Act

3. The following information and corresponding circumstances are prescribed for the purposes of subsection 293 (4) of the Act:

1. Recorded information that documents the content of conversations that took place during a counselling session.

Restrictions on use, s. 293 (9) of the Act

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 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 approved the plan.~~ 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.

(2) A research plan shall be in writing and set out the following information:

1. The affiliation of each person involved in the research.

2. The nature and objectives of the research and the public or scientific benefit of the research that the researcher anticipates.

3. A description of the research proposed to be conducted and the duration of the research.

4. A description of the personal information required and the potential sources.

5. A description of how the personal information will be used in the research and, if it will be linked to other information, a description of the other information as well as how the linkage will be done.

6. An explanation as to why the research cannot reasonably be accomplished without the personal information and, if it is to be linked to other information, an explanation as to why this linkage is required.

7. An explanation as to why consent to the disclosure of the personal information is not being sought from the individuals to whom the information relates.

8. A description of the reasonably foreseeable harms and benefits that may arise from the use of the personal information and how the researchers intend to address those harms.

9. If the research relates primarily to a group of persons who share a characteristic that is a prohibited ground of discrimination under Part I of the Human Rights Code, a description of the views of members or representatives of that group regarding the proposed research.

10. A description of all persons who will have access to the personal information, why their access is necessary, their roles in relation to the research and their related qualifications.

11. The safeguards that the person or entity will impose to protect the confidentiality and security of the personal information, including an estimate of how long information will be retained in an identifiable form and why.

12. Information as to how and when the personal information will be disposed of or returned to the service provider.

13. A description of how the entity or person will, at the earliest reasonable opportunity, notify the service provider from whom the personal information was received of any theft, loss or unauthorized use or disclosure of the personal information.

14. The funding source of the research.

15. Whether the person or entity has applied for the approval of another research ethics board and, if so, the response to or status of the application.

16. Whether the person or entity's interest in the disclosure of the personal information or the performance of the research would likely result in an actual or perceived conflict of interest with other duties of the prescribed entity.

(3) If a prescribed entity has received personal information from a service provider under subsection 293 (1) or (3) of the Act and the personal information is stolen, lost or used or disclosed without authority, the prescribed entity shall notify the service provider at the first reasonable opportunity.

(4) If a person or entity that is not a prescribed entity has received personal information from a service provider under subsection 293 (2) or (3) of the Act and the personal information is stolen, lost or used or disclosed without authority, the person or entity shall notify the service provider at the first reasonable opportunity.

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.~~ 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.

Exception to restriction on disclosure by prescribed entity

6. (1) Despite subsection 293 (9) of the Act, a prescribed entity, or a person or entity that is not a prescribed entity, may disclose personal information disclosed to it under subsection 293 (1), (2) or (3) of the Act to,

(a) another prescribed entity, if the disclosure is for the purposes described in subsection 293 (1) of the Act; or

(b) a researcher who has ~~had a research plan that meets the requirements of subsection 4 (2) approved by a research ethics board that meets the criteria set out in paragraph 1 of subsection 4 (1).~~,

i. met the requirements of paragraphs 2, 3 and 4 of subsection 4 (1);

ii. had a research plan that meets the requirements of subsection 4 (2) approved by a research ethics board that meets the criteria set out in paragraph 1 of subsection 4 (1);

iii. entered into an agreement with the prescribed entity or person or entity that is not a prescribed entity addressing the use, security, disclosure, and return or disposal of the information, in which the researcher agrees to, at minimum,

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

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

C. comply with the conditions and restrictions, if any, that the person or entity imposes with respect to the use, security, disclosure, return or disposal of the information;

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

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

F. 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;

G. notify the person or entity from whom the information was collected immediately in writing if the researcher becomes aware of any breach of the agreement; and

H. notify the person or entity from whom the information was collected at the first reasonable opportunity if personal information that was collected has been stolen, lost or used or disclosed without authority.

(2) If a prescribed entity has received personal information under this section and the personal information is stolen, lost or used or disclosed without authority, the prescribed entity shall notify the person or entity that disclosed the personal information at the first reasonable opportunity.

