June 2024

Child, Youth and Family Services Act Addendum to the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities

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

Contents

Process for the Review and Approval of Prescribed Entities

Amendments to the **Child, Youth and Family Services Act** (CYFSA), which came into force on January 1, 2020, permit service providers to disclose personal information to prescribed entities for the purposes of analysis or compiling statistical information related to planning, evaluation, monitoring, or management of services or the allocation of resources for those services, including their delivery, pursuant to section 293 of the CYFSA and its regulations. The entities prescribed for the purpose of section 293 of the CYFSA are set out in section 1 of Regulation 191/18 to the CYFSA (the "regulations").

These disclosures are permitted provided that the prescribed entities comply with the requirements set out in the CYFSA and its regulations as well as in any other regulation(s) that may be enacted under CYFSA.

Requirements for Disclosure to Prescribed Entities

In order for service providers to be permitted to disclose personal information to a prescribed entity under section 293 of the CYFSA, the prescribed entity must have in place practices and procedures ("policies, procedures, and practices") approved by the Information and Privacy Commissioner of Ontario ("IPC") to protect the privacy of individuals whose personal information it receives and to maintain the confidentiality of that information. This requirement is set out in section 293(5) of the CYFSA.

These practices and procedures must also be reviewed by the IPC every three years from the date of their initial approval in order for service providers to be able to continue to disclose personal information to a prescribed entity, and in order for the prescribed entity to be able to continue to collect, use, and disclose personal information as permitted by the CYFSA and its regulations. This requirement is set out in section 293(7) of the CYFSA.

The PHIPA Manual

The entities prescribed under the CYFSA are entities that are also prescribed under the ***Personal Health Information Protection Act*** (PHIPA). The ***Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*** (the "PHIPA Manual") outlines the process followed by the IPC in reviewing the practices and procedures implemented by prescribed persons ("PPs") and prescribed entities ("PEs") under PHIPA. These practices and procedures are implemented to protect the privacy of individuals whose personal health information the PPs and PEs receive and to maintain the confidentiality of that information. The PHIPA Manual also sets out the requirements that are reasonably necessary to protect the personal health information ("PHI") that PPs and PEs are permitted to collect and to assist PPs and PEs in complying with their obligations under PHIPA and its regulations.

Purpose of this CYFSA Addendum

This document is an addendum to the PHIPA Manual (the "CYFSA Addendum"). It sets out the requirements that apply to entities prescribed under the CYFSA that are different or

supplemental to the requirements set out in the PHIPA Manual. It also outlines the process that will be followed by the IPC in reviewing the practices and procedures implemented by such prescribed entities to protect the privacy of individuals whose personal information they receive under the CYFSA and to maintain the confidentiality of that information.

While this document draws on the content and requirements set out in the PHIPA Manual, its requirements and process for the review and approval of prescribed entities under the CYFSA are separate from the review and approval of prescribed entities under PHIPA. The CYFSA Addendum does not govern the practices and procedures implemented by prescribed entities when collecting, using, or disclosing personal health information under PHIPA.

Every three years, prescribed entities must demonstrate compliance with the requirements in the CYFSA Addendum in order to receive approval from the IPC to continue operating under their prescribed status. This is referred to in this Addendum as the "**three-year reviews**."

Please note, throughout the Addendum, 'must' indicates a requirement and 'should' indicates a recommendation. The CYFSA Addendum may be amended from time to time by the IPC. It is the responsibility of the prescribed entities to ensure continued compliance with it as amended.

Note that this CYFSA Addendum is not intended for use by any entity that might be prescribed under the CYFSA that is not also an entity prescribed under PHIPA.

Other Manuals and Addenda

Under PHIPA, a prescribed organization is responsible for developing and maintaining the electronic health record (EHR). The EHR is the electronic systems developed and maintained by the prescribed organization to enable custodians to collect, use, and disclose PHI. Like PPs and PEs under PHIPA, prescribed organizations must have their practices and procedures reviewed by the IPC every three years. The IPC maintains a separate ***Manual for the Review and Approval of Prescribed Organizations*** that sets out the requirements for review and approval of prescribed organizations.

Under the ***Coroners Act***, PEs named under that Act may collect personal information without individuals' consent from the Chief Coroner and use it for the purpose of research, analysis, or the compilation of statistics related to the health or safety of the public, or any segment of the public. Like PPs and PEs under PHIPA, PEs under the *Coroners Act* must have their practices and procedures reviewed by the IPC every three years. The IPC maintains ***The Coroners Act Addendum to the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*** that sets out the requirements for review and approval of PEs under the *Coroners Act*.

PPs, PEs, and prescribed organizations under PHIPA, as well as prescribed entities under the CYFSA and *Coroners Act* are each responsible for determining the manual(s) and addenda that apply to their specific organization, and for developing and implementing policies, procedures, and practices that comply with the requirements of all applicable legislation.

Review Process for Prescribed Entities

Each prescribed entity is required to have in place practices and procedures to protect the privacy of individuals whose personal information it receives under the CYFSA and to maintain the confidentiality of that information. At a minimum, these practices and procedures must include the:

- the policies, procedures, practices, agreements and other documentation set out in **Appendix "A"**
- contain the minimum content set out in **Appendix "B"** of the Addendum

The policies, procedures, and practices set out in **Appendix "A"** are based on an assessment of what would constitute a reasonable combination of practices and procedures given the:

- nature of the functions performed by the prescribed entities
- amount and sensitivity of the personal information collected
- number and roles of the individuals with access to the personal information
- obligations and duties of the prescribed entities under the CYFSA and its regulations

The process to be followed by the IPC in conducting its review will depend on whether the review relates to the **initial review** of the policies, procedures, and practices implemented by the prescribed entity or relates to the **ongoing review** of these policies, procedures, and practices, which is conducted every three years from the date of the initial approval.

Initial CYFSA Review of the Prescribed Entities

Each prescribed entity seeking the initial approval of the IPC under the CYFSA in respect of the practices and procedures implemented to protect the privacy of individuals whose personal information it receives and to maintain the confidentiality of that information, must submit the following to the IPC:

- The policies, procedures, and practices described in Appendix "A" and containing the minimum content set out in "Part 1 – Privacy Documentation" of Appendix "B" to the *CYFSA* Addendum.
- An initial sworn affidavit in the form set out in **Appendix "D"** regarding the policies, procedures, and practices required under "Part 2 – Additional Requirements" of Appendix "B" to the CYFSA Addendum.
- The sworn affidavit must be executed by the Chief Executive Officer or the Executive Director (or equivalent position), as the case may be, who is ultimately accountable for ensuring that the policies, procedures, and practices of the prescribed entity comply with the CYFSA and its regulations, as elaborated by the requirements in Part 2 of Appendices "A" and "B" of the CYFSA Addendum, and has taken steps that are reasonable in the circumstances to ensure that these policies, procedures, and practices are implemented.

- A random selection specified by the IPC of the policies, procedures, and practices required under "Part 2 – Additional Requirements" of **Appendix "B"** to the CYFSA Addendum.

These policies, procedures, and practices, and sworn affidavit must be submitted at least six months prior to the date that the approval of the IPC is requested.

Statements of Requested Exceptions

If there is, or is expected to be, a divergence between the policies, procedures, and practices of the prescribed entity and the requirements in **Appendix "A"** or **Appendix "B"** of the CYFSA Addendum, the prescribed entity must provide a written **Statement of Requested Exceptions** at the same time they submit their policies, procedures, and practices to the IPC. The Statement of Requested Exceptions must identify each requirement of the CYFSA Addendum from which the prescribed entities policies, procedures, and practices will, or currently, diverge, together with a rationale.

Further, for each requirement identified, the Statement of Requested Exceptions must either provide:

- a detailed plan and timeline for achieving compliance with the requirement or
- an explanation for why an exception to the requirement in the CYFSA Addendum should be granted by the IPC and how the prescribed entity has achieved, or will achieve, an equivalent standard to protect the privacy of the individuals whose personal information it receives and maintain the confidentiality of the information (where a prescribed entity has not yet achieved an equivalent standard, it must provide a detailed plan and timeline for achieving the equivalent standard)

Statements of Inapplicability

Where one or more of the requirements in **Appendix "A"** or **Appendix "B"** is inapplicable to a prescribed entity, the prescribed entity need not submit a **Statement of Requested Exceptions**, but must instead provide a written **Statement of Inapplicability** at the same time that they submit their policies, procedures, and practices to the IPC. The Statement of Inapplicability must identify each requirement that is inapplicable (if any), together with a rationale.

IPC Review of Submitted Materials

The IPC will consider each **Statement of Requested Exceptions** and each **Statement of Inapplicability** on a case-by-case basis. In its sole discretion, the IPC will determine whether and the extent to which the Statement of Requested Exceptions (or Statement of Inapplicability, as the case may be) should be approved and any conditions attached thereto.

Upon receipt, the IPC will review the policies, procedures, and practices implemented by the prescribed entity, along with any Statements of Requested Exceptions and Statements of Inapplicability submitted and will request any additional documentation and clarifications that it deems necessary.

On-Site Meeting

Once any additional documentation and necessary clarifications are received, an on-site meeting will be scheduled between the IPC and representatives of the prescribed entity. The purpose of the on-site meeting is to:

- discuss the policies, procedures, and practices implemented by the prescribed entity
- provide the IPC with an opportunity to ask questions arising from the review of the policies, procedures, and practices implemented
- provide the IPC with an opportunity to review the physical security measures put in place to protect personal information

Approval Process

Following the on-site meeting:

- The prescribed entity will be informed of any actions it is required to take prior to the approval of its policies, procedures and practices.
- Once all necessary actions have been taken, the IPC will prepare and provide to the prescribed entity a draft report for review and comment.
- The report, letter of approval, and any approved Statements of Requested Exceptions and Statements of Inapplicability will be finalized.
- The finalized report will be posted on the IPC's website, along with a letter of approval, and any approved Statements of Requested Exceptions and Statements of Inapplicability.
- The prescribed entity should also have a statement on its website informing the public that this documentation is publicly available on the IPC's website and should provide a link to the IPC's website where the prescribed entities documentation is made available.

Amending or Withdrawing Statements of Requested Exceptions or Statements of Inapplicability

Over the course of the review period, a Statement of Requested Exceptions or Statement of Inapplicability may no longer be relevant, accurate, or up to date. In such circumstances, the prescribed entity must inform the IPC as soon as reasonably possible and resubmit a corrected version (no later than two months prior to the required approval date).

Similarly, a prescribed entity may request to withdraw a Statement of Requested Exceptions or Statement of Inapplicability if it was submitted in error, or if it is no longer necessary. In either circumstance, the prescribed entity must inform the IPC as soon as reasonably possible (no later than two months prior to the required approval date) and must provide the IPC with a detailed explanation for how compliance with the requirements in **Appendix "A"** or **Appendix "B"** has since been achieved.

Approval Letter

The IPC's decision whether to approve the practices and procedures of a prescribed entity, and any Statements of Requested Exceptions or Statements of Inapplicability, will be issued in a letter, and may include recommendations for further improvements to the policies, procedures, and practices of the prescribed entity. The IPC will track all recommendations to ensure that the prescribed entity has implemented the recommendations within the timeframe specified by the IPC or, in any case, no later than the start of the next review period (being one year plus three months prior to the date the next approval by the IPC is required).

A person or entity may not operate as a prescribed entity, unless it has submitted its practices and procedures to the IPC, and the IPC has reviewed and approved these practices and procedures and has issued a letter and accompanying report to this effect, unless otherwise specified in legislation.

In Case of No Approval

If, on the date that approval is requested or required pursuant to the CYFSA and its regulations, the practices and procedures of the prescribed entity continue to represent a significant divergence from the requirements set out in the CYFSA Addendum and the divergence is not the subject of an approved **Statement of Requested Exceptions** (described above), the IPC will not approve the practices and procedures of the prescribed entity. Generally, the IPC will endeavour to notify the prescribed entity of the possibility of this outcome at least 30 days prior to the requested or required approval date, citing the significant divergence(s) that remain outstanding, but this notice may not always be possible in the circumstances. The prescribed entity will have up to 30 days to remedy the significant divergence(s), or to put forward a detailed plan and timeline for doing so. Based on the prescribed entity's response and demonstrated assurances, the IPC may, in its sole discretion, approve the practices and procedures of the prescribed entity.

In the case where the practices and procedures of a prescribed entity are not approved on the date of requested or required approval, the IPC will inform the prescribed entity in writing of the reasons why approval was not granted, including the significant divergence(s) that must be addressed by the prescribed entity prior to obtaining approval. The prescribed entity may resubmit its policies, procedures, and practices and any other requested documentation for approval by the IPC, as described in the IPC's letter. Once the significant divergence(s) have been adequately addressed, approval will be provided to operate as a prescribed entity. To prevent undue delay in operating as a prescribed entity, this approval may be provided in the intervening time period between typical three-year review periods.

Three-Year Review of Prescribed Entities

Preliminary Information to be Submitted

One year plus three months prior to the date that the continued approval is required pursuant to the CYFSA and its regulations, each prescribed entity seeking the continued approval of its policies, procedures, and practices must submit its Privacy, Information Security, Human Resources, and Organizational indicators as set out in **Appendix "C"** of the CYFSA Addendum

(the "indicators"). Typically, approval is provided by October 31 of the required approval year. Therefore, in typical circumstances, the prescribed entity will submit its indicators to the IPC on August 1 of the year prior to the required approval year.

Such indicators must be attached as an exhibit to the three-year review sworn affidavit the template of which is set out in **Appendix "E"** of the CYFSA Addendum.

The sworn affidavit must be executed by the Chief Executive Officer or the Executive Director (or equivalent position), as the case may be, who is ultimately accountable for ensuring that the policies, procedures, and practices of the prescribed entity comply with the CYFSA and its regulations, as elaborated by the requirements in Appendices **"A"** and **"B"** of the CYFSA Addendum, and has taken steps that are reasonable in the circumstances to ensure that these policies, procedures, and practices are implemented.

The IPC may request that the sworn affidavit be re-submitted during the IPC's three-year review, including where the previously submitted affidavit does not comply with the requirements of **Appendix "E"**, or the exhibits to that affidavit do not comply with the requirements of the CYFSA Addendum, or where the three-year review sworn affidavit is otherwise no longer accurate.

Statements of Requested Exceptions

If there is, has been (since the last review by the IPC), or is expected to be, a divergence between the policies, procedures, and practices of the prescribed entity and the requirements in **Appendix "A"** or **Appendix "B"** of the CYFSA Addendum, the prescribed entity must submit a written **Statement of Requested Exceptions** to the IPC, attached as an exhibit to the sworn affidavit, identifying each requirement of the CYFSA Addendum from which the prescribed entity's policies, procedures, and practices have diverged, currently diverge, or will diverge, together with a rationale.

Further, for each requirement identified, the Statement of Requested Exceptions must either provide:

- a detailed plan and timeline for achieving compliance with the requirement (or explaining how compliance has been achieved) or
- an explanation for why an exception to the requirement in the CYFSA Addendum should be granted by the IPC and how the prescribed entity has achieved, or will achieve, an equivalent standard to protect the privacy of the individuals whose personal information it receives and maintain the confidentiality of the information (where a prescribed entity has not yet achieved an equivalent standard, it must provide a detailed plan and timeline for achieving this equivalent standard)

Statements of Inapplicability

Where one or more of the requirements in **Appendix "A"** or **Appendix "B"** is inapplicable to a prescribed entity, the prescribed entity need not submit a **Statement of Requested Exceptions**, but must instead provide the IPC with a **Statement of Inapplicability** attached as an exhibit

to the sworn affidavit. The Statement of Inapplicability must identify each requirement that is inapplicable (if any), together with a rationale.

IPC Review of Submitted Materials

The IPC will consider each **Statement of Requested Exceptions** and **Statement of Inapplicability** on a case-by-case basis. In its sole discretion, the IPC will determine whether and the extent to which the Statement of Requested Exceptions (or Statement of Inapplicability, as the case may be) should be approved and any conditions attached thereto.

Upon receipt, the IPC will review the indicators submitted by the prescribed entity, along with any Statements of Requested Exceptions and Statements of Inapplicability submitted and will request any additional documentation and clarifications it deems necessary.

Selection of Policies, Procedures and Practices

Based on its review of the preliminary information submitted by the prescribed entity as set out above, the IPC will determine the scope of the policies, procedures, and practices of the prescribed entity that will be the priority focus of the IPC's review that year. The policies, procedures, and practices will be selected from the policies, procedures, and practices referred to in the CYFSA Addendum. The scope of the policies, procedures, and practices selected by the IPC for review may vary from one prescribed entity to the next and will be determined, in the IPC's sole discretion, based on an individualized assessment of privacy and information security risks. In determining the scope of this risk-based review, the IPC will take into consideration any factors the IPC considers relevant, including:

- whether there have been any changes to the prescribed entity's policies, procedures, and practices since the last review by the IPC
- privacy and information security issues (including recommendations) identified during previous reviews of the prescribed entity
- whether the policies, procedures, and practices have been recently reviewed by the IPC in following up on the status of recommendations made during the last review
- privacy and information security issues, including any privacy or **information security breaches**, identified through ongoing, current, or previous IPC consultations with the prescribed entity
- results of privacy and information security audits conducted by the prescribed entity since the last review
- recent decisions, guidelines, fact sheets, etc. issued by the IPC or other relevant oversight offices
- privacy and information security trends emerging from complaints and privacy and **information security breaches** reported to the IPC
- privacy and information security trends identified through the IPC's environmental scanning function
- privacy and information security issues recently reported in the media more generally

- privacy and information security issues identified in a Statement of Requested Exceptions or a Statement of Inapplicability
- changes in requirements arising from new or amended laws or regulations
- evolving industry privacy and information security standards and best practices
- any other information the IPC and the prescribed entity may consider relevant and important for the purposes of the review

On a date that is no later than one year plus one month prior to the date that continued approval is required pursuant to the CYFSA and its regulations, the IPC will provide each prescribed entity notice of which of its policies, procedures, and practices it will initially be required to submit to the IPC for review.

Typically, approval is provided on October 31 of the required approval year. Therefore, in typical circumstances, the IPC will provide notice to each prescribed entity of which of its policies, procedures, and practices will initially be the primary focus of that review no later than September 30 of the year prior to the required approval year.

In its sole discretion, the IPC may expand the scope of its review at any time during the review period to include other policies, procedures, and practices that are the subject of the IPC's review under subsection 293(5) and 293(7) of the CYFSA, depending on the level of privacy and information security risks revealed in the information and documentation provided by the prescribed entity.

Review of Selected Policies, Procedures and Practices

The prescribed entity must submit the selected policies, procedures, and practices to the IPC no later than one month from the date that the IPC informs the prescribed entity of its selection.

The IPC will review the selected policies, procedures, and practices. The IPC will assess whether the prescribed entity's policies, procedures, and practices protect the privacy of individuals whose personal information the prescribed entity receives and maintain the confidentiality of that information, and whether the prescribed entity is adhering to these policies, procedures, and practices. At a minimum, the IPC will assess whether the selected policies, procedures, and practices sufficiently address the content set out in **Appendix "B"** to the CYFSA Addendum.

Approval Process

Following its review of the selected policies, procedures, and practices submitted, the IPC will decide, in its sole discretion, whether further examination is required of the prescribed entity prior to the continued approval of its policies, procedures and practices.

Further examination may include one or more of the following:

- a detailed review by the IPC of additional policies, procedures, and practices of the prescribed entity
- requests for further details or clarifications regarding the submitted indicators, as may be necessary to assess compliance with the requirements set out in the CYFSA Addendum

- a request for further documentation from the prescribed entity with respect to one or more of its policies, procedures, and practices
- interviews with relevant personnel of the prescribed entity
- a request for further supporting evidence demonstrating how the prescribed entity is implementing or complying with its practices or procedures, or results of recent assessments or audits
- a request to meet with representatives of the prescribed entity to discuss the implementation of, and compliance with, its policies, procedures, and practices
- an on-site visit at the premises of the prescribed entity to further assess implementation of, and compliance with, its policies, procedures, and practices
- an assessment of any other aspect of the prescribed entity deemed relevant and appropriate in the sole discretion of the IPC

Based on its assessment, the IPC will inform the prescribed entity of any further action(s) it is required to take prior to receiving continued approval of its practices and procedures. Such further action(s) may include requiring the prescribed entity to:

- amend or provide additional detail in a Statement of Requested Exceptions or Statement of Inapplicability
- develop and implement one or more additional policies, procedures, and practices
- amend, implement or adhere to one or more of its existing policies, procedures, and practices or
- remediate any deficiencies and bring it into compliance with the requirements set out in the CYFSA Addendum

The prescribed entity must comply with such further action(s) as required by the IPC in order to obtain continued approval of its policies, procedures and practices.

Amending or Withdrawing Statements of Requested Exceptions or Statements of Inapplicability

Over the course of the review period, a Statement of Requested Exceptions or Statement of Inapplicability may no longer be relevant, accurate, or up to date. In such circumstances, the prescribed entity must inform the IPC as soon as reasonably possible and resubmit a corrected version (no later than two months prior to the required approval date).

Similarly, a prescribed entity may request to withdraw a Statement of Requested Exceptions or Statement of Inapplicability if it was submitted in error or if it is no longer necessary. In either circumstance, the prescribed entity must inform the IPC, as soon as reasonably possible (no later than two months prior to the required approval date), and must provide the IPC with a detailed explanation for how compliance with the requirements in **Appendix "A"** or **Appendix "B"** has since been achieved.

Approval Letter

If, on the date that the continued approval is required pursuant to the CYFSA and its regulations, the policies, procedures, and practices of the prescribed entity comply with the requirements set out in the CYFSA Addendum to the satisfaction of the IPC, and any divergence identified in a **Statement of Requested Exceptions** has been approved, the IPC may, in its sole discretion, approve the practices and procedures of the prescribed entity for a further three-year period.

