CHILD, YOUTH AND FAMILY SERVICES

APRIL 2020

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 UNDER THE *CHILD, YOUTH AND FAMILY SERVICES ACT*

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*. The entities prescribed under section 293 of the *CYFSA* are set out in section 1 of Regulation 191/18 to the *CYFSA* (the "regulation").

These disclosures are permitted provided that the prescribed entities comply with the requirements set out in the *CYFSA* and its regulation.

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 and procedures") approved by the Information and Privacy Commissioner of Ontario ("IPC") to protect the privacy of individuals whose personal information is received and to maintain the confidentiality of that information.

These policies 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 regulation. 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 policies and procedures implemented by persons and entities prescribed under *PHIPA*. These policies and procedures are implemented to protect the privacy of individuals whose personal health information the prescribed persons and prescribed entities receive and to maintain the confidentiality of that information. The *PHIPA* Manual also sets out obligations imposed on prescribed entities under *PHIPA*.

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 policies 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 policies and procedures implemented by prescribed entities when collecting, using, or disclosing personal health information under *PHIPA*.

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*.

REVIEW PROCESS FOR PRESCRIBED ENTITIES

Each prescribed entity will be required to have in place policies and procedures to protect the privacy of individuals whose personal information is received under the *CYFSA* and to maintain the confidentiality of that information. At a minimum, these policies and procedures must include the policies, procedures, agreements, and documentation set out in Appendix "A" and must contain the minimum content set out in Appendix "B."

The process that will be followed by the IPC in conducting its review will depend on whether the review relates to the initial review of the policies and procedures implemented by the prescribed entity or relates to the ongoing review of these policies and procedures, 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* must submit the following to the IPC:

- The policies and procedures described in Appendix "A" and containing the minimum content set out in "Part 1 – Privacy Documentation" of Appendix "B" to the *CYFSA* Addendum.
- A sworn affidavit in the form set out in Appendix "D" regarding the policies and procedures required under "Part 2 – Additional Requirements" of Appendix "B" to the *CYFSA* Addendum.
- A random selection specified by the IPC of the policies and procedures required under "Part 2 – Additional Requirements" of Appendix "B" to the *CYFSA* Addendum.

The policies, procedures, and sworn affidavit must be submitted to the IPC on a date to be determined by the IPC in consultation with the prescribed entity.

Upon receipt, the IPC will review the policies and procedures implemented by the prescribed entity and will request any additional documentation and clarifications deemed necessary.

Once any additional documentation and necessary clarifications are received, the IPC may schedule an on-site meeting with representatives of the prescribed entity to discuss the policies and procedures and to ask questions arising from the review.

Following the review, the prescribed entity will be informed of the actions that are required to be taken by the prescribed entity prior to the approval of its policies and procedures. Once all necessary actions have been taken, the IPC will prepare a draft report and submit the draft report to the prescribed entity for review and comment prior to the report being finalized. Once the report is finalized, it will be posted on the IPC's website, along with a letter of approval. The prescribed entity will also be required to post the report and letter of approval on its website.

A person or organization may not operate as a prescribed entity unless it has submitted its policies and procedures to the IPC and the IPC has reviewed and approved these policies and procedures and has issued a letter and accompanying report to this effect.

THREE-YEAR REVIEW OF THE PRESCRIBED ENTITIES

Following the initial approval, the IPC will conduct reviews of the policies and procedures every three years. Each prescribed entity seeking the continued approval of the policies and procedures must submit a detailed written report and sworn affidavit to the IPC one year prior to the date that the continued approval is required.

The written report must demonstrate that the prescribed entity has developed and implemented policies and procedures to protect the privacy of individuals whose personal information is received and to maintain the confidentiality of that information, including the policies and procedures set out in Appendix "A," and is adhering to these policies and procedures. It must also demonstrate that these policies and procedures, at a minimum, contain the content set out in Appendix "B."

If compliance with the requirements in Appendix "A" or Appendix "B" has not been achieved, the written report must provide a rationale for why compliance has not been achieved and must outline a strategy for achieving compliance. The strategy must set out the milestones for achieving compliance, the relevant time frames for achieving compliance, and the individual(s) responsible for achieving compliance.

If, in the opinion of the prescribed entity, there is a clear rationale for not complying with one or more of the requirements in Appendix "A" or Appendix "B," this must be identified in the written report. The written report must also provide detailed information in support of this opinion. For example, if a prescribed entity does not use personal information for research purposes, the prescribed entity would not be required to implement policies and procedures with respect to the use of personal information for research purposes or a log of approved uses of personal information for research purposes.

The written report must also report on, provide information concerning, and assess the performance of the prescribed entity with respect to each of the privacy, security, and other indicators set out in Appendix "C."

The sworn affidavit must be in the form set out in Appendix "E" and must be executed by the Chief Executive Officer or the Executive Director, as the case may be, who is ultimately accountable for ensuring that the prescribed entity complies with the *CYFSA*. The sworn affidavit requires the Chief Executive Officer or the Executive Director, among other things, to attest that the policies and procedures of the prescribed entity comply with the *CYFSA* and its regulation and with the requirements in this Addendum, and that the prescribed entity has taken steps that are reasonable in the circumstances to ensure compliance with the policies and procedures that it has implemented.