(3) If a prescribed entity or a person or entity that is not a prescribed entity receives notice that personal information that the person or entity disclosed under this section has been lost, stolen or used or disclosed without authority, the person or entity shall notify the service provider that disclosed the personal information at the first reasonable opportunity.

Applications under ss. 302, 304 and 305 of the Act

7. (1) The Consent and Capacity Board continued under the *Health Care Consent Act, 1996* is prescribed as the body for the purposes of sections 302, 304 and 305 of the Act.

(2) For the purposes of subsections 302 (10), 304 (4), and 305 (10) of the Act, in conducting an application under section 302, 304 or 305 of the Act, respectively, the Consent and Capacity Board shall comply with sections 73 to 79 of the *Health Care Consent Act, 1996*.

Additional requirements, s. 308 (2) of the Act

8. The following additional requirements are prescribed for the purposes of subsection 308 (2) of the Act:

1. The service provider shall notify the individual in plain, easy-to-understand language, and the notification shall include a general description of how the personal information was lost, stolen or used or disclosed without authority.

2. The service provider shall inform the individual of any steps the service provider has taken to,

   i. prevent a similar theft or loss or unauthorized use or disclosure of personal information from recurring, and

   ii. mitigate possible adverse effects on the individual that may be caused by the theft or loss or unauthorized use or disclosure.

3. The service provider shall provide the individual with the contact information of an employee of the service provider who can provide the individual with additional information about the theft or loss or unauthorized use or disclosure.

Prescribed circumstances, s. 308 (3) of the Act

9. Each of the following circumstances is prescribed for the purposes of subsection 308 (3) of the Act:

1. The service provider has reasonable grounds to believe that ~~the~~ personal information in the service provider's custody or control was used or disclosed without authority by a person who knew or ought to have known that the person was using or disclosing the information without authority.

2. The service provider has reasonable grounds to believe that ~~the~~ personal information in the service provider's custody or control was stolen.

3. The service provider has reasonable grounds to believe that ~~the~~ personal information in the service provider's custody or control that was stolen or lost or used or disclosed without authority was or will be further used or disclosed without authority.

4. The loss or unauthorized use or disclosure of the personal information is part of a pattern of similar losses or unauthorized uses or disclosures of personal information in the custody or control of the service provider.

5. The service provider has reasonable grounds to believe that personal information that the service provider disclosed, to a prescribed entity or a person or entity that is not a prescribed entity under subsection 293 (1), (2) or (3) of the Act, has been stolen or lost or used or disclosed without authority by the prescribed entity or the person or entity that is not a prescribed entity.

6. The service provider determines that the loss or unauthorized use or disclosure of ~~the~~ personal information in the service provider's custody or control is significant after considering all relevant circumstances including,

   i. the sensitivity of the personal information that was lost or used or disclosed without authority,

   ii. the volume of the personal information that was lost or used or disclosed without authority,

   iii. the number of persons whose personal information was lost or used or disclosed without authority, and

   iv. whether one or more service providers were involved in the loss or unauthorized use or disclosure of the personal information.

7. An employee of the service provider or any other person acting on behalf of the service provider is terminated, suspended or subjected to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal of personal information by the employee or other person.

8. An employee of the service provider or any other person acting on behalf of the service provider resigns and the service provider has reasonable grounds to believe that the resignation is related to an investigation or other action by the service provider with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of personal information by the employee or other person.

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.

(2) In this section, a reference to a record is a reference to a record that is in the service provider's custody or control and that contains personal information that was collected, used or disclosed by the service provider for the purpose of providing a service.

(3) In disposing of a record a service provider shall,

(a) take reasonable steps to protect the record against theft or loss or unauthorized use or disclosure;

(b) take reasonable steps to ensure that the personal information in the record cannot be reconstructed or retrieved; and

(c) document the record that has been disposed of in a way that does not document any of the personal information contained in the record.

(4) A service provider that ceases to provide the service to which a record relates shall not transfer the record to another service provider for the purpose of allowing that service provider to continue to provide that service unless the service provider that will receive the record has in place a records retention policy under this section that addresses the retention of the type of record being transferred.

(5) A service provider shall develop and maintain a records retention policy in accordance with this section and shall comply with that policy.