The IPC's decision whether to approve the practices and procedures of a prescribed entity, and any Statements of Requested Exceptions or Statements of Inapplicability, will be issued in a letter, and may include recommendations for further improvements to the policies, procedures, and practices of the prescribed entity. The IPC will track all recommendations to ensure that the prescribed entity has implemented the recommendations within the timeframe specified by the IPC or, in any case, no later than the start of the next review period (being one year plus three months prior to the date that the next approval by the IPC is required).

A person or entity may not continue to operate as a prescribed entity more than three years after the date of its prior approval unless the IPC has advised the prescribed entity, in writing, that its policies, procedures, and practices have been approved.

In Case of No Approval

If, on the date that the continued approval is required pursuant to the CYFSA and its regulations, the practices and procedures of the prescribed entity continue to represent a significant divergence from the requirements set out in the CYFSA Addendum and the divergence is not the subject of an approved **Statement of Requested Exceptions** (described above), the IPC will not approve the practices and procedures of the prescribed entity for a further three-year period. Generally, the IPC will endeavour to notify the prescribed entity of the possibility of this outcome at least 30 days prior to the required approval date, citing the significant divergence(s) that remain outstanding. The prescribed entity will have up to 30 days to remedy the significant divergence(s) or to put forward a detailed plan and timeline for doing so. Based on the prescribed entity's response and demonstrated assurances, the IPC may, in its sole discretion, approve the practices and procedures of the prescribed entity for a further three-year period on the date that continued approval is required pursuant to the CYFSA and its regulations.

In the case where the practices and procedures of a prescribed entity are not approved for a further three-year period on the date that continued approval is required pursuant to the CYFSA and its regulations, the IPC will inform the prescribed entity in writing of the reasons why approval was not granted, including the significant divergence(s) that must be addressed by the prescribed entity prior to regaining approval. The prescribed entity may resubmit its policies, procedures, and practices and any other requested documentation for approval by the IPC, as described in the IPC's letter. Once the significant divergence(s) have been adequately addressed, approval will be provided to resume operating as a prescribed entity. To prevent undue delay in resumption of prescribed entity activities, this approval may be provided in the intervening time period between typical three-year review periods.

Publication of Three-Year Review Documentation

The letter, indicators, sworn affidavit submitted by the prescribed entity, along with any approved **Statements of Requested Exceptions** and **Statements of Inapplicability** will be made publicly available on the IPC's website at **www.ipc.on.ca**.

Prescribed entities should also have a statement on their respective public-facing websites that informs the public that this documentation is publicly available on the IPC's website and should provide a link to the IPC's website where the prescribed entity's documentation is made available.

In Case of Confidential Content

Where the indicators submitted to the IPC, a **Statement of Requested Exceptions**, or a **Statement of Inapplicability** approved by the IPC contain specific information that the prescribed entity claims is confidential, the prescribed entity may request that the IPC not publish this specific information on its website. Such a request must be provided at least two months prior to the date of required approval. As part of its request, the prescribed entity must:

- identify the specific information it believes should not be published
- provide a rationale for why this information is confidential and should not be published
- provide a draft copy of the indicators, Statement of Requested Exceptions, or Statement of Inapplicability, redacting the precise information it claims to be confidential, and suggesting alternative language for publication that provides as much transparency and accountability as possible in the circumstances

The IPC will consider, on a case-by-case basis, whether to grant this request and may request additional information from the prescribed entity to support its claim of confidentiality. The IPC may approve or deny, in its sole discretion, the proposed redaction(s), as well as the proposed alternate language.

Overview of the CYFSA Addendum

A prescribed entity must have the necessary policies, procedures, and practices in place to ensure compliance with **Appendix "B"** of the CYFSA Addendum, whether those policies, procedures, and practices are separate from or integrated with the prescribed entity's policies, procedures, and practices developed under the PHIPA Manual.

Reviews under other Acts

Where a prescribed entity is subject to three-year reviews under different statutes, the reviews will be combined and conducted by a single review team at the IPC, if possible. The prescribed entity must also identify a single review team that will work on the three-year reviews under all statutes.

Appendix A: List of Required Policies, Procedures, and Practices

Part 1 – Privacy Policies, Procedures, and Practices

Categories	Required Policies, Procedures, and Practices	Page No. Appendix B
General Privacy Policies, Procedures, and Practices	1. *Privacy Policy in Respect of its Status as a Prescribed Entity*	16
	2. *Policy, Procedures, and Practices for Ongoing Review of Privacy Policies, Procedures, and Practices*	19
Transparency	3. *Policy on the Transparency of Privacy Policies, Procedures, and Practices*	21
Collection of Personal Information and Data Holdings	4. *Policy, Procedures, and Practices for the Collection of Personal Information*	23
	5. *Policy, Procedures, and Practices for the Segregation of Personal Information*	25
	6. *List of Data Holdings Containing Personal Information*	26
	7. *Policy, Procedures, and Practices for Statements of Purpose for Data Holdings Containing Personal Information*	26
	8. *Statements of Purpose for Data Holdings Containing Personal Information*	27
Access and Use of Personal Information	9. *Policy, Procedures, and Practices for Limiting Agent Access to and Use of Personal Information*	27
	10. *Log of Agents Granted Approval to Access and Use Personal Information*	31
	11. *Policy, Procedures, and Practices for the Use of Personal Information for Research*	31
	12. *Log of Approved Uses of Personal Information for Research*	37
Disclosure of Personal Information for Research	13. *Policy, Procedures, and Practices for Disclosure of Personal Information for Research Purposes and the Execution of Research Agreements*	38
	14. *Template Research Agreement*	42
	15. *Log of Research Agreements*	48

Categories	Required Policies, Procedures, and Practices	Page No. Appendix B
Disclosure of Personal Information for Purposes Other Than Research	16. ***Policy, Procedures, and Practices for Disclosure of Personal Information for Purposes Other Than Research***	49
	17. ***Policy, Procedures, and Practices for the Execution of Data Sharing Agreements***	53
	18. ***Template Data Sharing Agreement***	54
	19. ***Log of Data Sharing Agreements***	59
Third Party Service Provider Agreements	20. ***Policy, Procedures, and Practices for Executing Agreements with Third Party Service Providers in Respect of Personal Information***	59
	21. ***Template Agreement for Third Party Service Providers***	63
	22. ***Log of Agreements with Third Party Service Providers***	69
Data Linkage, De-Identification and Aggregation	23. ***Policy, Procedures, and Practices for the Linkage of Records of Personal Information***	70
	24. ***Log of Approved Linkages of Records of Personal Information***	72
	25. ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***	73
Privacy Impact Assessments	26. ***Policy, Procedures, and Practices for Privacy Impact Assessments***	75
	27. ***Log of Privacy Impact Assessments***	78
Privacy Audit Program	28. ***Policy, Procedures, and Practices in Respect of Privacy Audits***	79
	29. ***Log of Privacy Audits***	81
Privacy Breaches	30. ***Policy, Procedures, and Practices for Privacy Breach Management***	81
	31. ***Log of Privacy Breaches***	88
Privacy Complaints and Inquiries	32. ***Policy, Procedures, and Practices for Privacy Complaints***	89
	33. ***Log of Privacy Complaints***	93
	34. ***Policy, Procedures, and Practices for Privacy Inquiries***	94

Part 2 - Additional Requirements

For the list of required documentation under Part 2, see parts 2, 3, and 4 of Appendix "A" of the *PHIPA* Manual.

Appendix B: Minimum Content of Required Policies, Procedures, and Practices

Part 1 – Privacy Policies, Procedures, and Practices

General Privacy Policies, Procedures, and Practices

1. Privacy Policy in Respect of its Status as a Prescribed Entity

Status under the *Child, Youth and Family Services Act* (CYFSA)

The privacy policy in respect of its status as a prescribed entity ("Privacy Policy") must describe the status of the prescribed entity under the CYFSA and the duties and responsibilities that arise as a result of this status. In particular, the Privacy Policy must indicate that the prescribed entity has implemented policies, procedures, and practices to protect the privacy of individuals whose personal information it receives and to maintain the confidentiality of that information, and that these policies, procedures, and practices are subject to review by the IPC every three years.

The Privacy Policy must also articulate a commitment by the prescribed entity to comply with the provisions of the CYFSA and its regulations applicable to prescribed entities, as the case may be.

Privacy and Information Security Accountability Framework

The Privacy Policy must also describe the accountability framework for ensuring compliance with the CYFSA and its regulations and for ensuring compliance with the privacy and information security policies, procedures, and practices implemented by the prescribed entity.

In particular, the Privacy Policy must:

- indicate that the Chief Executive Officer or the Executive Director (or equivalent position), as the case may be, is ultimately accountable for ensuring compliance with:
    - the CYFSA and its regulations
    - the privacy and information security policies, procedures, and practices implemented
- identify the position(s) that have been delegated day-to-day authority to manage the privacy program and the information security program including:
    - to whom these positions report
    - their duties and responsibilities to manage the privacy program and the information security program
    - some of the key activities in respect of these programs

The Privacy Policy should also identify other positions or committees that support the privacy program and/or the information security program and their role in respect of these programs.

Collection of Personal Information

The Privacy Policy must:

- identify the:
    - purposes for which personal information is collected
    - types of personal information collected
    - the service providers and any other persons or organizations from which personal information is typically collected
- ensure that each purpose for which personal information is collected, identified in the Privacy Policy, and is consistent with the collections of personal information permitted by the CYFSA and its regulations
- articulate a commitment by the prescribed entity not to collect personal information if other information will serve the purpose and not to collect more personal information than is reasonably necessary to meet the purpose
- outline the policies, procedures, and practices implemented by the prescribed entity to ensure that both the amount and the type of personal information collected is limited to that which is reasonably necessary for its purpose
- contain a list of the data holdings of personal information maintained by the prescribed entity
- identify where an individual may obtain further information in relation to the purposes, elements and sources of each data holding of personal information

Use of Personal Information

The Privacy Policy must identify the purposes for which the prescribed entity uses personal information. In identifying these purposes, the Privacy Policy must:

- clearly distinguish between the use of personal information and the use of **de-identified and/or aggregate information**
- distinguish between the use of personal information for purposes of data analysis or the compilation of statistical information, and the use of personal information for research purposes under section 4 of O. Reg 191/18
- ensure that each use of personal information identified in the Privacy Policy is consistent with the specific uses of personal information permitted by the CYFSA and its regulations
- articulate a commitment by the prescribed entity not to use personal information if other information will serve the purpose and not to use more personal information than is reasonably necessary to meet the purpose
- identify some of the policies, procedures, and practices implemented by the prescribed entity to fulfill these data minimization requirements, including limits on the use of personal information by agents

The Privacy Policy must also state that the prescribed entity remains responsible for personal information used by its agents and identify the policies, procedures, and practices implemented to ensure that its agents only collect, use, disclose, retain and dispose of personal information in compliance with the CYFSA and its regulations and in compliance with the privacy and information security policies, procedures and practices.

Disclosure of Personal Information

The Privacy Policy of the prescribed entity must:

- identify specific purposes for which and the circumstances in which personal information is disclosed, to whom such disclosures are typically made and the statutory or other requirements that must be satisfied prior to such disclosures
- ensure that each disclosure identified in the Privacy Policy is consistent with the disclosures of personal information permitted by the CYFSA and its regulations
- clearly distinguish between the purposes for which and the circumstances in which personal information is disclosed and those where **de-identified and/or aggregate information** is disclosed
- indicate that the prescribed entity will review all **de-identified and/or aggregate information** prior to its disclosure to ensure that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual
- articulate a commitment by the prescribed entity not to disclose personal information if other information will serve the purpose and not to disclose more personal information than is reasonably necessary to meet the purpose
- identify some of the policies, procedures, and practices implemented by the prescribed entity to fulfill these data minimization requirements

Secure Retention, Transfer and Disposal of Records of Personal Information

The Privacy Policy must address the secure retention of records of personal information in both paper and electronic format, including:

- how long records of personal information are retained
- whether the records are retained in identifiable form
- the secure manner in which they are retained
- the manner in which records of personal information in both paper and electronic format will be securely transferred and disposed of

Implementation of Administrative, Technical and Physical Safeguards

The Privacy Policy must outline some of the administrative, technical, and physical safeguards implemented to protect the privacy of individuals whose personal information is received and to maintain the confidentiality of that information, including the steps taken to protect personal

information against theft, loss and unauthorized collection, use, or disclosure, and to protect records of personal information against unauthorized copying, modification or disposal.

Inquiries, Concerns or Complaints Related to Information Practices

The Privacy Policy must identify to whom, and how, individuals may direct inquiries, concerns, or complaints related to the privacy policies, procedures, and practices of the prescribed entity, or related to the compliance of the prescribed entity with the CYFSA and its regulations.

Specifically, the Privacy Policy must:

- include the name and/or title, mailing address, and contact information for the agent(s) to whom inquiries, concerns or complaints may be directed
- describe the manner and format in which these inquiries, concerns, or complaints may be made
- clarify that individuals may direct complaints regarding the compliance of the prescribed entity with section 293 of the CYFSA and its regulations to the IPC and provide the mailing address and contact information for the IPC
- identify where individuals may obtain further information in relation to the privacy policies, procedures, and practices of the prescribed entity

Compliance, Audit and Enforcement

The Privacy Policy must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

2. Policy, Procedures, and Practices for Ongoing Review of Privacy Policies, Procedures, and Practices

A policy, procedures, and practices must be developed and implemented for the ongoing review of the prescribed entity's privacy policies, procedures, and practices ("policy, procedures, and practices for ongoing review"). The purpose of this ongoing review is to determine on a regular

basis whether amendments are needed or whether new privacy policies, procedures, and practices are required.

The policy, procedures, and practices for ongoing review must identify the:

- frequency of the review of the privacy policies, procedures, and practices, which at minimum must be reviewed at least once prior to each three-year review by the IPC
- agent(s) responsible and the procedure for undertaking the review
- timeframe in which the review will be undertaken
- agent(s) responsible and the procedure for amending and/or drafting new privacy policies, procedures, and practices
- agent(s) responsible, and the procedure, for seeking and providing approval of any amendments or newly developed privacy policies, procedures, and practices, if deemed necessary as a result of the review
- agent(s) responsible and the procedure for communicating the amended or newly developed privacy policies, procedures, and practices
- method and nature of the communication to agents, the public, and other stakeholders, as may be relevant, depending on the nature of the subject matter

In undertaking the ongoing review and determining whether amendments and/or new privacy policies, procedures, and practices are necessary, the prescribed entity must have regard to:

- any relevant orders, decisions, guidelines, fact sheets, and best practices issued by the IPC and the courts under the CYFSA and its regulations
- evolving industry privacy standards and best practices
- amendments to the CYFSA and its regulations relevant to the prescribed entity
- findings, mitigations, and other relevant recommendations arising from privacy and information security audits, privacy impact assessments and investigations into **privacy complaints**, **privacy breaches**, and/or **information security breaches**
- findings and associated recommendations arising from prior three-year reviews
- whether the privacy policies, procedures, and practices of the prescribed entity continue to be consistent with its actual practices
- whether there is consistency between and among the privacy and information security policies, procedures, and practices implemented

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach***

Management, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices

- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

This policy, procedures, and practices may either be a stand-alone document or may be combined with the ***Policy, Procedures, and Practices for Ongoing Review of Information Security Policies, Procedures and Practices***.

Transparency

3. Policy on the Transparency of Privacy Policies, Procedures, and Practices

A policy must be developed and implemented that identifies the information made available to the public and other stakeholders relating to the privacy policies, procedures, and practices implemented by the prescribed entity ("transparency policy") and that identifies the means by which such information is made available.

At a minimum, the transparency policy should require the prescribed entity to make the following information publicly available:

- its **Privacy Policy**
- brochures, frequently asked questions, and/or other plain language tools related to the privacy policies, procedures, and practices implemented by the prescribed entity
- a list of the data holdings of personal information maintained by the prescribed entity
- the name and/or title, mailing address, and contact information of the agent(s) to whom inquiries, concerns, or complaints may be directed regarding the prescribed entity's compliance with its privacy policies, procedures, and practices and with the CYFSA and its regulations

Privacy impact assessments or summaries of the privacy impact assessments conducted should also be made available.

Brochures, Frequently Asked Questions, and Other Plain Language Tools

The transparency policy should set out the minimum content of the brochures, frequently asked questions, and/or other plain language tools and, in particular, such content should:

- describe the status of the prescribed entity under the CYFSA, the duties and responsibilities arising from this status, and the privacy policies, procedures, and practices implemented in respect of personal information, including the:
    - types of personal information collected and the persons or organizations from which this personal information is typically collected
    - the specific purposes for which personal information is collected
    - in accordance with the ***Policy, Procedures, and Practices for the Segregation of Personal Information***, the data linkages of the personal information, including the specific purposes for which the personal information is linked, the personal information used for linking, and the process used to link the personal information
    - the specific purposes for which personal information is used, and, if identifiable information is not routinely used, the nature of the information that is used
    - circumstances in which and the purposes for which personal information is disclosed and the persons or organizations to which it is typically disclosed
- identify some of the administrative, technical, and physical safeguards implemented to protect the privacy of individuals whose personal information is received and to maintain the confidentiality of that information, including the steps taken to protect personal information against theft, loss and unauthorized collection, use, or disclosure, and to protect records of personal information against unauthorized copying, modification, or disposal
- provide the name and/or title, mailing address, and contact information of the agent(s) to whom inquiries, concerns, or complaints may be directed regarding the prescribed entity's compliance with the privacy policies, procedures, and practices.

Statement on Public Website

The prescribed entity should have a statement on its website informing the public of the IPC's:

- role in reviewing and approving the prescribed entity's policies, procedures, and practices
- website where documentation in respect of these reviews and approvals can be found, and provide a link to the website

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices

- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

Collection of Personal Information and Data Holdings

4. Policy, Procedures, and Practices for the Collection of Personal Information

A policy, procedures, and practices must be developed and implemented to identify:

- the specific purposes for which personal information will be collected by the prescribed entity from service providers
- the nature of the personal information that will be collected
- the secure manner in which personal information will be collected

The policy, procedures, and practices must articulate a commitment by the prescribed entity not to collect:

- personal information, unless the collection is permitted by the CYFSA and its regulations
- personal information if other information will serve the purpose
- any more personal information than is reasonably necessary to meet the purpose

Review and Approval Process for Collection of Personal Information

The policy, procedures, and practices must identify the:

- agent(s) responsible for reviewing and determining whether to approve the collection of personal information
- process that must be followed
- requirements that must be satisfied
- the criteria that must be considered

At a minimum, the above criteria must require the responsible agent(s) to ensure that:

- the collection is permitted by the CYFSA and its regulations and that any and all conditions or restrictions set out in the CYFSA, and its regulations have been satisfied
- other information, namely **de-identified and/or aggregate information**, will not serve the identified purpose, and that no more personal information is being requested than is reasonably necessary to meet the identified purpose

The policy, procedures, and practices must also set out:

- the manner of documenting the decision, approving or denying the collection of personal information
- the reasons for the decision
- the method and format in which the decision will be communicated
- to whom the decision will be communicated

Conditions or Restrictions on the Approval to Collect Personal Information

The policy, procedures, and practices must identify the conditions or restrictions that are required to be satisfied prior to the collection of personal information, having regard to the requirements of the CYFSA and its regulations. Such policy, procedures, and practices must include:

- any documentation and/or agreements that must be completed, provided, or executed
- the agent(s) or other persons or organizations responsible for completing, providing, or executing the documentation and/or agreements
- the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the collection of personal information have, in fact, been satisfied

Secure Retention, Transfer, Return or Disposal of Personal Information

The policy, procedures, and practices must require:

- that records of personal information collected by the prescribed entity be retained in a secure manner in compliance with the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Information***
- that records of personal information collected by an agent of the prescribed entity, be transferred in a secure manner in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Information***
- identification of the agent(s) responsible for ensuring that the records of personal information that have been collected are either securely returned or securely disposed of, as the case may be, following the retention period or the date of termination set out in any documentation, and/or agreements executed prior to the collection of the personal information

If the records of personal information are required to be securely returned to the service provider from which they were collected, the policy, procedures, and practices must require the records to be transferred in a secure manner and in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Information***. If the records are to be disposed of, the policy, procedures, and practices must require the records to be disposed of in a secure manner and in compliance with the ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Information***.

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

5. Policy, Procedures, and Practices for the Segregation of Personal Information

A policies, procedures, and practices must be developed and implemented by prescribed entities with respect to the segregation of personal information collected from service providers under the CYFSA.

The policies, procedures, and practices must require:

- that personal information collected or used for CYFSA purposes be segregated from other personal information and personal health information held by the prescribed entity
- the precise manner in which the records of personal information will be securely segregated from other records containing other personal information or personal health information
- the secure manner of segregation must be consistent with the CYFSA, PHIPA, and other legal requirements, as well as orders, guidelines, fact sheets, and best practices issued by the IPC

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices

- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

6. List of Data Holdings Containing Personal Information

The prescribed entity must develop and retain an up-to-date list and brief description of the data holdings of personal information maintained by the prescribed entity under the CYFSA.

7. Policy, Procedures, and Practices for Statements of Purpose for Data Holdings Containing Personal Information

A policy, procedures, and practices must be developed and implemented with respect to the creation, review, amendment, and approval of statements of purpose for data holdings containing personal information.

The policy, procedures, and practices must require that the statements of purpose:

- set out the specific purpose of the data holding
- describe the personal information contained in the data holding
- identify the service providers and any other source(s) of the personal information
- explain the need for the personal information in relation to the identified purpose
- explain why **de-identified and/or aggregate information** will not serve the identified purpose

The policy, procedures, and practices must further specify the:

- agent(s) responsible and the process that must be followed in completing the statements of purpose for the data holdings containing personal information, including the agent(s) or other person(s) or organization(s) that must be consulted in the process
- agent(s) responsible for approving the statements of purpose
- role of the agent(s) that have been delegated day-to-day authority to manage the privacy program in respect of the statements of purpose
- person(s) and organization(s) that will be provided the statements of purpose, including, at a minimum, the service providers from whom the personal information in the data holding is collected
- frequency with which and the circumstances in which the statements of purpose must be reviewed
- agent(s) responsible and the process that must be followed in reviewing the statements of purpose and amending them, as necessary

- agent(s) or other person(s) or organization(s) that must be consulted in reviewing, and, if necessary, amending the statements of purpose
- agent(s) responsible for approving the amended statements of purpose
- person(s) and organization(s) that will be provided amended statements of purpose upon approval, including the service providers or other persons or organizations from whom the personal information in the data holding is collected

The policy, procedures, and practices must be reviewed on an ongoing basis to ensure their continued accuracy, that the personal information collected for purposes of the data holding is still necessary for the identified purpose(s), and that **de-identified and/or aggregate information** will not serve the identified purpose.

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices In Respect of Privacy Audits***

8. Statements of Purpose for Data Holdings Containing Personal Information

For each data holding containing personal information, the prescribed entity must complete a statement identifying the specific purpose of the data holding, the personal information contained in the data holding, the service providers and any other source(s) of the personal information, the need for the personal information in relation to the identified purpose, and why **de-identified and/or aggregate information** will not serve the identified purpose.

Access and Use of Personal Information

9. Policy, Procedures, and Practices for Limiting Agent Access to and Use of Personal Information

A policy, procedures, and practices must be developed and implemented to limit access to and use of personal information by agents based on the "need to know" principle. The purpose of this policy, procedures, and practices is to ensure that agents of the prescribed entity access

and use the least identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual or other responsibilities.

The policy, procedures, and practices must:

- identify the limited and narrowly defined purposes for which and circumstances in which agents are permitted to access and use personal information and the levels of access to personal information that may be granted
- ensure that the duties of agents with access to personal information are segregated in order to avoid a concentration of privileges that would enable a single agent to compromise personal information

For all other purposes and in all other circumstances, the policy, procedures, and practices must require agents to access and use **de-identified and/or aggregate information**, as defined in the ***Policy, procedures, and practices with Respect to De-Identification and Aggregation***.

The policy, procedures, and practices must explicitly prohibit access to and use of personal information if other information, such as **de-identified and/or aggregate information**, will serve the identified purpose and must prohibit access to or use of more personal information than is reasonably necessary to meet the identified purpose.

The policy, procedures, and practices must also prohibit agents from using **de-identified and/or aggregate information**, either alone or with other information, to identify an individual, unless the re-identification is done in accordance with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation*** and is permitted by the CYFSA or another Act. This must include prohibiting any attempt to decrypt information that is encrypted or identifying an individual based on unencrypted information and/or prior knowledge.

Review and Approval Process for Allowing Access and Use by Agents

The policy, procedures, and practices must identify the agent(s) responsible and the process to be followed in receiving, reviewing, and determining whether to approve or deny a request by an agent for access to and use of personal information, along with the various level(s) of access that may be granted by the prescribed entity.

In outlining the process to be followed, the policy, procedures, and practices must set out the:

- requirements to be satisfied in requesting, reviewing, and determining whether to approve or deny a request by an agent for access to and use of personal information
- criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request for access to and use of personal information, and the criteria for determining the appropriate level of access
- manner of documenting the decision, approving or denying the request for access to and use of personal information and the reasons for the decision
- method and format in which the decision will be communicated and to whom

- documentation that must be completed, provided, and/or executed upon rendering the decision
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom the documentation must be provided
- required content of the documentation

At a minimum, the agent(s) responsible for determining whether to approve or deny a request for access to and use of personal information must be satisfied that:

- the agent making the request routinely requires access to and use of personal information on an ongoing basis or for a specified period for their employment, contractual, or other responsibilities
- the identified purpose for which access to and use of personal information is being requested is permitted by the CYFSA and its regulations
- the identified purpose for which access to and use of personal information is being requested cannot reasonably be accomplished without personal information
- **de-identified and/or aggregate information** will not serve the identified purpose
- no more personal information will be accessed and used than is reasonably necessary to meet the identified purpose

Conditions or Restrictions on the Approval

The policy, procedures, and practices must identify the conditions or restrictions imposed on an agent granted approval to access and use personal information, such as read only, create, edit, update, or delete limitations, and the circumstances in which the conditions or restrictions will be imposed.

In the event that an agent only requires access to and use of personal information for a specified period, the policy, procedures, and practices must set out the process to be followed in ensuring that access to and use of the personal information is permitted only for that specified time period.

All approved accesses and uses of personal information should be subject to an automatic expiry, following which an agent is again required to request approval to access and use personal information in accordance with the policy, procedures, and practices. At a minimum, the expiry date should be one year from the date approval is granted and agents should seek re-approval on an annual basis.

The policy, procedures, and practices must also prohibit an agent from accessing and using personal information, except as necessary for their employment, contractual, or other responsibilities, from accessing and using personal information if other information will serve the identified purpose and from accessing and using more personal information than is reasonably necessary to meet the identified purpose. The prescribed entity must also ensure that all accesses to and uses of personal information are permitted by the CYFSA and its regulations.

Further, the policy, procedures, and practices must impose conditions or restrictions on the purposes for which and the circumstances in which an agent granted approval to access and use personal information is permitted to disclose that personal information. The prescribed entity must ensure that any such disclosures are permitted by the CYFSA and its regulations.

Notification and Termination of Access and Use by Agents

The policy, procedures, and practices must require an agent granted approval to access and use personal information, or their supervisor, to notify the prescribed entity when the agent is no longer employed or retained by the prescribed entity or no longer requires such access. In this regard, the policy, procedures, and practices must:

- set out the procedure to be followed in providing the notification
- identify the agent(s) to whom this notification must be provided
- stipulate the timeframe within which this notification must be provided
- specify the nature and format of the notification
- set out the documentation that must be completed, provided and/or executed, if any
- identify the agent(s) responsible for completing, providing, and/or executing the documentation and identify the agent(s) to whom the documentation must be provided
- set out the required content of the documentation
- identify the agent(s) responsible for terminating access to and use of the personal information
- set out the procedure to be followed in terminating access to and use of the personal information
- specify the method by which access will be terminated and the timeframe within which access to and use of the personal information must be terminated

The prescribed entity must ensure that the procedures implemented in this regard are consistent with the ***Policy, Procedures, and Practices upon Termination or Cessation of the Employment or Contractual Relationship***.

Secure Retention and Disposal

The policy, procedures, and practices must require an agent granted approval to access and use personal information to securely retain the records of personal information in compliance with the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Information*** and, where applicable, to securely dispose of the records of personal information in compliance with the ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Information***.

Tracking Approved Access to and Use of Personal Information

The policy, procedures, and practices must:

- require the prescribed entity to maintain information with regard to the agent(s) granted approval to access and use personal information in such a manner that the prescribed entity can promptly generate a log from the information
- identify the agent(s) responsible for maintaining the information
- address where documentation related to the receipt, review, approval, denial, or termination of access to and use of personal information is to be retained and the agent(s) responsible for retaining this documentation

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

10. Log of Agents Granted Approval to Access and Use Personal Information

A prescribed entity must maintain information with regard to agents granted approval to access and use personal information. The information must be maintained in such a manner that the prescribed entity can promptly generate a log from the information. At a minimum, the information, and any subsequent log generated from the information, must include the:

- name of the agent granted approval to access and use personal information
- data holdings of personal information to which the agent has been granted approval to access and use
- level or type of access and use granted
- date that access and use was granted
- termination date or the date of the next audit of access to and use of the personal information

11. Policy, Procedures, and Practices for the Use of Personal Information for Research

A policy, procedures, and practices must be developed and implemented to identify whether and in what circumstances, if any, the prescribed entity permits personal information to be

used for research purposes. If the prescribed entity does not permit personal information to be used for research purposes, the policy, procedures, and practices must explicitly prohibit the use of personal information for research purposes. If the prescribed entity does not permit **de-identified and/or aggregate information** to be used for research purposes, the policy, procedures, and practices must explicitly prohibit such use as well.

Where the Use of Personal Information is Permitted for Research

Where the prescribed entity permits personal information to be used for research purposes, the policy, procedures, and practices must articulate a commitment by the prescribed entity not to use personal information for research purposes if other information will serve the research purpose, and not to use more personal information than is reasonably necessary to meet the research purpose.

The policy, procedures, and practices must further set out the circumstances in which personal information is permitted to be used for research purposes.

Distinction Between the Use of Personal Information for Research and Other Purposes

The policy, procedures, and practices must:

- clearly distinguish between the use of personal information for research purposes and the use of personal information for purposes of data analysis, or the compilation of statistical information with respect to the management of, evaluation, or monitoring of services, the allocation of resources to or planning for those services, including their delivery under sections 293(1) or (3) of the CYFSA
- identify the criteria that must be considered in distinguishing between these uses, as well as the agent(s) responsible, and the procedure to be followed in making this determination

Review and Approval Process for Research Purposes

The policy, procedures, and practices must identify the agent(s) responsible for receiving, reviewing, and determining whether to approve or deny a request for the use of personal information for research purposes and the request process that must be followed. At a minimum, the request process must set out the:

- documentation that must be completed, provided and/or executed
- agent(s) responsible for completing, providing and/or executing the documentation
- agent(s) to whom this documentation must be provided
- required content of the documentation

The policy, procedures, and practices must also address the:

- requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request to use personal information for research purposes, having regard to the CYFSA and its regulations

- manner of documenting the decision approving or denying the request to use personal information for research purposes and the reasons for the decision
- method and format in which the decision will be communicated, and to whom

At a minimum, prior to any approval of the use of personal information for research purposes the agent(s) responsible for determining whether to approve or deny the request must ensure that:

- the written **research plan** complies with the requirements in the CYFSA and its regulations
- the written **research plan** has been approved by a research ethics board
- the prescribed entity must receive 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** as set out in section 4 of O. Reg 191/18
- the personal information being requested is consistent with the personal information identified in the written **research plan** approved by the research ethics board
- other information, namely **de-identified and/or aggregate information**, will not serve the research purpose
- no more personal information is being requested than is reasonably necessary to meet the research purpose

Conditions or Restrictions on the Approval for Research Purposes

Having regard to the CYFSA and its regulations, the policy, procedures, and practices must identify the conditions or restrictions that will be imposed on the approval to use personal information for research purposes.

At a minimum, the policies, procedures, and practices should require the agent(s) granted approval to use personal information for research purposes to comply with the following requirements:

- use the information only for the purposes set out in the **research plan** approved by the research ethics board
- not publish the information in a form that could reasonably enable a person to ascertain the identity of the individual
- not disclose any personal information disclosed to the agent except as required by law
- not make contact, or attempt to make contact, directly or indirectly, with any individual whose personal information has been disclosed to the agent
- notify the prescribed entity immediately in writing if the agent fails to fulfill any of the above-listed requirements

The policy, procedures, and practices must also:

- set out any documentation that must be completed, provided, or executed to record such conditions or restrictions

- identify the agent(s) responsible for completing, providing, or executing the documentation
- identify the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of personal information for research purposes are in fact being satisfied
- require the agent who is granted approval to use personal information for research purposes to retain the records of personal information in compliance with the written **research plan** approved by the research ethics board and in compliance with the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Information***
- address whether and in what circumstances an agent who is granted approval to use personal information for research purposes is required to securely return or securely dispose of the records of personal information, or is permitted to de-identify and retain the records following the retention period in the written **research plan** approved by the research ethics board

Secure Return of Records of Personal Information

If the records of personal information are required to be securely returned to the prescribed entity, the policy, procedures, and practices must require the records to be transferred in a secure manner and in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Information***.

The policy, procedures, and practices must further stipulate the timeframe following the retention period set out in the written **research plan** within which the records must be securely returned, the secure manner in which the records must be returned, and the agent to whom the records must be securely returned.

Secure Disposal of Records of Personal Information

If the records of personal information are required to be disposed of in a secure manner, the policy, procedures, and practices must require the records to be disposed of in accordance with the ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Information***.

Certificate of Destruction

The policy, procedures, and practices must identify the:

- agent of the prescribed entity to whom the **certificate of destruction** must be provided
- timeframe following the retention period in the written **research plan** within which the records must be securely disposed of and require a **certificate of destruction** to be provided
- required content of the **certificate of destruction**

A certificate that evidences the destruction of records of personal information must, at a minimum:

- identify the records of personal information securely disposed of

- indicate the date, time, and method of secure disposal employed
- bear the name and signature of the agent who performed the secure disposal

De-Identification of Records of Personal Information

If the records of personal information are required to be de-identified and retained by the agent rather than being securely returned or disposed of, the policy, procedures, and practices must:

- require the records of personal information to be de-identified in compliance with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***
- stipulate the timeframe following the retention period set out in the written **research plan** within which the records must be de-identified

The policy, procedures, and practices must also identify the agent(s) responsible for ensuring that records of personal information used for research purposes are securely returned, securely disposed of, or de-identified within the stipulated timeframe following the retention period set out in the written **research plan**, and the process to be followed in the event of non-compliance with these requirements.

Tracking Approved Uses of Personal Information for Research

The policy, procedures, and practices must:

- require that a log be maintained of the approved uses of personal information for research purposes
- identify the agent(s) responsible for maintaining such a log
- address where written **research plans**, copies of the approval decisions of research ethics boards, certificates of destruction, and other documentation related to the receipt, review, approval, or denial of requests for the use of personal information for research purposes will be retained
- identify the agent(s) responsible for retaining this documentation

Use of De-identified and/or Aggregate Information for Research

The policy, procedures, and practices must indicate whether or not **de-identified and/or aggregate information** may be used for research purposes. If the prescribed entity permits de-identified and/or aggregate information to be used for research purposes, the policy, procedures, and practices must set out the circumstances in which de-identified and/or aggregate information is permitted to be used for research purposes, and require that the records of personal information to be de-identified in compliance with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***.

Review and Approval Process

If the prescribed entity permits **de-identified and/or aggregate information** to be used for research purposes, the policy, procedures, and practices must identify the agent(s) responsible for receiving, reviewing, and determining whether to approve or deny a request for the use of

de-identified, and/or aggregate information for research purposes, and the request process that must be followed. At a minimum, the request process must set out the:

- documentation that must be completed, provided and/or executed, including the:
    - agent(s) responsible for completing, providing and/or executing the documentation
    - agent(s) to whom this documentation must be provided
    - required content of the documentation

The policy, procedures, and practices must also address the:

- requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request to use **de-identified and/or aggregate information** for research purposes
- manner of documenting the decision approving or denying the request for the use of **de-identified and/or aggregate information** for research purposes and the reasons for the decision
- method and the format in which the decision will be communicated, and to whom

At a minimum, the policy, procedures, and practices must:

- require the **de-identified and/or aggregate information** to be reviewed prior to the approval and use of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual, and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual
- identify the agent(s) responsible for undertaking this prior review

Conditions or Restrictions on the Approval

The policy, procedures, and practices must also identify the conditions or restrictions that will be imposed on the approval to use **de-identified and/or aggregate information** for research purposes, including any documentation that must be completed, provided, or executed and the agent(s) responsible for completing, providing, or executing the documentation.

At a minimum, the policy, procedures, and practices must prohibit an agent who is granted approval to use **de-identified and/or aggregate information** for research purposes from using that information, either alone or with other information, to identify an individual, unless the re-identification is done in accordance with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation*** and is permitted by the CYFSA or another Act. This must include prohibiting any attempt to decrypt information that is encrypted or identifying an individual based on unencrypted information and/or prior knowledge.

The policy, procedures, and practices must also identify the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of **de-identified and/or aggregate information** for research purposes are in fact being satisfied.

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

12. Log of Approved Uses of Personal Information for Research

A prescribed entity that permits the use of personal information for research purposes must maintain a log of the approved uses that, at a minimum, includes:

- the name of the research study
- the name of the agent(s) to whom the approval was granted
- the date of the decision of the research ethics board approving the written **research plan**
- the specific purpose of the research study
- the date that the approval to use personal information for research purposes was granted by the prescribed entity
- the date that the personal information was provided to the agent(s)
- the nature of the personal information provided to the agent(s)
- the retention period for the records of personal information identified in the written **research plan** approved by the research ethics board
- whether the records of personal information will be securely returned, securely disposed of, or de-identified and retained following the retention period
- the date the records of personal information were securely returned, or a **certificate of destruction** was received, or the date by which the records of personal information must be returned or disposed of, if applicable

Disclosure of Personal Information for Research

13. Policy, Procedures, and Practices for Disclosure of Personal Information for Research Purposes and the Execution of Research Agreements

A policy, procedures, and practices must be developed and implemented to identify whether and in what circumstances, if any, the prescribed entity permits personal information to be disclosed for research purposes in accordance with section 6 of O. Reg 191/18. If the prescribed entity does not permit personal information to be disclosed for research purposes, the policy, procedures, and practices must explicitly prohibit the disclosure of personal information for research purposes and indicate whether or not **de-identified and/or aggregate information** may be disclosed for research purposes.

If the prescribed entity does *not* permit **de-identified and/or aggregate information** to be disclosed for research purposes, the policy, procedures, and practices must explicitly prohibit the disclosure of de-identified and/or aggregate information as well.

Where the Disclosure of Personal Information is Permitted for Research

Where the prescribed entity permits the disclosure of personal information for research purposes in accordance with section 6 of O. Reg 191/18, the policy, procedures, and practices must:

- articulate a commitment by the prescribed entity not to disclose personal information for research purposes if other information will serve the research purpose and not to disclose more personal information than is reasonably necessary to meet the research purpose
- set out the circumstances in which personal information is permitted to be disclosed for research purposes

Review and Approval Process

The policy, procedures, and practices must identify that the prescribed entity is responsible for receiving, reviewing, and determining whether to approve or deny a request for the disclosure of personal information for research purposes, as well as the process that must be followed. At a minimum, the request process must set out the:

- documentation that must be completed, provided, and/or executed by agent(s) of the prescribed entity or by the researcher
- agent(s) to whom this documentation must be provided
- required content of the documentation

Having regard to the CYFSA and its regulations, the policy, procedures, and practices must also address the requirements that must be satisfied and the criteria that must be considered by the prescribed entity whether to approve the request for the disclosure of personal information for research purposes.

At a minimum, prior to any approval of the disclosure of personal information for research purposes, the policy, procedures, and practices must require the prescribed entity to ensure that:

- the prescribed entity is in receipt of a written **research plan** that has been approved by the research ethics board
- the written **research plan** complies with the requirements in the CYFSA and its regulations
- the prescribed 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**
- the personal information being requested is consistent with the personal information identified in the written **research plan** approved by the research ethics board
- other information, namely **de-identified and/or aggregate information**, will not serve the research purpose
- no more personal information is being requested than reasonably necessary to meet the research purpose

The policy, procedures, and practices must also set out:

- the manner of documenting the decision, approving or denying the request for the disclosure of personal information for research purposes and the reasons for the decision
- the method by which and the format in which the decision will be communicated
- to whom the decision will be communicated

Conditions or Restrictions on the Approval

The policy, procedures, and practices must identify the conditions, restrictions, or recommendations that are required to be satisfied prior to the approval of disclosure of personal information for research purposes, including any documentation and/or agreements that must be completed, provided, or executed, and the agent(s) or researcher responsible for completing, providing, or executing the documentation and/or agreements. At a minimum, the policy, procedures, and practices must:

- require that a **Research Agreement** be executed in accordance with the ***Template Research Agreement*** prior to the disclosure of personal information for research purposes
- the prescribed entity must be satisfied that the researcher will comply with the requirements set out in section 6(2)(c) of O. Reg 191/18
- identify the agent(s) responsible for ensuring that any conditions, restrictions, or recommendations that must be satisfied prior to the disclosure of personal information for research purposes have, in fact, been satisfied, including the execution of a **Research Agreement**

- require the records of personal information disclosed for research purposes to be transferred in a secure manner in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Information***

Secure Return, Disposal or De-Identification of Records of Personal Information for Research

The policy, procedures, and practices must:

- identify the agent(s) responsible for ensuring that records of personal information disclosed to a researcher for research purposes are either securely returned, securely disposed of, or de-identified in compliance with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***, as the case may be, within a specific timeframe following the retention period set out in the **Research Agreement**
- address the process to be followed by the responsible agent(s) where records of personal information are not securely returned, a **certificate of destruction** is not received, or written confirmation of de-identification is not received within the time set out in the **Research Agreement**

Documentation Related to Approved Disclosures of Records of Personal Information for Research

The policy, procedures, and practices must also:

- address where documentation related to the receipt, review, approval, or denial of requests for the disclosure of personal information for research purposes will be retained, including, written **research plans**, proof that the research plan has been approved by a research ethics boards, **Research Agreements**, and certificates of destruction
- identify the agent(s) responsible for retaining this documentation

Disclosure of De-Identified and/or Aggregate Information for Research Purposes

If the prescribed entity permits **de-identified and/or aggregate information** to be disclosed for research purposes, the policy, procedures, and practices must set out the circumstances in which de-identified, and/or aggregate information is permitted to be disclosed for research purposes.