(6) The policy shall set out,

(a) each type of record maintained by the service provider and a description of the personal information contained in the record, including the format in which the record is maintained;

(b) the classification of each type of record according to the sensitivity of the personal information contained in the record and the manner in which that personal information is normally used or disclosed by the service provider;

(c) a time period for which each type of record shall be retained by the service provider; and

(d) the method by which the service provider will,

(i) dispose of each type of record in a manner consistent with subsection (3), or

(ii) if the service provider ceases providing the service to which a record relates, store or transfer the record in a manner consistent with subsection (4).

(7) In determining the time periods described in clause (6) (c), a service provider shall consider the following:

1. Whether another service provider also has custody or control of the record or requires the record for the purpose of providing a service.

2. Whether, in the view of the service provider, the record is one to which an individual has a right of access under section 312 of the Act.

3. Whether the record is one which relates to circumstances that are or may be the subject of a possible legal proceeding, other than a legal proceeding described in clause 312 (1) (c) of the Act.

4. Whether the service provider has been informed by the Minister or another service provider that the Minister or service provider may require the information for the purpose set out in paragraph 3 of subsection 283 (1) of the Act or clause 291 (1) (d) of the Act.

5. Any other requirement under the Act or another Act that relates to the amount of time that the record must be retained by the service provider.

(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).

Reporting to Commissioner

11. (1) On or before March 31 in each year, a service provider shall report the following information to the Commissioner:

1. The number of requests for access to a record under subsection 313 (1) of the Act received by the service provider in the previous year.

2. The number of times a service provider, in response to a request made under subsection 313 (1) of the Act in the previous year, refused to provide access to a record or part of a record and the number of times the service provider relied on each of the clauses or, in the case of a refusal under clause 312 (1) (d) of the Act, each of the subclauses, under subsection 312 (1) of the Act to do so.

3. The number of times the service provider responded within 30 days of receiving a request for access to a record under subsection 313 (1) of the Act and the number of times the service provider extended the deadline to respond to such a request to not more than 90 days under subsection 314 (3) of the Act.

4. The number of requests to correct a record made to a service provider under subsection 315 (2) of the Act in the previous year and the number of times a service provider, in response to such a request,

    i. refused the request because it did not find that the correction was warranted under subsection 315 (9) of the Act,

ii. relied on each of either subsection 315 (6) or (10) of the Act to refuse the request, or

iii. received a statement of disagreement under subsection 315 (12) of the Act.

5. The number of times the service provider responded within 30 days of receiving a request to correct a record under subsection 315 (2) of the Act and the number of times the service provider extended the deadline to respond to such a request to not more than 90 days under subsection 315 (4) of the Act.

6. The number of times personal information in the service provider's custody or control that was collected, used or disclosed for the purpose of providing a service was stolen.

7. The number of times personal information in the service provider's custody or control that was collected, used or disclosed for the purpose of providing a service was lost.

8. The number of times personal information in the service provider's custody or control that was collected, used or disclosed for the purpose of providing a service was used without authority.

9. The number of times personal information in the service provider's custody or control that was collected, used or disclosed for the purpose of providing a service was disclosed without authority.

10. The number of times personal information in the service provider's custody or control that was collected, used or disclosed for the purpose of providing a service was used in a manner that is outside the scope of the service provider's description of its information practices under clause 311 (1) (a) of the Act.

11. The number of times personal information in the service provider's custody or control that was collected, used or disclosed for the purpose of providing a service was disclosed in a manner that is outside the scope of the service provider's description of its information practices under clause 311 (1) (a) of the Act.

(2) The report required by subsection (1) shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner.

Notice by service provider to individual

12. If a service provider receives notice under subsection 4 (3), 4 (4) or 6 (3) that personal information it disclosed to a prescribed entity or a person or entity that is not a prescribed

entity under subsection 293 (1), (2) or (3) of the Act has been stolen, lost or used or disclosed without authority, the service provider shall,

(a) notify the individual to whom the information relates at the first reasonable opportunity of the theft, loss or unauthorized use or disclosure; and

(b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under section 316 of the Act.

Commencement

13. [commencement].