Review and Approval Process

The policy, procedures, and practices must identify that the prescribed entity is responsible for receiving, reviewing, and determining whether to approve or deny a request for the disclosure of **de-identified and/or aggregate information** for research purposes, and the request process that must be followed. At a minimum, the request process must set out the:

- documentation that must be completed, provided, and/or executed by agent(s) of the prescribed entity or by a researcher, having regard to the CYFSA and its regulations
- agent(s) to whom this documentation must be provided

- required content of the documentation
- manner of documenting the decision approving or denying the request for the disclosure of **de-identified and/or aggregate information** for research purposes and the reasons for the decision
- method and format in which the decision will be communicated, and to whom

The policy, procedures, and practices should address whether the prescribed entity requires the preparation of a written **research plan** in accordance with the CYFSA and its regulations and/or requires research ethics board approval of the written research plan prior to the approval and the subsequent disclosure of **de-identified and/or aggregate information** for research purposes.

The policy, procedures, and practices must also address the requirements that must be satisfied and the criteria that must be considered by the prescribed entity to approve or deny the request for the disclosure of **de-identified and/or aggregate information** for research purposes. At a minimum, the policy, procedures, and practices must:

- require the **de-identified and/or aggregate information** to be reviewed prior to the approval and the subsequent disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual
- identify the agent(s) responsible for undertaking the review

Conditions or Restrictions on the Approval

The policy, procedures, and practices must:

- comply with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***
- identify the conditions, restrictions, or recommendations that are required to be satisfied prior to the disclosure of **de-identified and/or aggregate information** for research purposes, including:
    - any documentation and/or agreements that must be completed, provided, or executed
    - the agent(s) or researcher responsible for completing, providing, or executing the documentation and/or agreements

At a minimum, the prescribed entity must require the researcher to whom the **de-identified and/or aggregate information** will be disclosed to acknowledge and agree, in writing, that the researcher will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is permitted by the CYFSA or another Act and is in accordance with the written **research plan** approved by the research ethics board. This must include prohibiting any attempt to decrypt information that is encrypted or identifying an individual based on unencrypted information and/or prior knowledge.

In accordance with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***, a prescribed entity may address different release models (i.e. public, semi-public, and non-public) in its policies, procedures, and practices. Where the policies, procedures, and practices of a prescribed entity address different release models and the calculated risk of re-identification has met the threshold for the data release to be made "public," such written acknowledgement may not be necessary.

The policy, procedures, and practices must also:

- identify the documentation and/or agreements that must be completed, provided, or executed and the agent(s) or researcher responsible for completing, providing, or executing the documentation and/or agreements
- identify that the prescribed entity is responsible for ensuring that any conditions, restrictions, or recommendations that must be satisfied prior to the disclosure of the **de-identified and/or aggregate information** have, in fact, been satisfied, including the execution of the written acknowledgement and agreement
- require the prescribed entity to track receipt of the executed written acknowledgements and agreements
- set out the procedure that must be followed and related documentation that must be maintained

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

14. Template Research Agreement

A **Research Agreement** must be executed with the researchers to whom personal information will be disclosed prior to the disclosure of the personal information for research purposes under section 6 of O. Reg 191/18. At a minimum, the **Research Agreement** must address the matters set out below.

General Provisions

The **Research Agreement** must:

- only permit the researcher to use the personal information for the purposes set out in the written **research plan** approved by the research ethics board and must prohibit the use of the personal information for any other purpose
- prohibit the researcher from permitting any person to access and use the personal information except those persons described in the written **research plan** approved by the research ethics board
- describe the status of the prescribed entity under the CYFSA and the duties and responsibilities arising from this status
- provide a definition of personal information that is consistent with the Freedom of Information and Protection of Privacy Act (FIPPA)
- specify the precise nature of the personal information that will be disclosed by the prescribed entity for research purposes
- where applicable, set out any restrictions with respect to small cell-sizes (e.g. less than five), having regard to the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation*** implemented by the prescribed entity and the written **research plan**

Purposes of Collection, Use, and Disclosure

The **Research Agreement** must:

- identify the research purpose for which the personal information is being disclosed by the prescribed entity
- identify the purposes for which the personal information may be used or disclosed by the researcher
- specify the statutory authority for each collection, use, and disclosure identified
- explicitly state whether the personal information may be linked to other information

In identifying the purposes for which the personal information may be used, the **Research Agreement** must explicitly:

- state whether the personal information may be linked to other information
- prohibit the personal information from being linked, except in accordance with the written **research plan** approved by the research ethics board

The **Research Agreement** must also require the researcher to acknowledge that:

- the personal information that is being disclosed pursuant to the **Research Agreement** is necessary for the identified research purpose(s) and that other information, namely **de-identified and/or aggregate information**, will not serve the research purpose

- no more personal information is being collected and will be used than is reasonably necessary to meet the research purpose

The **Research Agreement** must also impose restrictions on the disclosure of personal information. At a minimum, the Research Agreement must require the researcher to acknowledge and agree not to:

- disclose the personal information, except as required by law and subject to the exceptions and additional requirements prescribed in the CYFSA's regulations
- publish the personal information in a form that could reasonably enable a person to ascertain the identity of the individual or
- make contact or attempt to make contact with the individual to whom the personal information relates, directly or indirectly

Compliance with the Statutory Requirements for the Disclosure for Research Purposes

The **Research Agreement** must require:

- the researcher and the prescribed entity to acknowledge and agree that the researcher has submitted a written **research plan** which has been approved by a research ethics board that meets the requirements of the CYFSA and its regulations
- the researcher to also acknowledge and agree that the researcher will comply with the:
    - **Research Agreement**
    - written **research plan** approved by the research ethics board
    - recommendations, if any, specified by the research ethics board in respect of the written **research plan**

Secure Transfer of Records of Personal Information

The **Research Agreement** must:

- require the secure transfer of records of personal information that will be disclosed pursuant to the **Research Agreement**
- set out the secure manner in which records of personal information will be transferred, including:
    - under what conditions and to whom the records will be transferred
    - the procedure that will be followed in ensuring that the records of personal information are transferred in a secure manner. In identifying the secure manner in which the records of personal information will be transferred, the **Research Agreement** must have regard to the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Information*** implemented by the prescribed entity

Secure Retention of Records of Personal Information

The **Research Agreement** must:

- identify the retention period for the records of personal information subject to the **Research Agreement**, including the length of time that the records of personal information will be retained in identifiable form (the retention period identified must be consistent with that set out in the written **research plan** approved by the research ethics board)
- require the researcher to ensure that the records of personal information are retained in a secure manner and must identify the precise manner in which the records of personal information in paper and electronic format will be securely retained (in identifying the secure manner in which the records of personal information will be retained, the **Research Agreement** may have regard to the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Information***, and must have regard to the written **research plan** approved by the research ethics board)
- require the researcher to take steps that are reasonable in the circumstances to ensure that the records of personal information subject to the **Research Agreement** are:
    - protected against theft, loss, and unauthorized collection, use, or disclosure
    - protected against unauthorized copying, modification, or disposal
- detail the reasonable steps that the researcher is required to take, which, at a minimum, must include those set out in the written **research plan** approved by the research ethics board

The **Research Agreement** must also address whether the records of personal information subject to the Research Agreement will be returned in a secure manner, will be disposed of in a secure manner, or will be de-identified and retained by the researcher following the retention period set out in the Research Agreement. In this regard, the provisions in the Research Agreement must be consistent with the written **research plan** approved by the research ethics board.

Secure Return of Records of Personal Information

If the records of personal information are required to be returned in a secure manner, the **Research Agreement** must stipulate the:

- timeframe following the retention period within which the records must be securely returned
- secure manner in which the records must be returned
- agent of the prescribed entity to whom the records must be securely returned

In identifying the secure manner in which the records of personal information will be returned, regard may be had to the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Information*** implemented by the prescribed entity.

Secure Disposal of Records of Personal Information

If the records of personal information subject to the **Research Agreement** are required to be disposed of in a secure manner, the Research Agreement must:

- provide a definition of secure disposal that is consistent with the CYFSA and its regulations
- identify the precise manner in which the records of personal information must be securely disposed of
- stipulate the timeframe following the retention period set out in the **Research Agreement** within which:
    - the records of personal information must be securely disposed of
    - a **certificate of destruction** must be provided

In identifying the secure manner in which the records of personal information will be disposed of, the method of secure disposal identified must at a minimum be consistent with:

- the CYFSA and its regulations
- orders and decisions issued by the IPC under the CYFSA and its regulations. These orders under PHIPA may also be useful for reference purposes: **Order HO-001** and **Order HO-006**
- guidelines, fact sheets, and best practices issued by the IPC pursuant to the CYFSA and its regulations, including **Fact Sheet 10: Secure Destruction of Personal Information**
- policies, procedures, and practices implemented by the prescribed entity, such as the ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Information***

Certificate of Destruction

The **Research Agreement** must identify the:

- agent of the prescribed entity to whom the **certificate of destruction** must be provided
- timeframe following secure disposal within which the **certificate of destruction** must be provided
- required content of the **certificate of destruction**

A certificate that evidences the destruction of records of personal information must, at a minimum:

- identify the records of personal information securely disposed of
- stipulate the date, time, location, and method of secure disposal employed
- bear the name and signature of the person who performed the secure disposal

Where Records Are De-identified and Retained

If the records of personal information are required to be de-identified and retained by the researcher rather than being securely returned or disposed of, the manner and process for de-identification must be set out in the **Research Agreement**. In identifying the manner and process for de-identification, regard may be had to the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation*** implemented by the prescribed entity. The Research Agreement must also:

- require the researcher to submit written confirmation that the records were de-identified
- stipulate the timeframe following the retention period set out in the **Research Agreement** within which the written confirmation must be provided
- specify the agent of the prescribed entity to whom the written confirmation must be provided

The **Research Agreement** must also require the researcher to whom the **de-identified and/or aggregate information** will be disclosed to acknowledge and agree, in writing, that the researcher will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is permitted by the CYFSA or another Act and is in accordance with the written **research plan** approved by the research ethics board. This must include prohibiting any attempt to decrypt information that is encrypted or identifying an individual based on unencrypted information and/or prior knowledge.

In accordance with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***, a prescribed entity may address different release models (i.e. public, semi-public, and non-public) in its policies, procedures, and practices. Where the policies, procedures, and practices of a prescribed entity address different release models and the calculated risk of re-identification has met the threshold for the data release to be made "public," such written acknowledgement may not be necessary.

Breach Notification to Prescribed Entity

At a minimum, the **Research Agreement** must require the researcher to notify the prescribed entity immediately, in writing, if the researcher becomes aware:

- of a breach or suspected breach of the **Research Agreement**
- a breach or suspected breach of subsection 6(2)(c) of O. Reg 191/18 or
- if personal information subject to the **Research Agreement** is stolen, lost or collected, used, or disclosed without authority, or is believed to have been stolen, lost or collected, used, or disclosed without authority

The **Research Agreement** should also identify the agent of the prescribed entity to whom notification must be provided and must require the researcher to take steps that are reasonable in the circumstances to contain the breach.

Consequences of Breach and Monitoring Compliance

The **Research Agreement** must also:

- provide the prescribed entity with the right to audit the researcher's compliance with the agreement
- set out the manner and circumstances in which compliance will be audited and the notice, if any, that will be provided to the researcher of the audit
- require the researcher to ensure that all persons who will have access to the personal information, as identified in the written **research plan** approved by the research ethics board, are aware of and agree to comply with the terms and conditions of the **Research Agreement** prior to being given access to the personal information
- set out the method by which this will be ensured by the researcher, such as requiring the persons identified in the written **research plan** to sign an acknowledgement prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the **Research Agreement**
- outline the consequences of a breach of the agreement

15. Log of Research Agreements

A prescribed entity must maintain a log of executed Research Agreements. At a minimum, the log must include:

- the name of the research study
- the name of the principal researcher
- the date(s) of receipt of the written **research plan** and the approval of the research ethics board
- the specific purpose of the research
- the date that the approval to disclose the personal information for research purposes was granted by the prescribed entity
- the date that the **Research Agreement** was executed
- the date that the personal information was disclosed
- the nature of the personal information disclosed
- the retention period for the records of personal information as set out in the **Research Agreement**
- whether the records of personal information will be securely returned, securely disposed of, or de-identified and retained by the researcher following the retention period set out in the **Research Agreement**
- the date that the records of personal information were securely returned, a **certificate of destruction** was received, or written confirmation of de-identification was received, or the date by which they must be returned, disposed of, or de-identified

Disclosure of Personal Information for Purposes Other Than Research

16. Policy, Procedures, and Practices for Disclosure of Personal Information for Purposes Other Than Research

A policy, procedures, and practices must be developed and implemented that limits the disclosure of personal information by prescribed entities for purposes other than research to disclosures required by law and disclosures to another prescribed entity for the purposes described in section 293(1) of the CYFSA. The policy, procedures, and practices must explicitly prohibit all other disclosures of personal information for non-research purposes. If the prescribed entity does not permit **de-identified and/or aggregate information** to be disclosed for purposes other than research, the policy, procedures, and practices must explicitly prohibit such disclosure as well.

Where the Disclosure of Personal Information is Permitted

Where the prescribed entity permits personal information to be disclosed for purposes other than research, the policy, procedures, and practices must:

- articulate a commitment by the prescribed entity not to disclose personal information if other information will serve the purpose and not to disclose more personal information than is reasonably necessary to meet the purpose
- set out the purposes other than research for which and the circumstances in which the disclosure of personal information is permitted
- require that all such disclosures comply with the CYFSA and its regulations

Review and Approval Process

The policy, procedures, and practices must identify the agent(s) responsible for receiving, reviewing, and determining whether to approve or deny a request for the disclosure of personal information for purposes other than research and the process that must be followed. At a minimum, the request process must set out the:

- documentation that must be completed, provided and/or executed
- agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation
- agent(s) to whom this documentation must be provided
- required content of the documentation

Having regard to the CYFSA and its regulations, the policy, procedures, and practices must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request for the disclosure of personal information for purposes other than research.

At a minimum, the agent(s) responsible for determining whether to approve or deny the request for the disclosure of personal information for purposes other than research must be required to ensure that:

- the disclosure is permitted by the CYFSA and its regulations and that any and all conditions or restrictions set out in the CYFSA, and its regulations have been satisfied
- other information, namely **de-identified and/or aggregate information**, will not serve the identified purpose of the disclosure
- no more personal information is being requested than is reasonably necessary to meet the identified purpose

With respect to the decision approving or denying the request for the disclosure of personal information for purposes other than research, the policy, procedures, and practices must also set out:

- the reasons for the decision
- the manner of documenting the decision approving or denying the request for the disclosure of personal information for purposes other than research
- the method by which and the format in which the decision will be communicated
- to whom the decision will be communicated

Conditions or Restrictions on the Approval

The policy, procedures, and practices must identify the conditions or restrictions that are required to be satisfied prior to the disclosure of personal information for purposes other than research, including any documentation and/or agreements that must be completed, provided, or executed, and the agent(s) or other persons or organizations responsible for completing, providing, or executing the documentation and/or agreements. At a minimum, the policy, procedures, and practices must:

- require a **Data Sharing Agreement** to be executed in accordance with the ***Policy, Procedures, and Practices for the Execution of Data Sharing Agreements*** and the ***Template Data Sharing Agreement*** prior to any disclosure of personal information for purposes other than research
- identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal information have, in fact, been satisfied, including the execution of a **Data Sharing Agreement**
- require records of personal information to be transferred in a secure manner in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Information***

Secure Return or Disposal of Records of Personal Information

The policy, procedures, and practices must:

- identify the agent(s) responsible for ensuring that records of personal information disclosed to a person or organization for purposes other than research are either securely returned or securely disposed of, as the case may be, following the retention period in the **Data Sharing Agreement** or the date of termination of the Data Sharing Agreement
- address the process to be followed where records of personal information are not securely returned, or a **certificate of destruction** is not received within a reasonable period of time following the retention period in the **Data Sharing Agreement**, or the date of termination of the Data Sharing Agreement
- identify the agent(s) responsible for implementing this process and the stipulated timeframe following the retention period or the date of termination within which this process must be implemented

In the context of disclosures that are required by law, different legal requirements with respect to the secure return or disposal of records of personal information may apply.

Documentation Related to Approved Disclosures of Personal Information

The policy, procedures, and practices must address where documentation related to the receipt, review, approval, or denial of requests for the disclosure of personal information for purposes other than research will be retained and the agent(s) responsible for retaining this documentation.

Disclosure of De-identified and/or Aggregate Information

The policy, procedures, and practices must indicate whether **de-identified and/or aggregate information** may be disclosed for purposes other than research, and if so, must set out the circumstances in which de-identified and/or aggregate information is permitted to be disclosed for non-research purposes and comply with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***.

Review and Approval Process

If the prescribed entity permits **de-identified and/or aggregate information** to be disclosed for non-research purposes, the policy, procedures, and practices must identify the agent(s) responsible for receiving, reviewing, and determining whether to approve or deny a request for the disclosure of de-identified and/or aggregate information, and the process that must be followed. At a minimum, the request process must set out the:

- documentation that must be completed, provided and/or executed
- agent(s) or other persons or organizations responsible for completing, providing, and/or executing the documentation
- agent(s) to whom this documentation must be provided
- required content of the documentation

The policy, procedures, and practices must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for the disclosure of **de-identified and/or aggregate information** for purposes other than research.

At a minimum, the policy, procedures, and practices must:

- require the **de-identified and/or aggregate information** to be reviewed prior to the approval and the subsequent disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual
- identify the agent(s) responsible for undertaking this review

The policy, procedures, and practices must also specify the:

- manner of documenting the decision approving or denying the request for the disclosure of **de-identified and/or aggregate information** for purposes other than research and the reasons for the decision
- method by which and the format in which the decision will be communicated and to whom

Conditions or Restrictions on the Approval

The policy, procedures, and practices must also identify the conditions or restrictions that are required to be satisfied prior to the approval and the subsequent disclosure of **de-identified and/or aggregate information** for non-research purposes, including any documentation and/or agreements that must be completed, provided, or executed and the agent(s) or other persons or organizations responsible for completing, providing, or executing the documentation and/or agreements.

At a minimum, the prescribed entity must require the person or organization to which the **de-identified and/or aggregate information** will be disclosed to acknowledge and agree, in writing, that the person or organization will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is permitted by the CYFSA or another Act. This must include prohibiting any attempt to decrypt information that is encrypted or identifying an individual based on unencrypted information and/or prior knowledge.

In accordance with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***, a prescribed entity may address different release models (i.e. public, semi-public, and non-public) in its policies, procedures, and practices. Where the policies, procedures, and practices of a prescribed entity address different release models and the calculated risk of re-identification has met the threshold for the data release to be made "public," such written acknowledgement may not be necessary.

The policy, procedures, and practices must also identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the

de-identified and/or aggregate information have, in fact, been satisfied, including the execution of the written acknowledgement. Further, the policy, procedures, and practices must require the responsible agent(s) to track receipt of the executed written acknowledgments and must set out the procedure that must be followed and the documentation that must be maintained.

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

17. Policy, Procedures, and Practices for the Execution of Data Sharing Agreements

A policy, procedures, and practices must be developed and implemented to identify the:

- circumstances requiring the execution of a **Data Sharing Agreement**
- process that must be followed when executing a **Data Sharing Agreement**
- requirements that must be satisfied prior to the execution of a **Data Sharing Agreement**

With respect to collections and disclosures of personal information for purposes other than research, the policy, procedures, and practices must:

- set out the circumstances requiring the execution of a **Data Sharing Agreement** prior to the collection of personal information for purposes other than research
- require the execution of a **Data Sharing Agreement** prior to any disclosure of personal information for purposes other than research
- identify the agent(s) responsible for ensuring that a **Data Sharing Agreement** is executed
- set out the process that must be followed and the requirements that must be satisfied, which, at a minimum, must set out the:
    - documentation that must be completed, provided, and/or executed
    - agent(s) or other persons or organizations responsible for completing, providing, and/or executing the documentation

- agent(s) to whom the documentation must be provided
- required content of the documentation

In relation to the disclosure of personal information for purposes other than research, the agent(s) responsible for ensuring that a **Data Sharing Agreement** is executed must be satisfied that the disclosure was approved in accordance with the ***Policy, Procedures, and Practices for Disclosure of Personal Information For Purposes Other Than Research***. In relation to the collection of personal information for purposes other than research, the agent(s) responsible for ensuring that a **Data Sharing Agreement** is executed must be satisfied that the collection was approved in accordance with the ***Policy, Procedures, and Practices for the Collection of Personal Information***.

The policy, procedures, and practices must also:

- require that a log of **Data Sharing Agreements** be maintained
- identify the agent(s) responsible for maintaining such a log
- address where documentation related to the execution of **Data Sharing Agreements** will be retained
- identify the agent(s) responsible for retention of executed **Data Sharing Agreements**

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

18. Template Data Sharing Agreement

A prescribed entity must ensure that a **Data Sharing Agreement** is executed in the circumstances set out in the ***Policy, Procedures, and Practices for the Execution of Data Sharing Agreements*** that, at a minimum, addresses the matters set out below.

General Provisions

The **Data Sharing Agreement** must:

- describe the status of the prescribed entity under the CYFSA and the duties and responsibilities arising from this status
- provide a definition of personal information that is consistent with FIPPA
- specify the precise nature of the personal information subject to the **Data Sharing Agreement** (where it is not reasonably possible for a prescribed entity to list or itemize every data element or variable, the prescribed entity may identify categories of data elements or variables)
- identify the person or organization that is collecting personal information or disclosing personal information pursuant to the **Data Sharing Agreement**

Purposes of Collection, Use, and Disclosure

The **Data Sharing Agreement** must identify the purposes for which the personal information subject to the Data Sharing Agreement is being collected and for which purposes the personal information will be used.

In identifying these purposes, the **Data Sharing Agreement** must explicitly state whether or not the personal information collected pursuant to the Data Sharing Agreement will be linked to other information. If the personal information will be linked to other information in accordance with the ***Policy, Procedures, and Practices for the Segregation of Personal Information***, the Data Sharing Agreement must identify and describe:

- the nature of the information to which the personal information will be linked
- the source of the information to which the personal information will be linked
- how the linkage will be conducted
- why the linkage is required for the identified purpose(s)

The **Data Sharing Agreement** must also:

- contain an acknowledgement that:
    - the personal information collected pursuant to the **Data Sharing Agreement** is necessary for the purpose for which it was collected
    - other information, namely **de-identified and/or aggregate information**, will not serve the purpose
    - no more personal information is being collected and will be used than is reasonably necessary to meet the purpose
- identify the purposes, if any, for which the personal information subject to the **Data Sharing Agreement** may be further disclosed and any limitations, conditions, or restrictions imposed thereon

- require the collection, use, and disclosure of personal information subject to the **Data Sharing Agreement** to comply with the CYFSA and its regulations
- set out the specific statutory authority for each collection, use, and disclosure contemplated in the **Data Sharing Agreement**
- set out any restrictions with respect to small cell-sizes (e.g. less than five), having regard to the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation*** implemented by the prescribed entity

Secure Transfer of Records of Personal Information

The **Data Sharing Agreement** must require the secure transfer of the records of personal information subject to the Data Sharing Agreement and must specifically set out the:

- secure manner in which the records of personal information will be transferred, including under what conditions and to whom the records will be transferred
- procedure that must be followed in ensuring that the records are transferred in a secure manner (in identifying the secure manner in which the records of personal information will be transferred, regard should be had to the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal information*** implemented by the prescribed entity)

Secure Retention of Records of Personal Information

The retention period for the records of personal information subject to the **Data Sharing Agreement** must be specified in the Data Sharing Agreement. In identifying the relevant retention period, the records of personal information must be retained only for as long as necessary to fulfill the purposes for which the records of personal information were collected.

The **Data Sharing Agreement** must:

- require the records of personal information to be retained in a secure manner
- specify the manner in which the records of personal information in paper and electronic format will be securely retained, including whether the records will be retained in identifiable form. In identifying the secure manner in which the records of personal information will be retained, the **Data Sharing Agreement** should have regard to the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Information*** implemented by the prescribed entity
- require reasonable steps to be taken to ensure that the records of personal information subject to the **Data Sharing Agreement** are protected against:
    - theft, loss and unauthorized collection, use, or disclosure
    - unauthorized copying, modification or disposal
- detail the reasonable steps that are required to be taken

The **Data Sharing Agreement** must address whether the records of personal information subject to the Data Sharing Agreement will be returned or disposed of in a secure manner following the:

- retention period set out in the **Data Sharing Agreement** or
- date of termination of the **Data Sharing Agreement**, as the case may be

Secure Return of Records of Personal Information

If the records of personal information are required to be returned in a secure manner, the **Data Sharing Agreement** must stipulate the:

- timeframe following the retention period or following the date of termination of the **Data Sharing Agreement** within which the records of personal information must be securely returned
- secure manner in which the records must be returned, having regard to the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Information*** implemented by the prescribed entity
- agent to whom the records must be securely returned

Secure Disposal of Records of Personal Information

If the records of personal information are required to be disposed of in a secure manner, the **Data Sharing Agreement** must:

- provide a definition of secure disposal that is consistent with the CYFSA and its regulations
- specify the manner in which the records of personal information subject to the **Data Sharing Agreement** must be securely disposed of
- stipulate the timeframe following the retention period or following the date of termination of the **Data Sharing Agreement** within which the records of personal information must be securely disposed of
- specify the timeframe within which a **certificate of destruction** must be provided

In identifying the secure manner in which the records of personal information will be disposed of, the method of secure disposal identified must at a minimum be consistent with:

- the CYFSA and its regulations
- orders and decisions issued by the IPC under the CYFSA and its regulations. These orders under PHIPA may also be useful for reference purposes: **Order HO-001** and **Order HO-006**
- guidelines, fact sheets and best practices issued by the IPC pursuant to the CYFSA and its regulations, including **Fact Sheet 10: Secure Destruction of Personal Information**
- the ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Information*** implemented by the prescribed entity

Certificate of Destruction

The **Data Sharing Agreement** must identify the:

- person to whom the **certificate of destruction** must be provided
- timeframe following secure disposal within which the **certificate of destruction** must be provided
- required content of the **certificate of destruction**

A certificate that evidences the destruction of records of personal information must, at a minimum:

- identify the records of personal information securely disposed of
- stipulate the date, time, location and method of secure disposal employed
- bear the name and signature of the person who performed the secure disposal

Breach Notification to Prescribed Entity

At a minimum, the **Data Sharing Agreement** must require that notification be provided at the first reasonable opportunity if:

- the **Data Sharing Agreement** has been breached or is suspected to have been breached or
- the personal information subject to the **Data Sharing Agreement** is stolen, lost or collected, used or disclosed without authority or is believed to have been stolen, lost or collected, used or disclosed without authority

The **Data Sharing Agreement** should also identify whether the notification of breach must be oral and/or in writing and to whom the notification must be provided. The **Data Sharing Agreement** must also require that reasonable steps be taken to contain the breach.

Consequences of Breach and Monitoring Compliance

The **Data Sharing Agreement** must:

- provide the prescribed entity with the right to audit compliance with the agreement
- set out the manner and circumstances in which compliance will be audited and the notice, if any, that will be provided of the audit
- require that all persons who will have access to the personal information are aware of and agree to comply with the terms and conditions of the **Data Sharing Agreement** prior to being given access to the personal information
- set out the method by which this will be ensured (this may include requiring the persons who will have access to the personal information to sign an acknowledgement, prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the **Data Sharing Agreement**)
- outline the consequences of a breach of the agreement

19. Log of Data Sharing Agreements

A prescribed entity must maintain a log of executed **Data Sharing Agreements**. At a minimum, the log must include:

- the name of the person or organization from whom the personal information was collected or to whom the personal information was disclosed
- the purpose of the collection or disclosure
- the date that the collection or disclosure of personal information was approved, as the case may be
- the date that the **Data Sharing Agreement** was executed
- the date the personal information was collected or disclosed, as the case may be
- the nature of the personal information subject to the **Data Sharing Agreement**
- the retention period for the records of personal information set out in the Data Sharing Agreement or the date of termination of the **Data Sharing Agreement**
- whether the records of personal information will be securely returned, or will be securely disposed of following the retention period set out in the **Data Sharing Agreement**, or the date of termination of the Data Sharing Agreement
- the date the records of personal information were securely returned, or a **certificate of destruction** was provided, or the timeframes by which they must be returned or disposed of

Third Party Service Provider Agreements

20. Policy, Procedures, and Practices for Executing Agreements with Third Party Service Providers in Respect of Personal Information

A policy, procedures, and practices for executing agreements with third party service providers ("TPSPs") must:

- require written agreements to be entered into with TPSPs contracted or otherwise engaged to provide services to the prescribed entity prior to permitting TPSPs to access and use the personal information of the prescribed entity
- require the written agreements to contain the relevant language from the ***Template Agreement for Third Party Service Providers***
- identify the agent(s) responsible for ensuring that an agreement is executed, as well as the process that must be followed and the requirements that must be satisfied prior to the execution of a **TPSP Agreement**

Limitations on Access to and Use of Personal Information

The policy, procedures, and practices with respect to **TPSP Agreements** must require the prescribed entity to:

- prohibit a TPSP from accessing or using personal information if other information, namely **de-identified and/or aggregate information**, will serve the purpose or from accessing or using more personal information to be accessed or used than is reasonably necessary to meet the purpose
- identify the agent responsible for making this determination
- ensure that TPSPs agree to comply with the restrictions and conditions that are necessary to enable the prescribed entity to comply with the CYFSA and its regulations (this includes prohibiting TPSPs from accessing or using the personal information of the prescribed entity unless the TPSP is permitted to do so in the **TPSP Agreement** and agrees to comply with the restrictions that apply to the prescribed entity)
- outline the process to be followed by the prescribed entity in auditing the TPSP's compliance with the agreement and must set out the manner and circumstances in which compliance will be audited and the notice, if any, that will be provided to the TPSP of the audit
- outline the consequences of a breach of the agreement

Vulnerability Management Practices

The policy, procedures, and practices should ensure that TPSPs have vulnerability management practices that meet a standard of protection that is at least equivalent to that of the prescribed entity, in accordance with the ***Policy, Procedures, and Practices for Vulnerability and Patch Management***.

Secure Transfer, Retention, Back-Up, and Disposal

The policy, procedures, and practices must also:

- identify any purposes for which and circumstances in which records of personal information of the prescribed entity may be transferred to TPSPs, including for secure retention or secure disposal
- detail the procedure to be followed in securely transferring records of personal information to the TPSP and in securely retrieving records from the TPSP, including the:
    - secure manner in which the records will be transferred and retrieved
    - conditions pursuant to which the records will be transferred and retrieved
    - agent(s) responsible for ensuring the secure transfer and retrieval of the records
    - require the records to be transferred in a secure manner in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Information***

The policy, procedures, and practices must address the documentation that is required to be maintained in relation to the transfer of records of personal information to a TPSP for secure retention and/or secure disposal. In particular, the policy, procedures, and practices must require:

- the agent(s) responsible for ensuring the secure transfer to document the date, time, mode of transfer, and whether the records are transferred for secure retention and/or secure disposal
- the maintenance of a repository of written confirmations received from the TPSP upon receipt of the records of personal information
- a detailed inventory to be maintained of records of personal information being securely retained by the TPSP and of records of personal information retrieved by the prescribed entity
- the identification of the agent(s) responsible for maintaining the detailed inventory

The policy, procedures, and practices must:

- outline the procedure to be followed in tracking the dates that certificates of destruction are received from the TPSP and the agent(s) responsible for conducting such tracking
- set out the process to be followed where a **certificate of destruction** is not received within the time set out in the agreement with the TPSP
- identify the agent(s) responsible for implementing the procedure and processes related to certificates of destruction
- set out the process to be followed where records of personal information are not securely returned or a **certificate of destruction** is not received following the termination of the agreement, including:
    - the agent(s) responsible for implementing this process
    - the timeframe following termination of the agreement within which this process must be implemented
    - the agent(s) responsible for ensuring that records of personal information provided to a TPSP are either securely returned to the prescribed entity or are securely disposed of, as the case may be, following the termination of the agreement

Where a TPSP is contracted to securely retain or securely dispose of records of personal information of the prescribed entity, the policy, procedures, and practices must further:

- require that a written agreement be executed with the TPSP containing the relevant language from the ***Template Agreement for Third Party Service Providers***
- identify the agent(s) responsible for ensuring that the **TPSP Agreement** has been executed prior to transferring the records of personal information for secure retention and/or secure disposal

These requirements apply where a TPSP is contracted to retain backed-up records of personal information of the prescribed entity, or where a TPSP backs-up records of personal information of the prescribed entity it has been contracted to retain, regardless of whether the TPSP uses remote-based (cloud) systems or on-premise systems.

Tracking Agreements

The policy, procedures, and practices must require that a log be maintained of all **TPSP agreements** executed with TPSPs who are permitted to access or use personal information. The policy, procedures, and practices must further:

- identify the agent(s) responsible for maintaining such a log and for tracking the **TPSP Agreements**
- outline the process to be followed in tracking all TPSPs who are permitted to access or use personal information which includes setting out the documentation that must be completed, provided, and/or executed to verify that the agreements have been executed, including the:
    - agent(s) responsible for completing, providing, executing, and ensuring the execution of the documentation
    - agent(s) to whom this documentation must be provided
    - required content of the documentation
- outline the process to be followed and the agent(s) responsible for identifying TPSPs who have not executed the agreement and for ensuring that these TPSPs do so, within a set timeframe
- indicate where documentation related to the execution of **TPSP Agreements** will be retained
- identify the agent(s) responsible for retaining this documentation

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***

- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

21. Template Agreement for Third Party Service Providers

A written **TPSP Agreement** must be entered into with TPSPs that will be permitted to access and use personal information of the prescribed entity. This includes TPSPs contracted or otherwise engaged to retain, transfer, or dispose of records of personal information or to provide services for the purpose of enabling the prescribed entity to use electronic means to collect, use, modify, disclose, retain, transfer or dispose of personal information ("**electronic service providers**"). At a minimum, the **TPSP Agreement** must address the matters set out below.

General Provisions

The **TPSP Agreement** must:

- describe the status of the prescribed entity under the CYFSA and the duties and responsibilities arising from this status
- state whether or not the TPSP is an agent of the prescribed entity in providing services pursuant to the agreement

All TPSPs that are permitted to access and use personal information in the course of providing services to the prescribed entity must be considered agents of the prescribed entity, with the possible exception of **electronic service providers**. Agreements with electronic service providers must explicitly state whether or not the TPSP is also an agent of the prescribed entity in providing services pursuant to the agreement.

If the TPSP is an agent of the prescribed entity, the **TPSP Agreement** must require the TPSP to comply with the provisions of the CYFSA and its regulations relating to prescribed entities, as the case may be, and to comply with the privacy and information security policies, procedures, and practices implemented by the prescribed entity in providing services pursuant to the agreement.

The **TPSP Agreement** should provide a definition of personal information consistent with FIPPA. Where appropriate, the TPSP Agreement should also specify the precise nature of the personal information that the TPSP will be permitted to access and use in the course of providing services pursuant to the agreement.

The **TPSP Agreement** must also require that the services provided by the TPSP pursuant to the agreement be performed in a professional manner, in accordance with evolving industry privacy and information security standards and best practices, and by properly trained agents of the TPSP.

Obligations with Respect to Access and Use

The **TPSP Agreement** must identify the limited and narrowly defined purposes for which the TPSP is permitted to access and use the personal information of the prescribed entity and any limitations, conditions or restrictions imposed thereon, including where a TPSP is not an agent of the prescribed entity (i.e. a TPSP who acts solely as an electronic service provider).

In the case of a TPSP that is not an agent of the prescribed entity, the **TPSP Agreement** must prohibit TPSPs from using personal information except:

- as permitted in the **TPSP Agreement**
- for the purposes for which the prescribed entity is permitted to use personal information under the CYFSA and its regulations
- as necessary in the course of providing services pursuant to the agreement or as required by law

In the case of a TPSP that is also an agent of the prescribed entity, the **TPSP Agreement** must further:

- prohibit the TPSP from using personal information if other information, such as **de-identified and/or aggregate information**, will serve the purposes identified in the agreement
- prohibit the use of more personal information than is reasonably necessary to meet the purposes identified in the agreement
- identify one or more use(s) that is / are consistent with the uses of personal information permitted by the CYFSA and its regulations or another law

Obligations with Respect to Disclosure

The **TPSP Agreement** must identify the purposes, if any, for which the TPSP is permitted to disclose the personal information of the prescribed entity and any limitations, conditions, or restrictions imposed thereon.

In identifying the limited and narrowly defined purposes for which the TPSP is permitted to disclose personal information, the prescribed entity must ensure that each disclosure identified in the **TPSP Agreement** is consistent with, and reasonably necessary for, the disclosures of personal information permitted by the CYFSA and its regulations and is not contrary to the CYFSA, its regulations or another law.

In the case of a TPSP that is not an agent of the prescribed entity (i.e., a TPSP who acts solely as an electronic service provider), the **TPSP Agreement** must prohibit the TPSP from disclosing personal information to which it has access in the course of providing services except as required by law.

In the case of a TPSP that is also an agent of the prescribed entity, the **TPSP Agreement** must further prohibit the TPSP from disclosing personal information:

- except as permitted in the **TPSP Agreement**
- except for the purposes for which the prescribed entity is permitted to disclose personal information under the CYFSA and its regulations
- if other information will serve the purposes identified in the **TPSP Agreement**
- if the disclosure includes more personal information than is reasonably necessary to meet the purposes identified in the agreement

Secure Transfer

The **TPSP Agreement** must identify the purposes for which and the circumstances in which records of personal information of the prescribed entity may be transferred to the TPSP and transferred from the TPSP back to the prescribed entity, if any.

Where it is necessary to transfer records of personal information to or from the prescribed entity, the **TPSP Agreement** must require the TPSP and the prescribed entity to transfer the records of personal information in a secure manner and must set out the responsibilities of the TPSP and prescribed entity in this regard.

In particular, the **TPSP Agreement** must:

- specify the secure manner in which the records will be transferred
- the conditions pursuant to which the records will be transferred
- to whom the records will be transferred
- the procedure that must be followed in ensuring that the records are transferred in a secure manner

In identifying the secure manner in which records of personal information must be transferred, the **TPSP Agreement** must have regard to the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Information*** implemented by the prescribed entity.

In addition, where the retention or disposal of records of personal information outside the premises of the prescribed entity is the primary service provided to the prescribed entity, the **TPSP Agreement** must require the TPSP to provide documentation to the prescribed entity setting out the date, time, and mode of transfer of the records of personal information and confirming receipt. In these circumstances, the **TPSP Agreement** must also obligate the TPSP to maintain a detailed inventory of the records of personal information transferred.

Secure Retention and Back-Up

Where the third party is contracted to retain records of personal information on behalf of the prescribed entity, the **TPSP Agreement** must require the TPSP to do so in a secure manner and must identify the precise methods by which records of personal information will be securely retained by the TPSP, including records in both paper and electronic format retained on various media.

The **TPSP Agreement** must further outline the responsibilities of the TPSP in securely retaining the records of personal information having regard to the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Information*** implemented by the prescribed entity.

In addition, the **TPSP Agreement** must require the TPSP to securely segregate the records of personal information subject to the agreement from other personal information and personal health information retained by the third party service provider, in accordance with the ***Policy, Procedures, and Practices for the Segregation of Personal Information***.

Where a TPSP is contracted to retain backed-up records of personal information, or where a TPSP backs up records of personal information it has been contracted to retain, the **TPSP Agreement** must require the records to be backed-up and retained in a secure manner, having regard to the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Information*** and the ***Policy, Procedures, and Practices for Back-up and Recovery of Records of Personal Information*** implemented by the prescribed entity.

In identifying the secure manner by which the records of personal information will be securely backed-up and retained, the agreement must:

- identify the precise methods by which the records will be securely backed-up and retained by the TPSP, including records in both paper and electronic format retained on various media
- set out the responsibilities of the TPSP in securely backing-up and retaining the records

Where the retention of records of personal information or backed-up records of personal information is the primary service provided by the TPSP, the **TPSP Agreement** must require the TPSP to:

- maintain a detailed inventory of the records of personal information or backed-up records of personal information being retained on behalf of the prescribed entity
- a method to track the records being retained

Where a TPSP is contracted to retain records of personal information or backed-up records of personal information, or where a TPSP backs up records of personal information it has been contracted to retain, the **TPSP Agreement** must set out the circumstances in which the TPSP is required to make such records available to the prescribed entity. In regard to the circumstances in which backed-up records of personal information are required to be made available, the agreement must be in compliance with the ***Policy, Procedures, and Practices for Back-Up and Recovery of Records of Personal Information***.

The above requirements apply regardless of whether the TPSP uses remote-based (cloud) systems or on-premise systems.

Secure Return or Disposal of records of Personal Information

Where the **TPSP Agreement** provides that records of personal information of the prescribed entity may be transferred to the TPSP, the agreement must address whether records of personal information will be securely returned to the prescribed entity or will be disposed of in a secure manner. At a minimum, the TPSP Agreement must require that records of personal information of the prescribed entity transferred to the TPSP be securely returned or disposed of in a secure manner following the termination of the agreement.

If the records of personal information are required to be returned in a secure manner, the **TPSP Agreement** must stipulate the:

- timeframe within which the records of personal information must be securely returned

- secure manner in which the records must be returned
- agent of the prescribed entity to whom the records must be securely returned

In identifying the secure manner in which the records of personal information will be returned, the **TPSP Agreement** must have regard to the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Information*** implemented by the prescribed entity.

If the records of personal information are required to be disposed of in a secure manner, the **TPSP Agreement** must provide a definition of secure disposal that is consistent with the CYFSA and its regulations. At a minimum, the agreement must also identify the precise manner by which the records of personal information are to be securely disposed of by the TPSP, consistent with:

- the **CYFSA** and its **regulations**
- orders and decisions issued by the IPC under the CYFSA and its regulations (orders issued under PHIPA may also be useful for reference purposes, including: **Order HO-001** and **Order HO-006**)
- guidelines, fact sheets, and best practices issued by the IPC pursuant to the CYFSA and its regulations, including **Fact Sheet 10: Secure Destruction of Personal Information**
- the ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Information*** implemented by the prescribed entity

The **TPSP Agreement** must also stipulate the responsibilities of the TPSP in securely disposing of the records of personal information, including the:

- conditions pursuant to which the records will be securely disposed of by the TPSP
- precise method by which records must be securely disposed of, including records retained on various media, in both paper and/or electronic format
- person(s) responsible for ensuring the secure disposal of the records

Certificate of Destruction

The **TPSP Agreement** must identify the:

- agent of the prescribed entity to whom the **certificate of destruction** must be provided
- timeframe following secure disposal within which the **certificate of destruction** must be provided
- required content of the **certificate of destruction**

A certificate that evidences the destruction of records of personal information must, at a minimum:

- identify the records of personal information securely disposed of
- stipulate the date, time and method of secure disposal employed
- bear the name and signature of the person who performed the secure disposal

Implementation of Safeguards

The **TPSP Agreement** must require the TPSP to take steps that are reasonable in the circumstances to ensure that the records of personal information subject to the agreement are accessed and used in the course of providing services pursuant to the agreement are protected against theft, loss, and unauthorized collection, use, or disclosure, and protected against unauthorized copying, modification or disposal.

The **TPSP Agreement** must detail the reasonable steps required to be implemented by the TPSP having regard to the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Information*** implemented by the prescribed entity.

Training of Agents of the Third-Party Service Provider

The **TPSP Agreement** must require the TPSP to:

- provide training to its agents on the importance of protecting the privacy of individuals whose personal information is accessed and used in the course of providing services pursuant to the agreement
- inform its agents of the consequences that may arise in the event of a breach of these obligations
- ensure that its agents who will have access to the records of personal information are aware of and agree to comply with the terms and conditions of the agreement prior to being given access to the personal information (the **TPSP Agreement** must set out the method by which this will be ensured. This should include requiring agents of the TPSP to sign an acknowledgement, prior to being granted access to the personal information, indicating that they are aware of and agree to comply with the terms and conditions of the agreement)

Subcontracting of the Services

In the event that the **TPSP Agreement** permits the TPSP to subcontract the services provided under the agreement, the TPSP must be required to:

- acknowledge and agree that it will provide the prescribed entity with advance notice of its intention to do so
- enter into a written agreement with the subcontractor on terms consistent with its obligations to the prescribed entity
- provide the prescribed entity with a right to obtain a copy of the written sub-contracting agreement, upon request

Breach Notification to Prescribed Entity

At a minimum, the **TPSP Agreement** must require the TPSP to notify the prescribed entity at the first reasonable opportunity if:

- there has been a breach or suspected breach of the **TPSP Agreement**

- personal information handled by the TPSP on behalf of the prescribed entity is stolen, lost, or collected, used, or disclosed without authority or
- personal information handled by the TPSP on behalf of the prescribed entity is believed to have been stolen, lost, or collected, used, or disclosed without authority

The **TPSP Agreement** should also identify whether the notification must be oral, written, or both and to whom the notification must be provided. The **TPSP Agreement** must also require the TPSP to take steps that are reasonable in the circumstances to contain the breach, or to contain the theft, loss, or any unauthorized collection, use, or disclosure, and collaborate with the prescribed entity in its investigation.

Consequences of Breach and Monitoring Compliance

The **TPSP Agreement** must provide the prescribed entity with the right to audit the TPSP's compliance with the agreement and must also set out the manner and circumstances in which compliance will be audited and the notice, if any, that will be provided to the TPSP of the audit.

The **TPSP Agreement** should also allow the prescribed entity to request and obtain a copy of any independent audit of the TPSP's privacy and information security policies, procedures, and practices.

The **TPSP Agreement** must outline the consequences of a breach of the agreement.

22. Log of Agreements with Third Party Service Providers

A prescribed entity must maintain a log of executed agreements with TPSPs that are permitted to access and use personal information. At a minimum, the log must include:

- the name of the TPSP
- the nature of the services provided by the TPSP that require access to and use of personal information
- the date that the agreement with the TPSP was executed
- the date that the records of personal information or access to the records of personal information, if any, was first provided
- the nature of the personal information provided or to which access was provided
- the date of termination of the agreement with the TPSP
- whether the records of personal information were transferred to the TPSP, and if so the nature of the records transferred
- whether the records of personal information, if any, will be securely returned or will be securely disposed of upon termination of the agreement
- the date the records of personal information were securely returned or a **certificate of destruction** was provided, or the date that access to the personal information was terminated, or the date by which the records of personal information must be returned, or disposed of, or access terminated

Data Linkage, De-Identification and Aggregation

23. Policy, Procedures, and Practices for the Linkage of Records of Personal Information

A policy, procedures, and practices must be developed and implemented with respect to linkages of records of personal information.

The policy, procedures, and practices must identify whether or not the prescribed entity permits the linkage of records of personal information and, if it is not permitted, the policy, procedures, and practices must explicitly prohibit the linkage of records of personal information. If the linkage of records of personal information is permitted, the purposes for which and the circumstances in which such linkages are permitted must be identified.

In identifying the purposes for which and the circumstances in which the linkage of records of personal information is permitted, regard must be had to the sources of the records of personal information that are requested to be linked and the identity of the person or organization that will ultimately make use of the linked records of personal information, including where the linkage of records of personal information is:

- solely in the custody of the prescribed entity for the exclusive use by the prescribed entity
- in the custody of the prescribed entity with records of personal information to be collected from another person or organization for the exclusive use by the prescribed entity
- solely in the custody of the prescribed entity for purposes of disclosure of the linked records of personal information to another person or organization
- in the custody of the prescribed entity with records of personal information to be collected from another person or organization for purposes of disclosure of the linked records of personal information to that other person or organization

The policy, procedures, and practices must have regard to the ***Policy, Procedures, and Practices for the Segregation of Personal Information*** implemented by the prescribed entity. Particularly, segregation requirements must be taken into consideration in the process of reviewing, approving requests to link records of PI, and establishing conditions or restrictions on the approval.

Reviewing and Approving Requests to Link Records of Personal Information

The policy, procedures, and practices must identify the agent(s) responsible for receiving, reviewing, and determining whether to approve or deny the request to link records of personal information and the process that must be followed. This request process must set out the:

- documentation that must be completed, provided, and/or executed
- agent(s) or other persons or organizations responsible for completing, providing, and/or executing the documentation
- agent(s) to whom the documentation must be provided
- required content of the documentation

The policy, procedures, and practices must also address the:

- requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request to link records of personal information
- requirement for agent(s) to document the legal authority for linking the records of personal information.
- manner of documenting the decision approving or denying the request to link records of personal information and the reasons for the decision
- method and format in which the decision will be communicated and to whom

Conditions or Restrictions on the Approval

Where the linked records of personal information will be disclosed by the prescribed entity to another person or organization, the policy, procedures, and practices must require that the disclosure be approved pursuant to the ***Policy, Procedures, and Practices for Disclosure of Personal Information for Research Purposes and the Execution of Research Agreements*** or the ***Policy, Procedures, and Practices for Disclosure of Personal Information For Purposes Other Than Research***, as applicable.

Where the linked records of personal information will be used by the prescribed entity, the policy, procedures, and practices must require that the:

- use be approved pursuant to the ***Policy, Procedures, and Practices for the Use of Personal Information for Research*** or the ***Policy, Procedures, and Practices for Limiting Agent Access to and Use of Personal Information***, as may be applicable
- linked records of personal information be de-identified and/or aggregated as soon as reasonably possible pursuant to the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation*** and that, to the extent possible, only ***de-identified and/or aggregate information*** be used by agents of the prescribed entity

Process for the Linkage of Records of Personal Information

The policy, procedures, and practices must outline the process to be followed in linking records of personal information, the manner in which the linkage of records of personal information must be conducted and the agent(s) responsible for linking records of personal information when approved in accordance with this policy, procedures, and practices.

Secure Retention

The policy, procedures, and practices must require that linked records of personal information be retained in compliance with the Policy until they are **de-identified and/or aggregated** pursuant to the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***.

Secure Disposal

The policy, procedures, and practices must address the secure disposal of records of personal information linked by the prescribed entity and, in particular, must require that the records of personal information be securely disposed of in compliance with the ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Information***.

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

Tracking Approved Linkages of Records of Personal Information

The policy, procedures, and practices must require that the prescribed entity maintain information with regard to all requests and approvals to link records of personal information approved by the prescribed entity in such a manner that the prescribed entity can promptly generate a log from the information. Furthermore, the policy, procedures, and practices must:

- identify the agent(s) responsible for maintaining the information
- address where documentation related to the receipt, review, approval, or denial of requests to link records of personal information will be retained
- identify the agent(s) responsible for retaining this documentation

24. Log of Approved Linkages of Records of Personal Information

A prescribed entity, as the case may be, must maintain information with regard to all requests and approvals to link records of personal information. The information with regard to all requests and approvals must be maintained in such a manner that the prescribed entity can promptly generate a log from the information. At a minimum, the information, and any subsequent log generated from the information, must include the:

- name of the agent, person or organization who requested the linkage
- date that the linkage of records of personal information was approved

- nature of the records of personal information linked

25. Policy, Procedures, and Practices with Respect to De-Identification and Aggregation

A policy, procedures, and practices must be developed and implemented with respect to de-identification and aggregation that takes a risk-based approach and that:

- requires that personal information to not be used or disclosed if other information, namely **de-identified and/or aggregate information**, will serve the identified purpose
- provides a definition of **de-identified information and aggregate information**, which must have regard to small cell-sizes (e.g. less than five), and be consistent with the meaning of "**personal information**" in FIPPA
- requires removal, encryption, transformation, and/or truncation in order to constitute de-identified information and sets out the manner in which the information must be grouped, collapsed, or averaged in order to constitute aggregate information
- identifies the agent(s) responsible for de-identifying and/or aggregating information and the procedure to be followed
- requires **de-identified and/or aggregate information**, including information in small cell sizes (e.g. less than five), to be reviewed prior to use or disclosure in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual
- sets out the process to be followed in reviewing the **de-identified and/or aggregate information** and the criteria to be used in assessing and calculating the risk of re-identification
- identifies the agent(s) responsible for conducting this review

Different Release Models

The policy, procedures, and practices may address the following three different release models for **de-identified and/or aggregate information**: "public," "semi-public," and "non-public," having regard to the IPC's **De-Identification Guidelines for Structured Data** as well as evolving industry information security standards and best practices. Depending on the release model used, the required level of de-identification and/or aggregation may vary.

Small Cell Sizes

The policy, procedures, and practices must address small cell-sizes (e.g. less than five) and must require that the prescribed entity take a risk-based approach that involves calculating an acceptable level of re-identification risk for a given data release that utilizes techniques such as masking, generalization and suppression. The policy, procedures, and practices must set out the process and criteria for conducting such a risk-based analysis, having regard to the IPC's **De-Identification Guidelines for Structured Data**, as well as evolving industry information security standards and best practices.

In articulating the policy, procedures, and practices with respect to small cell-sizes, regard must be had to the restrictions related to small cell-sizes (e.g. less than five) contained in **Data Sharing Agreements**, *Research Agreements* and written **research plans** pursuant to which the personal information was collected by the prescribed entity.

Re-Identification

In establishing the criteria to be used in assessing the risk of re-identification, the prescribed entity must have regard to the type of identifying information available, including information that can be used to identify an individual directly (e.g., name, address) or indirectly (e.g., date-of-birth, postal code, gender).

The prescribed entity should explore new tools available or that are being developed to assist in ensuring that the policy, procedures, and practices developed with respect to de-identification and aggregation are based on an assessment of the actual risk of re-identification.

The policy, procedures, and practices must also prohibit agents from using **de-identified and/or aggregate information**, including information in small cell-sizes, to identify an individual, unless the re-identification is done in accordance with the policy, procedures, and practices and is permitted by the CYFSA or another Act. This must include prohibiting any attempt to decrypt information that is encrypted for the purpose of re-identification, or identifying an individual based on unencrypted information and/or prior knowledge.

Where the prescribed entity permits an agent to re-identify an individual from **de-identified and/or aggregate information**, the policy, procedures, and practices must identify the limited and specific purposes for which, and circumstances in which, de-identified and/or aggregate information may be re-identified and must identify the conditions or restrictions imposed on an agent granted approval to re-identify an individual from de-identified and/or aggregate information. The prescribed entity must ensure that any such approvals are granted in accordance with the policy, procedures, and practices and are permitted by the CYFSA or another Act.

The policy, procedures, and practices must identify the agent(s) responsible for receiving, reviewing, and determining whether to approve or deny the request to re-identify an individual from **de-identified and/or aggregate information** and the process that must be followed. This process must set out the:

- documentation that must be completed, provided, and/or executed
- agent(s) or other persons or organizations responsible for completing, providing, and/or executing the documentation
- agent(s) to whom the documentation must be provided
- required content of the documentation

The policy, procedures, and practices must also identify the mechanisms implemented to ensure that the persons or organizations to whom **de-identified and/or aggregate information** is disclosed will not use the de-identified and/or aggregate information, either alone or with other

information, to identify an individual, unless such re-identification is permitted by the CYFSA or another Act.

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

Privacy Impact Assessments

26. Policy, Procedures, and Practices for Privacy Impact Assessments

A policy, procedures, and practices must be developed and implemented to identify the circumstances in which privacy impact assessments are required to be conducted.

Circumstances in which Privacy Impact Assessments are Required to be Conducted

In identifying the circumstances in which privacy impact assessments are required to be conducted, the policy, procedures, and practices should ensure that prescribed entities conduct privacy impact assessments:

- on existing and proposed data holdings involving personal information
- whenever a new or a change to an existing information system, technology or program involving personal information is contemplated

With regard to the process that must be followed in identifying when privacy impact assessments are to be completed and reviewed, the policy, procedures, and practices must also identify the:

- process that must be followed in determining when privacy impact assessments are required to be completed and reviewed and the agent(s) responsible for making this determination
- process to be followed in ensuring that privacy impact assessments are in fact conducted, completed, reviewed, and amended, as necessary, and the agent(s) responsible for conducting the required follow-up

Circumstances in which Privacy Impact Assessments are Not Required

If there are limited and specific circumstances in which privacy impact assessments are not required to be conducted, having regard to the minimal level of risk involved, the policy, procedures, and practices must:

- require documentation of the rationale for why a privacy impact assessment is not required
- set out the documentation that must be completed, provided and/or executed
- identify the agent(s) responsible for completing, providing and/or executing the documentation
- identify the agent(s) to whom this documentation must be provided
- set out the required content of the documentation, including the criteria that must be used in making the determination that a privacy impact assessment is not to be conducted

Timing of Conducting and Reviewing Privacy Impact Assessments

The policy, procedures, and practices must also address the timing of privacy impact assessments:

- with respect to proposed data holdings involving personal information and the introduction of new or changes to existing information systems, technologies or programs involving personal information, the policy, procedures, and practices must require that privacy impact assessments be:
    - conducted at the conceptual design stage
    - reviewed and amended, if necessary, during the detailed design and implementation stage
- with respect to existing data holdings involving personal information, the policy, procedures, and practices must require:
    - a timetable be developed to ensure privacy impact assessments are conducted, as and/or updated, as and when necessary
    - the identification of the agent(s) responsible for developing the timetable

Once privacy impact assessments have been completed, the policy, procedures, and practices must require the:

- review of privacy impact assessments to take place on an ongoing basis to ensure that they continue to be accurate and continue to be consistent with the information practices of the prescribed entity
- identification of the circumstances in which and the frequency with which privacy impact assessments are required to be reviewed

Required Content of Privacy Impact Assessments

The policy, procedures, and practices must also stipulate the required content of privacy impact assessments. At a minimum, the privacy impact assessments must be required to describe:

- the data holding, information system, technology or program at issue
- the nature and type of personal information collected, used, or disclosed or that is proposed to be collected, used or disclosed
- the sources of the personal information
- the purposes for which the personal information is collected, used, or disclosed, or is proposed to be collected, used, or disclosed
- the reason that the personal information is required for the purposes identified
- the flows of the personal information
- the statutory authority for each collection, use, and disclosure of personal information identified
- the limitations imposed on the collection, use, and disclosure of the personal information
- whether or not the personal information is or will be linked to other information
- whether or not the personal information will be de-identified and/or aggregated and the specific purposes for which and circumstances in which the **de-identified and/or aggregate information** will be re-identified, if any, the conditions or restrictions imposed
- the retention period for the records of personal information
- the secure manner in which the records of personal information are or will be retained, transferred, and disposed of
- the functionality for logging access, use, modification, and disclosure of the personal information and the functionality to audit logs for unauthorized use or disclosure
- the risks to the privacy of individuals whose personal information is or will be part of the data holding, information system, technology, or program and an assessment of the risks
- recommendations to address and eliminate or reduce the privacy risks identified
- the administrative, technical, and physical safeguards implemented or proposed to be implemented to protect the personal information

Privacy Impact Assessment Findings and Recommendations

The policy, procedures, and practices must also outline the process for documenting the findings, and reviewing and addressing the mitigations and any other recommendations arising from privacy impact assessments, including the agent(s) responsible for:

- assigning other agent(s) to address the mitigations and any other relevant recommendations
- establishing timelines to address the mitigations and any other recommendations

- monitoring and ensuring the treatment of the mitigations and any other relevant recommendations within stated timelines
- evaluating the residual risks remaining after implementation

The policy, procedures, and practices must require that a log be maintained of:

- privacy impact assessments that have been completed
- privacy impact assessments that have been undertaken but that have not been completed
- privacy impact assessments that have not been undertaken
- the identification of the agent(s) responsible for maintaining such a log

In developing the policy and procedures, regard should be given to the various guidelines produced by the IPC and available at **www.ipc.on.ca**. Including the **Planning for Success: Privacy Impact Assessment Guide**.

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices In Respect of Privacy Audits***

27. Log of Privacy Impact Assessments

A prescribed entity must maintain a log of privacy impact assessments that have been completed and of privacy impact assessments that will be or have been undertaken, but that have not yet been completed. The log must describe the:

- data holding, information system, technology or program involving personal information that is at issue
- date that the privacy impact assessment was completed or is expected to be completed
- agent(s) responsible for completing or ensuring the completion of the privacy impact assessment

- findings, mitigations, and any other recommendations arising from the privacy impact assessment
- agent(s) responsible for addressing each mitigation and any other recommendation
- date that each mitigation or recommendation was or is expected to be addressed
- manner in which each recommendation was or is expected to be addressed

A prescribed entity must also maintain a log of data holdings involving personal information and of new or changes to existing information systems, technologies, or programs involving personal information for which privacy impact assessments have not been undertaken. For each such data holding, information system, technology, or program, the log either set out the:

- reasons that a privacy impact assessment will not be undertaken
- agent(s) responsible for making this determination
- date the determination was made

Privacy Audit Program

28. Policy, Procedures, and Practices in Respect of Privacy Audits

A policy, procedures, and practices must be developed and implemented that sets out the types of privacy audits that are required to be conducted. At a minimum, the audits required to be conducted must include:

- audits to assess compliance with the privacy policies, procedures, and practices implemented by the prescribed entity
- audits of the agent(s) permitted to access and use personal information pursuant to ***Policy, Procedures, and Practices for Limiting Agent Access to and Use of Personal Information***

With respect to each privacy audit that is required to be conducted, the policy, procedures, and practices must:

- set out the purposes of the privacy audit
- describe the nature and scope of the privacy audit (i.e. document reviews, interviews, site visits, inspections)
- identify the agent(s) responsible for conducting the privacy audit
- establish the frequency with which and the circumstances in which each privacy audit is required to be conducted
- require a privacy audit schedule to be developed
- identify the agent(s) responsible for developing the privacy audit schedule

At a minimum, audits of agents granted approval to access and use personal information under the ***Policy and Procedures for Limiting Agent Access to and Use of Personal Information*** must be conducted on an annual basis.

For each type of privacy audit that is required to be conducted, the policy, procedures, and practices must also set out the process to be followed prior to conducting the audit, including:

- criteria that must be considered in selecting the subject matter of the audit
- whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification must be provided

The policy, procedures, and practices must also set out the process that must be followed in reviewing and addressing the mitigations and any other recommendations resulting from privacy audits, including the agent(s) responsible for:

- assigning other agent(s) to address the mitigations and any other recommendations as required
- establishing timelines to address the mitigations and any other relevant recommendations
- monitoring and ensuring the treatment of mitigations and any other recommendations within the stated timelines
- evaluating the residual risks remaining after implementation

Required Documentation

The policy, procedures, and practices must further discuss the requirements for undertaking each privacy audit, including the:

- documentation that must be completed, provided and/or executed
- agent(s) responsible for completing, providing and/or executing the documentation
- agent(s) to whom this documentation must be provided
- required content of the documentation

The policy, procedures, and practices must also set out the nature of the documentation that must be completed, provided, and/or executed at the conclusion of the privacy audit, including the:

- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom the documentation must be provided
- required content of the documentation

Privacy Audit Findings

The policy, procedures, and practices must also address the manner, circumstances, and format in which the findings of privacy audits are communicated, including the mitigations and other relevant recommendations arising from the privacy audits and the status of addressing them. This must include:

- identifying the agent(s) responsible for communicating the findings of the privacy audit
- the mechanism and format for communicating the findings of the privacy audit, including the level of detail for communicating the findings

- the timeframe within which the findings of the privacy audit must be communicated
- to whom the findings of the privacy audit will be communicated, including whether the findings must be communicated to the Chief Executive Officer or the Executive Director (or equivalent position)

The policy, procedures, and practices must:

- require that a log be maintained of privacy audits
- identify the agent(s) responsible for maintaining the log of findings, mitigations, and other recommendations and for tracking that the mitigations/recommendations arising from the privacy audits are addressed within the identified timeframe
- address where documentation related to privacy audits will be retained
- identify the agent(s) responsible for retaining this documentation

Compliance, Audit and Enforcement

The policy, procedures, and practices must require the agent(s) responsible for conducting privacy audits to notify the prescribed entity, at the first reasonable opportunity, of a **privacy breach**, or suspected privacy breach in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, and/or of an **information security breach**, or information security incident in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***.

29. Log of Privacy Audits

A prescribed entity must maintain a log of privacy audits that have been completed. The log must set out the:

- nature and type of the privacy audit conducted
- date that the privacy audit was completed
- agent(s) responsible for completing the privacy audit
- findings, mitigations, and other relevant recommendations arising from the privacy audit
- agent(s) responsible for addressing each recommendation
- date that each recommendation was or is expected to be addressed
- manner in which each recommendation was or is expected to be addressed

Privacy Breaches

30. Policy, Procedures, and Practices for Privacy Breach Management

A policy, procedures, and practices must be developed and implemented to address the identification, reporting, containment, notification, investigation, and remediation of **privacy breaches**.

The policy, procedures, and practices must define the term "**privacy breach**" to, at a minimum, include:

- the collection, use, and disclosure of personal information that is not in compliance with the CYFSA or its regulations
- a contravention of the privacy policies, procedures, or practices implemented by the prescribed entity, related to the requirements of the CYFSA Addendum
- a contravention of written acknowledgments, **Data Sharing Agreements**, **Research Agreements**, **Confidentiality Agreements**, and **TPSP Agreements**, related to the requirements of the CYFSA Addendum
- circumstances where personal information is stolen, lost, or collected, used, or disclosed without authority, or where records of personal information are subject to unauthorized copying, modification or disposal

The policy, procedures, and practices may refer to some types of **privacy breaches** using the term "privacy incident" instead of "privacy breach", so long as the policy, procedures, and practices' requirements for privacy incidents otherwise comply with the requirements of the CYFSA Addendum applicable to privacy breaches, wherever necessary and applicable.

In developing the policy, procedures, and practices, the prescribed entity must have regard to the guidelines produced by the IPC entitled **Reporting a Privacy Breach to the Information and Privacy Commissioner: Guidelines for Service Providers**.

Identification of Privacy Breaches

The policy, procedures, and practices must set out the manner in which **privacy breaches** or suspected privacy breaches will be identified by agents of the prescribed entity. At a minimum, the policy, procedures, and practices must indicate that privacy breaches or suspected privacy breaches will be identified through notifications, including by agents and **electronic service providers** of the prescribed entity, privacy audits, and **privacy complaints** and inquiries.

The policy, procedures, and practices must require that agents notify the prescribed entity of a **privacy breach** or suspected privacy breach at the first reasonable opportunity. The policy, procedures, and practices must:

- identify the agent(s) who must be notified of the **privacy breach** or suspected privacy breach and must provide their contact information
- stipulate whether the notification must be provided orally and/or in writing and the nature of the information that must be included within the notification
- address the documentation that must be completed, provided, and/or executed with respect to notification, including the:
    - agent(s) responsible for completing, providing, and/or executing the documentation
    - agent(s) to whom this documentation must be provided
    - required content of the documentation

Determination of Whether a Privacy Breach Occurred

Upon notification of a **privacy breach**, the policy, procedures, and practices must require a determination to be made as to:

- whether a **privacy breach** has in fact occurred, and if so, what, if any, personal information has been breached
- the extent of the **privacy breach**
- whether the breach is a **privacy breach**, or an **information security breach**, or both
- the identification of the agent(s) responsible for making this determination

Prioritization Framework

The policy, procedures, and practices should include a prioritization framework based on risk that supports the systematic allocation of resources for addressing privacy breaches or suspected privacy breaches. Such a framework should include:

- specific criteria for determining the prioritization level for a particular **privacy breach** or suspected privacy breach at a given point in time, allowing for escalation or de-escalation in response to an evolving situation
- criteria that includes the consideration of factors, such as the:
    - potential impact of the **privacy breach**
    - recoverability from the **privacy breach** or suspected privacy breach
    - the extent to which personal information may be affected

Where a prioritization framework is included, the policy, procedures, and practices should identify the:

- agent(s) responsible for the prioritization framework
- agent(s) responsible for approving the prioritization framework
- procedures that must be followed, including any documentation that must be completed, provided, and/or executed by the agent(s) responsible for developing the prioritization framework and approving the prioritization framework
- agent(s) to whom this documentation must be provided
- required content of the documentation

Breach Notification to Senior Management

The policy, procedures, and practices must further address when and in what circumstances senior management, including the Chief Executive Officer or the Executive Director (or equivalent position), will be notified of a **privacy breach** or suspected privacy breach. This must include:

- identifying the agent(s) responsible for notifying senior management
- the timeframe within which notification must be provided

- the manner in which this notification must be provided
- the nature of the information that must be provided to senior management upon notification, including the level of detail that must be provided

Relationship to Policy, Procedures, and Practices for Information Security Breach Management

The policy, procedures, and practices must address the process to be followed in identifying, reporting, containing, notifying, investigating and remediating an event that is both a **privacy breach** or suspected privacy breach, as well as an **information security breach** or information security incident.

Containment

The policy, procedures, and practices must require that containment be initiated immediately and must identify the:

- agent(s) responsible for containment and the procedure that must be followed, including any documentation that must be completed, provided and/or executed by the agent(s) responsible for containing the breach
- required content of the documentation

In undertaking containment, the policy, procedures, and practices must ensure that reasonable steps are taken in the circumstances to protect personal information from further theft, loss, or unauthorized collection, use, or disclosure, and to protect records of personal information from further unauthorized copying, modification, or disposal. At a minimum, these steps must include ensuring that:

- no copies of the records of personal information have been made
- the records of personal information are either retrieved or disposed of in a secure manner

Where the records of personal information are securely disposed of, written confirmation should be obtained relating to the date, time, and method of secure disposal, as well as:

- assurance that additional **privacy breaches** cannot occur through the same means
- a determination of whether the **privacy breach** would allow unauthorized access to any other information
- if necessary, an acknowledgement of further actions being taken to prevent additional privacy breaches

The policy, procedures, and practices must also identify the:

- process to be followed in reviewing the containment measures implemented and determining whether the **privacy breach** has been effectively contained or whether further containment measures are necessary
- agent(s) responsible for reviewing the containment measures

- documentation that must be completed, provided, and/or executed in reviewing the containment measures
- agent(s) responsible for completing, providing, and/executing the documentation
- agent(s) to whom this documentation must be provided
- required content of the documentation

Breach Notification to Service Providers or Other Organizations

The policy, procedures, and practices must require the prescribed entity to notify, at the earliest reasonable opportunity, the service provider or other organization that disclosed the personal information to the prescribed entity whenever personal information has been or is believed to be stolen, lost or collected, used, or disclosed without authority, and whenever required pursuant to the agreement with the service provider or other organization.

In particular, the policy, procedures, and practices must set out the:

- agent(s) responsible for notifying the service provider or other person or organization
- format of the notification
- nature of the information that must be provided upon notification

At a minimum, the policy, procedures, and practices must require the service provider or other person or organization to be advised of:

- the extent of the **privacy breach**
- the nature of the personal information at issue
- the measures implemented to contain the **privacy breach**
- further actions that will be undertaken with respect to the **privacy breach**, including investigation and remediation

Breach Notification to the IPC

The policy, procedures, and practices must require the prescribed entity to notify the IPC immediately, in writing, if a researcher to whom the prescribed entity disclosed personal information notifies the prescribed entity of a breach that relates to the theft, loss, or unauthorized use or disclosure of personal information, as required by section 6(3) of O.Reg 191/18.

At a minimum, the policy and procedures must require the IPC to be advised of:

- the extent of the **privacy breach**
- the nature of the personal information at issue
- the measures implemented to contain the **privacy breach**
- further actions that will be undertaken with respect to the **privacy breach**, including investigation and remediation

The policy, procedures, and practices must also set out a process for determining whether the IPC, or any other persons or organizations must be notified of the **privacy breach** and must set out the:

- agent(s) responsible for providing such notification
- format of the notification
- nature of the information that must be provided upon notification
- timeframe for notification

The prescribed entity must notify the IPC, at the first reasonable opportunity, of privacy breaches in the circumstances set out in subsection 6(3) of the CYFSA's regulations, as if the prescribed entity were a service provider.

Breach Notification to Affected Individuals

However, as a secondary collector of personal information, a prescribed entity should not directly notify the individual to whom the personal information relates of a **privacy breach**. Where applicable, the required notification to individuals must be provided by the relevant service provider(s), unless an alternative decision regarding breach notification to affected individuals is approved by the IPC.

Investigation of Breach

The policy, procedures, and practices must further identify the:

- agent(s) responsible for investigating the **privacy breach**
- nature and scope of the investigation (i.e., document reviews, interviews, site visits, inspections)
- process that must be followed in investigating the **privacy breach**. This process must set out the:
    - documentation that must be completed, provided, and/or executed in undertaking the investigation
    - agent(s) responsible for completing, providing, and/or executing the documentation
    - agent(s) to whom this documentation must be provided
    - required content of the documentation

The policy, procedures, and practices must also identify the agent(s) responsible for:

- assigning other agent(s) to address the mitigations and any other relevant recommendations as required
- establishing timelines to address the mitigations and any other recommendations
- monitoring and ensuring the treatment of the mitigations and any other recommendations within the stated timelines

- evaluating the residual risks remaining after implementation

The policy, procedures, and practices must also set out the nature of the documentation that must be completed, provided, and/or executed at the conclusion of the investigation of the **privacy breach**, including the:

- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom the documentation must be provided
- required content of the documentation

Communication of Findings of Investigation and Recommendations

The policy, procedures, and practices must also address the manner, circumstances and format in which the findings, mitigations, and other recommendations of the investigation of the **privacy breach** are communicated, including the status of implementation of the recommendations. This must include identifying:

- the agent(s) responsible for communicating the findings of the investigation
- the mechanism and format for communicating the findings of the investigation, including the level of detail for communicating the findings
- the timeframe within which the findings of the investigation must be communicated
- to whom the findings of the investigation must be communicated, including whether the findings must be communicated to the Chief Executive Officer or the Executive Director (or equivalent position)

Tracking Privacy Breaches

The policy, procedures, and practices must:

- require that a log be maintained of privacy breaches
- identify the agent(s) responsible for maintaining the log and for tracking the findings, mitigations, or other relevant recommendations arising from the investigation of privacy breaches are addressed within the identified timelines
- address where documentation related to the identification, reporting, containment, notification, investigation, and remediation of privacy breaches will be retained
- identify the agent(s) responsible for retaining this documentation

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices

- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices In Respect of Privacy Audits***

31. Log of Privacy Breaches

A prescribed entity must maintain a log of **privacy breaches** and suspected privacy breaches. At a minimum, the log must set out:

- the date of the **privacy breach** or suspected privacy breach
- the date that the privacy breach was identified or suspected
- the nature of the personal information, if any, that was the subject matter of the privacy breach, and the nature and extent of the privacy breach or suspected privacy breach
- a description of the privacy breach or suspected privacy breach and who identified the privacy breach or suspected privacy breach
- the cause of the privacy breach or suspected privacy breach
- whether an unauthorized person who is not an agent or electronic service provider caused the privacy breach or suspected privacy breach, and the name or a description of the unauthorized person, if applicable
- the date that the Chief Executive Officer or Executive Director (or equivalent position) and senior management were notified of the privacy breach or suspected privacy breach, if applicable
- the date that the privacy breach or suspected privacy breach was contained and the nature of the containment measures
- the name of the agent(s) responsible for containing the privacy breach or suspected privacy breach
- the date that the investigation was commenced
- the date that the investigation was completed
- the agent(s) responsible for conducting the investigation
- the findings, mitigations, and other relevant recommendations arising from the investigation
- the agent(s) responsible for addressing each recommendation
- the manner in which each recommendation was or is expected to be addressed
- the date by which each recommendation was or is expected to be addressed

- the date that the Chief Executive Officer or Executive Director (or equivalent position) and senior management were notified of the findings, mitigations, and other relevant recommendations arising from the investigation, if applicable
- the date that the service provider or other organization that disclosed the personal information to the prescribed entity was notified, if applicable
- the date that notification was provided to the IPC, if applicable
- the date that notification was provided to individuals, if applicable

Privacy Complaints and Inquiries

32. Policy, Procedures, and Practices for Privacy Complaints

A policy, procedures, and practices must be developed and implemented to address the process to be followed in receiving, documenting, tracking, investigating, remediating, and responding to **privacy complaints**. A definition of the term "privacy complaint" must be provided that, at a minimum, includes concerns or complaints relating to the privacy policies, procedures, and practices implemented by the prescribed entity and related to the compliance of the prescribed entity with the CYFSA and its regulations.

The policy, procedures, and practices must identify the information that must be communicated to the public relating to the manner in which, to whom and where individuals may direct privacy concerns or complaints.

At a minimum, the following must be made publicly available:

- the name and/or title, mailing address, and contact information of the agent(s) to whom concerns or complaints may be directed
- information related to the manner in which and format in which privacy concerns or complaints may be directed to the prescribed entity
- information advising individuals that they may make a complaint to the IPC regarding the prescribed entity's compliance with the CYFSA and its regulations
- the mailing address and contact information for the IPC

Process for Receiving Complaints

The policy, procedures, and practices must further establish the process to be followed in receiving **privacy complaints**. This must include:

- any documentation that must be completed, provided and/or executed by the complainant
- the agent(s) responsible for receiving the privacy complaint
- the required content of the documentation, if any
- the nature of the information to be requested from the complainant

Determination of Whether to Investigate a Complaint

Upon receipt of a privacy complaint, the policy, procedures, and practices must require a determination to be made as to whether the privacy complaint will be investigated. The policy, procedures, and practices must identify the:

- agent(s) responsible for making this determination
- timeframe within which this determination must be made
- process that must be followed
- criteria that must be used in making the determination, including any documentation that must be completed, provided and/or executed
- required content of the documentation

Where Complaint Will Not Be Investigated

In the event that it is determined that an investigation will not be undertaken, the policy, procedures, and practices must require that a letter be provided to the complainant that includes:

- acknowledgement of receipt of the privacy complaint
- a response to the privacy complaint
- advising that an investigation of the privacy complaint will not be undertaken along with the rationale for the decision not to investigate
- advising the complainant that they may make a complaint to the IPC if there are reasonable grounds to believe that the prescribed entity has contravened or is about to contravene the CYFSA or its regulations
- the contact information for the IPC

Where Complaint Will Be Investigated

In the event that it is determined that an investigation will be undertaken, the policy, procedures, and practices must require that a letter be provided to the complainant that includes:

- an acknowledgement of receipt of the privacy complaint
- advising that an investigation of the privacy complaint will be undertaken
- an explanation of the privacy complaint investigation procedure
- an indication of whether the complainant will be contacted for further information concerning the privacy complaint
- the projected timeframe for completion of the investigation
- an identification of the nature of the documentation that will be provided to the complainant following the investigation

The policy, procedures, and practices must identify the agent(s) responsible for sending the above noted letters to complainants and the timeframe within which the letters will be sent to the individuals.

Where an investigation of a privacy complaint will be undertaken, the policy, procedures, and practices must identify the:

- agent(s) responsible for investigating the privacy complaint
- nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections)
- process that must be followed in investigating the privacy complaint
- documentation that must be completed, provided, and/or executed in undertaking the investigation, including the:
    - agent(s) responsible for completing, providing, and/or executing the documentation
    - agent(s) to whom this documentation must be provided
    - required content of the documentation

The policy, procedures, and practices must set out the process for addressing the mitigations and any other relevant recommendations arising from the investigation of **privacy complaints** and the agent(s) responsible for:

- assigning other agent(s) to address the mitigations and any other relevant recommendations
- establishing timelines to address the mitigations and any other recommendations
- monitoring and ensuring the treatment of the mitigations and any other relevant recommendations within the stated timelines
- evaluating the residual risks remaining after implementation

The policy, procedures, and practices must also set out the nature of the documentation that will be completed, provided, and/or executed at the conclusion of the investigation of the privacy complaint, including the:

- agent(s) responsible for completing, preparing, and/or executing the documentation
- agent(s) to whom the documentation must be provided
- required content of the documentation

The policy, procedures, and practices must also address the manner, circumstances, and format in which the findings of the investigation of the privacy complaint, including recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This must include:

- identifying the agent(s) responsible for communicating the findings of the investigation

- the mechanism and format for communicating the findings of the investigation, including the level of detail for communicating the findings
- the timeframe within which the findings of the investigation must be communicated
- to whom the findings must be communicated, including whether the findings must be communicated to the Chief Executive Officer or the Executive Director (or equivalent position)

The policy, procedures, and practices must further require the complainant to be notified, in writing, of:

- the nature and findings of the investigation and of the measures taken, if any, in response to their privacy complaint
- their right to make a complaint to the IPC if there are reasonable grounds to believe that the CYFSA or its regulations has been or is about to be contravened
- the contact information for the IPC

The policy, procedures, and practices must also identify the agent(s) responsible for providing the written notification to the complainant and the timeframe within which the written notification must be provided.

The policy, procedures, and practices should also address whether and in what circumstances:

- any other person or organization must be notified of **privacy complaints** and the results of the investigation of privacy complaints, and if so the:
    - manner and format in which notification must be provided
    - timeframe within which the notification must be provided
    - agent(s) responsible for providing the notification

Tracking Privacy Complaints

The policy, procedures, and practices must:

- require a log to be maintained of **privacy complaints**
- identify the agent(s) responsible for maintaining the log and for tracking the findings
- assess whether the mitigations and other relevant recommendations arising from the investigation of **privacy complaints** are addressed within the identified timelines
- specify where documentation related to the receipt, investigation, notification, and remediation of **privacy complaints** will be retained
- detail the agent(s) responsible for retaining the documentation

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

Relationship to Other Policies, Procedures and Practices

The relationship between this policy, procedures, and practices and the ***Policy, Procedures, and Practices for Privacy Breach Management*** must also be addressed.

This policy, procedures, and practices may either be a stand-alone document or may be combined with the ***Policy, Procedures, and Practices for Privacy Inquiries***.

33. Log of Privacy Complaints

A prescribed entity must maintain a log of **privacy complaints** received that, at a minimum, sets out:

- the date that the privacy complaint was received and the nature of the privacy complaint
- the determination as to whether the privacy complaint will be investigated and the date that the determination was made
- the agent(s) who made the determination as to whether the privacy complaint would be investigated
- where the determination was made that the privacy complaint will not be investigated, the date that the complainant was advised that the complaint will not be investigated and informed of their right to file their complaint with the IPC
- where the determination is made that the privacy complaint will be investigated:
    - the date that the complainant was advised that the complaint will be investigated
    - the agent(s) responsible for conducting the investigation
    - the dates that the investigation was commenced and completed
    - the findings and other relevant recommendations arising from the investigation

- the date that the Chief Executive Officer or Executive Director (or equivalent position) and senior management were notified of the findings and other relevant recommendations arising from the investigation, if applicable
- the agent(s) responsible for addressing each recommendation
- the date that each recommendation was or is expected to be addressed
- the manner in which each recommendation was or is expected to be addressed
- the date that the complainant was advised of the findings of the investigation, of the measures taken, if any, in response to the privacy complaint, and of their right to file their complaint with the IPC

34. Policy, Procedures, and Practices for Privacy Inquiries

A policy, procedures, and practices must be developed and implemented to address the process to be followed in receiving, documenting, tracking and responding to privacy inquiries. A definition of the term "privacy inquiry" must be provided that, at a minimum, includes inquiries relating to the privacy policies, procedures, and practices implemented by the prescribed entity and related to the compliance of the prescribed entity with the CYFSA and its regulations.

A prescribed entity must communicate to the public the manner in which, to whom, and where individuals may direct privacy inquiries. At a minimum, the information communicated to the public must include:

- the name and/or title, mailing address, and contact information of the agent(s) to whom privacy inquiries may be directed
- information relating to the manner in which privacy inquiries may be directed to the prescribed entity
- information as to where individuals may obtain further information about the privacy policies, procedures, and practices implemented by the prescribed entity

The policy, procedures, and practices must further establish the process to be followed in receiving and responding to privacy inquiries. This must include:

- the agent(s) responsible for receiving and responding to privacy inquiries
- the role of the agent(s) who have been delegated day-to-day authority to manage the privacy program and the information security program must also be identified
- any documentation that must be completed, provided, and/or executed
- the required content and format of the documentation the prescribed entity would issue in response to a privacy inquiry

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices In Respect of Privacy Audits***

Relationship to Policy, procedures, and practices for Privacy Complaints

This policy, procedures, and practices may either be a stand-alone document or may be combined with the ***Policy, Procedures, and Practices for Privacy Complaints***.

Part 2 – Additional Requirements

The detailed requirements under this part of the CYFSA Addendum are found in parts 2, 3, and 4 of **Appendix "B"** of the PHIPA Manual. These parts of the PHIPA Manual apply to prescribed entities under the CYFSA, subject to the following changes:

- references to "PHIPA" must be read as "the CYFSA"
- references to "personal health information" must be read as "personal information"
- references to "prescribed person or prescribed entity" or "PP or PE" must be read as "prescribed entity"
- references to "health information custodian" or "custodian" must be read as "service provider"
- special regard must be given to the breach notification requirements in section 6(3) of O. Reg 191/18

A prescribed entity must have the necessary policies, procedures, and practices in place to ensure compliance with **Appendix "B"** of the CYFSA Addendum, whether those policies, procedures, and practices are separate from or integrated with the prescribed entity's policies, procedures, and practices developed under the PHIPA Manual.

Appendix C: Privacy, Information Security, Human Resources, and Organizational Indicators

Part 1 – Privacy Indicators

Categories	Privacy Indicators
General Privacy Policies, Procedures and Practices	• The completion date of each review of each privacy policy, procedure and practice by the prescribed entity since the prior review of the IPC. • Whether amendments were made to existing privacy policies, procedures, and practices as a result of the review, and if so, a list of the amended privacy policies, procedures, and practices and, for each policy, procedure and practice amended, a brief description of the amendments made. • Whether new privacy policies, procedures, and practices were developed and implemented as a result of the review, and if so, a brief description of each of the policies, procedures, and practices developed and implemented. • The date that each amended and newly developed privacy policy, procedure and practice was communicated to agents and, for each amended and newly developed privacy policy, procedure and practice communicated to agents, the nature of the communication. • Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.
Collection of Personal Information and Data Holdings	• The number of data holdings containing personal information maintained by the prescribed entity. • The number of statements of purpose developed for data holdings containing personal information. • The number and a list of the statements of purpose for data holdings containing personal information that were reviewed since the prior review by the IPC. • Whether amendments were made to existing statements of purpose for data holdings containing personal information as a result of the review, and if so, a list of the amended statements of purpose and, for each statement of purpose amended, a brief description of the amendments made.

Categories	Privacy Indicators
Access and Use of Personal Information	• The number of agents granted approval to access and use personal information for purposes other than research since the prior review by the IPC. • The number of requests received for the use of personal information for research since the prior review by the IPC. • The number of requests for the use of personal information for research purposes that were granted and that were denied since the prior review by the IPC.
Disclosure of Personal Information for Research	• The number of requests received for the disclosure of personal information for research purposes since the prior review by the IPC. • The number of requests for the disclosure of personal information for research purposes that were granted and that were denied since the prior review by the IPC. • The number of **Research Agreements** executed with researchers to whom personal information was disclosed since the prior review by the IPC.
Disclosure of Personal Information for Purposes Other Than Research	• The number of requests received for the disclosure of personal information for purposes other than research since the prior review by the IPC. • The number of requests for the disclosure of personal information for purposes other than research that were granted and that were denied since the prior review by the IPC. • The number of **Data Sharing Agreements** executed for the collection of personal information by the prescribed entity since the prior review by the IPC. • The number of **Data Sharing Agreements** executed for the disclosure of personal information by the prescribed entity since the prior review by the IPC.
Data Linkage, De-Identification, and Aggregation	• The number and a list of data linkages of personal information approved since the prior review by the IPC. • The number of requests received for the disclosure of **de-identified and/or aggregate information** for both research and other purposes since the prior review by the IPC. • The number of acknowledgements or agreements executed by persons to whom **de-identified and/or aggregate information** was disclosed for both research and other purposes since the prior review by the IPC.
Third Party Service Provider Agreements	• The number of agreements executed with third party services providers with access to personal information since the prior review by the IPC.

Categories	Privacy Indicators

Privacy Impact Assessments	• The number and a list of privacy impact assessments completed since the prior review by the IPC and for each privacy impact assessment:
	  ○ the data holding, information system, technology or program
	  ○ the date of completion of the privacy impact assessment
	  ○ a brief description of each finding, mitigation or other recommendation
	  ○ the date each mitigation or other recommendation was addressed or is expected to be addressed
	  ○ the manner in which each mitigation or other recommendation was addressed or is expected to be addressed
	• The number and a list of privacy impact assessments undertaken but not completed since the prior review by the IPC and the proposed date of completion.
	• The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion.
	• The number of determinations made since the prior review by the IPC that a privacy impact assessment is not required and, for each determination, the data holding, information system, technology or program at issue and a brief description of the reasons for the determination.
	• The number and a list of privacy impact assessments reviewed since the prior review by the IPC and a brief description of any amendments made.

Privacy Audit Program	• The dates of audits of agents granted approval to access and use personal information since the prior review by the IPC and for each audit conducted:
	  ○ a brief description of each recommendation made
	  ○ the date each recommendation was addressed or is expected to be addressed
	  ○ the manner in which each recommendation was addressed or is expected to be addressed

Categories	Privacy Indicators
Privacy Audit Program (Cont'd)	• The number and a list of all other privacy audits completed since the prior review by the IPC and for each audit: ○ a description of the nature and type of audit conducted ○ the date of completion of the audit ○ a brief description of each recommendation made ○ the date each recommendation was addressed or is expected to be addressed ○ the manner in which each recommendation was addressed or is expected to be addressed
Privacy Breaches	• The total number of notifications of **privacy breaches** or suspected privacy breaches received by the prescribed entity since the prior review by the IPC. This indicator may be further subdivided to distinguish between privacy breaches that constitute: ○ a collection, use, or disclosure of personal information that is not in compliance with the CYFSA or its regulations ○ a contravention of the privacy policies, procedures or practices implemented by the prescribed entity, related to the requirements of the CYFSA Addendum ○ a contravention of written acknowledgments, **Data Sharing Agreements**, **Research Agreements**, **Confidentiality Agreements** and **TPSP Agreements**, related to the requirements of the CYFSA Addendum ○ circumstances where personal information is stolen, lost or collected, used or disclosed without authority or where records of personal information are subject to unauthorized copying, modification or disposal • With respect to each privacy breach or suspected privacy breach: ○ the date of the privacy breach or suspected privacy breach ○ the date that the privacy breach was identified or suspected ○ the nature of the personal information that was the subject matter of the privacy breach and the nature and extent of the privacy breach or suspected privacy breach ○ a description of the privacy breach or suspected privacy breach and who identified the privacy breach or suspected privacy breach, The cause of the privacy breach or suspected privacy breach ○ the date that the Chief Executive Officer or Executive Director (or equivalent position) and senior management was notified of the privacy breach or suspected privacy breach, if applicable

Categories	Privacy Indicators
Privacy Breaches (Cont'd)	○ whether an unauthorized person who is not an agent or electronic service provider caused the privacy breach or suspected privacy breach and the name or a description of the unauthorized person, if applicable ○ the containment measures implemented ○ the date(s) that the containment measures were implemented ○ the date(s) that notification was provided to the service providers or any other organizations ○ the date that the investigation was commenced ○ the date that the investigation was completed ○ a brief description of each finding, mitigation and any other recommendation made ○ the date that the Chief Executive Officer or Executive Director (or equivalent position) and senior management was notified of the findings, mitigations and other recommendations arising from the investigation, if applicable ○ the date each recommendation was addressed or is expected to be addressed ○ the manner in which each recommendation was addressed or is expected to be addressed ○ the date notification was provided to the IPC, if applicable ○ the date that notification was provided to individuals, if applicable
Privacy Complaints and Inquiries	• The number of **privacy complaints** received since the prior review by the IPC. • Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the IPC and with respect to each privacy complaint investigated: ○ the date that the privacy complaint was received ○ the nature of the privacy complaint ○ the date that the investigation was commenced ○ the date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation ○ the date that the investigation was completed ○ a brief description of each finding, mitigation and any other recommendation made

Categories	Privacy Indicators
Privacy Complaints and Inquiries (Cont'd)	○ the date the Chief Executive Officer or Executive Director (or equivalent position), and senior management were notified of the findings, mitigations and other recommendations arising from the investigation, if applicable ○ the date each recommendation was addressed or is expected to be addressed ○ the manner in which each recommendation was addressed or is expected to be addressed ○ the date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint • Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the IPC and with respect to each privacy complaint not investigated: ○ the date that the privacy complaint was received ○ the nature of the privacy complaint ○ the date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter

Part 2 – Information Security Indicators

Categories	Information Security Indicators
General Information Security Policies, Procedures and Practices	• The completion date of each review of each information security policy, procedure and practice by the prescribed entity since the prior review of the IPC. • Whether amendments were made to existing information security policies, procedures, and practices as a result of the review and, if so, a list of the amended information security policies, procedures, and practices and, for each policy, procedure and practice amended, a brief description of the amendments made. • Whether new information security policies, procedures, and practices were developed and implemented as a result of the review, and if so, a brief description of each of the policies, procedures, and practices developed and implemented. • The dates that each amended and newly developed information security policy, procedure and practice was communicated to agents and, for each amended and newly developed information security policy, procedure and practice communicated to agents, the nature of the communication. • Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.
Physical Security	• The dates of audits of agents granted approval to access the premises and locations within the premises where records of personal information are retained since the prior review by the IPC and for each audit: ○ a brief description of each recommendation made ○ the date each recommendation was addressed or is expected to be addressed ○ the manner in which each recommendation was addressed or is expected to be addressed
Information Security	• The number of instances in which the prescribed entity failed to conduct vulnerability scanning in accordance with the ***Policy, Procedures, and Practices for Vulnerability and Patch Management*** since the prior review by the IPC, and for each instance the: ○ time and date of the failure to conduct vulnerability scanning ○ nature of the failure ○ reason for the failure ○ time and date at which vulnerability scanning resumed

Categories	Information Security Indicators
Information Security (Cont'd)	• The number of instances in which any patches or other mitigation methods were not implemented within the required timelines to address risks rated with high severity or critical severity or for which a decision was made to not implement a patch or other mitigation method, and for each instance: ○ the severity level of the patch or other mitigation method ○ a description of the patch or other mitigation method ○ a brief description of the reason why the patch or other mitigation method was not implemented within the required time frame or why a decision was made to not implement the patch or other mitigation method
Information Security Audit Program	• The dates of the audits of the privacy and information security event logs since the prior review by the IPC and a general description of the findings, if any, arising from the audits of the privacy and information security event logs. • The number of instances in which the monitoring tools and mechanisms implemented by the prescribed entity were unavailable, unattended or there was otherwise a failure to monitor in accordance with the ***Policy, Procedures, and Practices for Logging, Monitoring and Auditing Privacy and Information Security Events*** since the prior review by the IPC, and for each instance the: ○ time and date of the monitoring failure ○ nature of the failure ○ reason for the failure ○ time and date at which monitoring resumed • The number of high vulnerabilities and the number of critical vulnerabilities identified by vulnerability assessments conducted on the results of vulnerability scans since the prior review by the IPC. • The number of instances in which recommendations to mitigate high or critical vulnerabilities identified by vulnerability assessments conducted on the results of vulnerability scans since the prior review by the IPC were not implemented in accordance with the required time frame and, if so, for each instance: ○ the risk severity of the vulnerability ○ a description of the vulnerability

Categories	Information Security Indicators
Information Security Audit Program (Cont'd)	○ a brief description of the reason why each recommendation to mitigate the vulnerability was not implemented in accordance with the time frame ○ the number of information security components within the information environment for which each recommendation was not implemented in accordance with the time frame • The number and a list of information security audits completed since the prior review by the IPC and for each audit: ○ a description of the nature and type of audit conducted ○ the date of completion of the audit ○ a brief description of each recommendation made ○ the date that each recommendation was addressed or is expected to be addressed ○ the manner in which each recommendation was addressed or is expected to be addressed
Information Security Breaches	• The total number of notifications of information security breaches or information security incidents received by the prescribed entity since the prior review by the IPC. This indicator may be further subdivided to distinguish between information security breaches that: ○ actually, or imminently jeopardize the confidentiality, integrity or availability of information or the information environment ○ constitute a contravention or imminent threat of contravention of the CYFSA or its regulations or ○ constitute a contravention or imminent threat of contravention of the terms of any written agreements, other legal obligations, or information security policies, procedures, and practices implemented by the prescribed entity, related to the requirements of the CYFSA Addendum • With respect to each information security breach or information security incident: ○ the date of the information security breach or information security incident ○ the date that the information security breach or information security incident was identified or suspected ○ the nature of the personal information, if any, that was the subject matter of the information security breach and the nature and extent of the information security breach ○ a description of the information security breach or information security incident and who identified the information security breach or information security incident

Categories	Information Security Indicators
Information Security Breaches (Cont'd)	○ the cause of the information security breach or information security incident ○ the date that Chief Executive Officer or Executive Director (or equivalent position) and senior management were notified of the information security breach or information security incident, if applicable ○ whether an unauthorized person who is not an agent or electronic service provider caused the information security breach or information security incident and the name or a description of the unauthorized person, if applicable ○ the containment measures implemented ○ the date(s) that the containment measures were implemented ○ the date(s) that notification was provided to the service providers or any other organizations ○ the date that the investigation was commenced ○ the date that the investigation was completed ○ a brief description of each finding, mitigation and any other recommendation made ○ the date that the Chief Executive Officer or Executive Director (or equivalent position) and senior management was notified of the findings, mitigations and other recommendations arising from the investigation, if applicable ○ the date each recommendation was addressed or is expected to be addressed ○ the manner in which each recommendation was addressed or is expected to be addressed ○ the date notification was provided to the IPC, if applicable ○ the date that notification was provided to individuals, if applicable

Part 3 – Human Resources Indicators

Categories	Human Resources Indicators
Privacy Training and Awareness	• The number of agents who have completed and who have not completed initial privacy training since the prior review by the IPC. • The date of commencement of the employment, contractual or other relationship for agents who have yet to complete initial privacy training and the scheduled date of the initial privacy training. • The number of agents who have completed and who have not completed ongoing privacy training each year since the prior review by the IPC. • The dates and number of communications to agents by the prescribed entity in relation to privacy since the prior review by the IPC and a brief description of each communication.
Information Security Training and Awareness	• The number of agents who have completed and who have not completed initial information security training since the prior review by the IPC. • The date of commencement of the employment, contractual or other relationship for agents who have yet to complete initial information security training and the scheduled date of the initial information security training. • The number of agents who have completed and who have not completed ongoing information security training each year since the prior review by the IPC. • The dates and number of communications to agents by the prescribed entity in relation to information security since the prior review by the IPC.
Confidentiality Agreements	• The number of agents who have executed and who have not executed **Confidentiality Agreements** each year since the prior review by the IPC. • The date of commencement of the employment, contractual or other relationship for agents who have yet to execute the Confidentiality Agreement and the date by which the Confidentiality Agreement must be executed.
Termination or Cessation	• The number of notifications received from agents since the prior review by the IPC related to termination or cessation of their employment, contractual or other relationship with the prescribed entity.

Part 4 – Organizational Indicators

Categories	Organizational Indicators
Risk Management	• The dates that the corporate risk register was reviewed by the prescribed entity since the prior review by the IPC. • Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.
Business Continuity and Disaster Recovery	• The dates that the business continuity and disaster recovery plan was tested since the prior review by the IPC. • Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made.

Appendix D: Initial Review Sworn Affidavit

I, [INSERT NAME], of the City of [INSERT CITY NAME], in the province of Ontario, MAKE OATH AND SAY:

1. I am [INSERT POSITION TITLE] at [INSERT NAME OF PRESCRIBED ENTITY] and, as such, have knowledge of the matters to which I hereinafter depose. In swearing this affidavit, I have exercised care and diligence that would reasonably be expected of a/an [INSERT POSITION TITLE] in these circumstances, including making due inquiries of staff and agents of [INSERT NAME OF PRESCRIBED ENTITY] who have more direct knowledge of the relevant matters.

2. [INSERT NAME OF PRESCRIBED ENTITY] has policies, procedures, and practices in place to comply with "Part 2 – Additional Requirements" of Appendix "B" of the *Child, Youth and Family Services Act Addendum to the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* that has been published by the Information and Privacy Commissioner of Ontario, as it may be amended from time to time, and subject to any:

a. Statements of Requested Exceptions attached hereto as Exhibit A, and
b. Statements of Inapplicability attached hereto as Exhibit B.

SWORN (OR AFFIRMED) BEFORE ME)

at the City/Town/Etc. of _____ , in the)

County/Regional Municipality/Etc. of _____)

_____ , on _____ 20 _____)

_____
SIGNATURE OF DEPONENT

_____
Commissioner for Taking Affidavits

Appendix E: Three–Year Review Sworn Affidavit

I, [INSERT NAME], of the City of [INSERT CITY NAME], in the province of Ontario, MAKE OATH AND SAY:

1. I am [INSERT POSITION TITLE] at [INSERT NAME OF PRESCRIBED ENTITY] and, as such, have knowledge of the matters to which I hereinafter depose. In swearing this affidavit, I have exercised care and diligence that would reasonably be expected of a/an [INSERT POSITION TITLE] in these circumstances, including making due inquiries of staff and agents of [INSERT NAME OF PRESCRIBED ENTITY] who have more direct knowledge of the relevant matters.

2. [INSERT NAME OF PRESCRIBED ENTITY] has in place policies, procedures, and practices to protect the privacy of individuals whose personal information is received and to maintain the confidentiality of that information in accordance with its obligations under the *Child, Youth and Family Services Act, 2017* and the regulations thereto, as may be amended from time to time.

3. The policies, procedures, and practices implemented by [INSERT NAME OF PRESCRIBED ENTITY] comply with the *Child, Youth and Family Services Act Addendum to the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* that has been published by the Information and Privacy Commissioner of Ontario, as it may be amended from time to time, and subject to any:

a. Statements of Requested Exceptions attached hereto as Exhibit A, and
b. Statements of Inapplicability attached hereto as Exhibit B.

4. Attached hereto as Exhibit C are the Privacy, Information Security, Human Resources and Organizational indicators of [INSERT NAME OF PRESCRIBED ENTITY] in compliance with the *Child, Youth and Family Services Act Addendum to the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

5. [INSERT NAME OF PRESCRIBED ENTITY] has taken steps that are reasonable in the circumstances to ensure compliance with the policies, procedures, and practices implemented and to ensure that the personal information it receives is protected against theft, loss and unauthorized collection, use or disclosure and to ensure that records containing personal information are protected against unauthorized copying, modification or disposal.

SWORN (OR AFFIRMED) BEFORE ME)

at the City/Town/Etc. of _____ , in the)

County/Regional Municipality/Etc. of _____)

_____ , on _____ 20 _____)

_____

SIGNATURE OF DEPONENT

_____

Commissioner for Taking Affidavits

Appendix F: Glossary

Term	Definition
Agent	Means a person that, with the authorization of the prescribed entity, acts for or on behalf of the prescribed entity in respect of personal information for the purposes of the prescribed entity, and not the agent's own purposes, whether or not the agent has the authority to bind the prescribed entity, whether or not the agent is employed by the prescribed entity and whether or not the agent is being remunerated.
Certificate of Destruction	A certificate that evidences the destruction of records of PI that must, at a minimum: • identify the records of PI securely disposed of • stipulate the date, time, location and method of secure disposal employed • bear the name and signature of the person who performed the secure disposal
Confidentiality Agreement	An agreement that is executed between a prescribed entity and each of its Agents in accordance with the ***Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Agents*** and the ***Template Confidentiality Agreement with Agents***.
CYFSA	Refers to the *Child, Youth and Family Services Act*.
CYFSA Addendum	Refers to this document.
Data Sharing Agreement	An agreement that is executed between a prescribed entity and another party in accordance with the ***Policy, Procedures, and Practices for the Execution of Data Sharing Agreements*** and the ***Template Data Sharing Agreement***.
De-identified and/or Aggregate Information	In relation to the PI of an individual, means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual, and "de-identification" has a corresponding meaning.
Electronic service providers	An electronic service provider (ESP) is a person who supplies services that enable a prescribed entity to collect, use, modify, disclose, retain or dispose of PI electronically.
FIPPA	Refers to the *Freedom of Information and Protection of Privacy Act*.
Identifying Information	Includes information that identifies an individual or for which it is reasonably foreseeable that it could be used, either alone or with other information, to identify an individual.

Term	Definition
Information Environment	The networks, information systems, technologies, applications, software, servers, components, and configurations that enable the collection, use, and disclosure of PI in the custody or control of a prescribed entity, and work to keep the PI secure.
Information Security Breach	An occurrence that, at a minimum: • actually, or imminently, jeopardizes the confidentiality, integrity or availability of information or the information environment or • constitutes a contravention or imminent threat of contravention of the CYFSA or its regulations, the terms of any written agreements, other legal obligations, or information security policies, procedures, and practices implemented by the prescribed entity
Information Security Component	Any individual network, information system, technology, application, software, server or configuration within the information environment.
IPC	Refers to the Information and Privacy Commissioner of Ontario.
Personal Information	Personal information within the meaning section 2 of FIPPA.
Prescribed Entity	Entities prescribed for the purposes of subsection 293 of the CYFSA and that are prescribed in subsection 1 of O.Reg 191/18 (the “regulations”).
Privacy Breach	An occurrence that, at a minimum, includes: • the collection, use, and disclosure of PI that is not in compliance with the CYFSA and its regulations • a contravention of the privacy policies, procedures or practices implemented by the prescribed entity • a contravention of written acknowledgments, Data Sharing Agreements, Research Agreements, Confidentiality Agreements and TPSP Agreements or • circumstances where PI is stolen, lost or collected, used or disclosed without authority or where records of PI are subject to unauthorized copying, modification or disposal
Privacy Complaint	At a minimum, includes concerns or complaints relating to the privacy policies, procedures, and practices implemented by the prescribed entity and related to the compliance of the prescribed entity with the CYFSA and its regulations.
Regulations	Regulation 191/18 to the CYFSA as well as any other regulations that may be enacted under the CYFSA from time to time.
Research Agreement	An agreement between the prescribed entity and researchers to whom PI will be disclosed under section 6(2)(b) of the regulation to the CYFSA. The research agreement is executed prior to the disclosure of PI.

Term	Definition
Research Plan	A research plan sets out in writing the intentions of a researcher in conducting planned research in accordance with the CYFSA and its regulations.
Service Provider	A service provider has the same meaning as it does under sections 2 and 281 of the CYFSA.
Statement of Requested Exceptions	A prescribed entity must submit a written Statement of Requested Exceptions to the IPC if compliance with the requirements in **Appendix "A"** or **Appendix "B"** of the CYFSA Addendum has not been achieved, is not expected to be achieved or will no longer be achieved. The Statement of Requested Exceptions must be attached as an exhibit to the sworn affidavit and include a rationale for each requirement not achieved or not expected to be achieved as of the date of the submission.
Statement of Inapplicability	A prescribed entity must submit a written Statement of Inapplicability where one or more of the requirements in Appendix "A" or Appendix "B" is inapplicable to a prescribed entity. Statements of Inapplicability must be attached as an exhibit to the sworn affidavit and must identify each requirement of the CYFSA Addendum that is inapplicable and provide the IPC with a rationale for the identified inapplicability.
Third Party Service Provider (TPSP)	A third-party service provider (TPSP) contracted or otherwise engaged to provide services to or for the prescribed entity.
TPSP Agreement	An agreement executed between the prescribed entity and a TPSP in accordance with the ***Policy, Procedures, and Practices for Executing Agreements with Third Party Service Providers in Respect of Personal Information*** and the ***Template Agreement for Third Party Service Providers***.

Child, Youth and Family Services Act Addendum to the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities

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

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

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

June 2024