Upon receipt, the IPC will review the written report and accompanying sworn affidavit and decide, in its sole and absolute discretion, whether further action is required on the part of the prescribed entity. The further action may include one or more of the following:

- a full detailed review by the IPC of all the policies and procedures implemented by the prescribed entity;
- a partial detailed review by the IPC of one or more of the policies and procedures implemented by the prescribed entity;
- a request for further information from the prescribed entity with respect to one, more, or all of its policies and procedures;
- an on-site meeting between the IPC and representatives of the prescribed entity;
- requiring the prescribed entity to amend, implement, or adhere to one or more of its policies and procedures or to develop and implement one or more additional policies or procedures;
- requiring the prescribed entity to amend the written report or sworn affidavit submitted; and/or
- any other action by the prescribed entity deemed appropriate in the sole and absolute discretion of the IPC.

If further action is warranted, the prescribed entity will be informed of the further action(s) it is required to take prior to the continued approval of its policies and procedures. The prescribed entity must comply with such further action(s) as required by the IPC in order to obtain continued approval.

Provided all further actions have been taken in a timely manner and to the satisfaction of the IPC, or in the event that no further action is warranted, the IPC will advise the prescribed entity, in writing, that it continues to meet the requirements of the *CYFSA* and its regulation. This is subject to any further actions that the IPC may require the prescribed entity to take prior to the next scheduled review of its policies and procedures.

The IPC will then make the letter advising the prescribed entity that it continues to meet the requirements of the *CYFSA* and its regulation, and the detailed written report and sworn affidavit submitted by the prescribed entity, publicly available on its website at www.ipc.on.ca. The prescribed entity will also be required to make this documentation publicly available on its website.

A person or organization may not continue to operate as a prescribed entity unless it has submitted a detailed written report and accompanying sworn affidavit to the IPC and the IPC has advised the prescribed entity, in writing, that it continues to meet the requirements of the *CYFSA* and its regulation.

OVERVIEW OF THE *CYFSA* ADDENDUM

Prescribed entities must develop policies and procedures in accordance with "Part 1 – Privacy Documentation" of Appendix "B" that are separate from the prescribed entity's policies and procedures developed under the *PHIPA* Manual.

Separate *CYFSA* policies and procedures may not be necessary under "Part 2 – Additional Requirements" of Appendix "B" to the *CYFSA* Addendum, as its requirements correspond with those set out in parts 2, 3, and 4 of Appendix "B" of the *PHIPA* Manual. Instead, a prescribed entity may create *CYFSA* addenda to policies and procedures developed in accordance with parts 2, 3, and 4 of Appendix "B" of the *PHIPA* Manual.

Whichever approach is taken, a prescribed entity must have the necessary policies and procedures in place to ensure compliance.

DEFINITIONS

- **Addendum** refers to this document
- **Agent** means a person that acts for or on behalf of a prescribed entity, service provider, or other organization and includes an employee of a prescribed entity, service provider, or other organization
- ***CYFSA*** refers to the *Child, Youth and Family Services Act*
- ***FIPPA*** refers to the *Freedom of Information and Protection of Privacy Act*
- **IPC** refers to the Information and Privacy Commissioner of Ontario
- **Personal information** has the same meaning as it does under *FIPPA*
- ***PHIPA*** refers to the *Personal Health Information Protection Act*
- ***PHIPA* Manual** refers to the IPC *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*
- **Policy and procedures** include policies, procedures, and practices unless specified otherwise
- **Regulation** refers to Ontario Regulation 191/18 to the *CYFSA*
- **Research Agreement** refers to a research agreement under section 6(2)(b) of the regulation to the *CYFSA* between a prescribed entity and a researcher
- **Service provider** has the same meaning as it does under sections 2 and 281 of the *CYFSA*

APPENDIX "A"

LIST OF REQUIRED DOCUMENTATION

PART 1 - PRIVACY DOCUMENTATION

Categories	Required Documentation	Page No. Appendix "B"
General Privacy Policies and Procedures	1. Privacy policy in respect of its status as a prescribed entity	8
	2. Policy and procedures for ongoing review of privacy policies and procedures	10
Transparency	3. Policy on the transparency of privacy policies and procedures	11
Collection of Personal Information	4. Policy and procedures for the collection of personal information	12
	5. Policy and procedures for the segregation of personal information	14
	6. List of data holdings containing personal information	14
	7. Policy and procedures for statements of purpose for data holdings containing personal information	14
	8. Statements of purpose for data holdings containing personal information	15
Use of Personal Information	9. Policy and procedures for limiting agent access to and use of personal information	15
	10. Log of agents granted approval to access and use personal information	18
	11. Policy and procedures for the use of personal information for research	18
	12. Log of approved uses of personal information for research	22
Disclosure of Personal Information	13. Policy and procedures for disclosure of personal information for purposes other than research	23
	14. Policy and procedures for disclosure of personal information for research purposes and the execution of research agreements	26
	15. Template research agreement	29
	16. Log of research agreements	32

Categories	Required Documentation	Page No. Appendix "B"
Data Sharing Agreements	17. Policy and procedures for the execution of data sharing agreements	33
	18. Template data sharing agreement	34
	19. Log of data sharing agreements	36
Agreements with Third Party Service Providers	20. Policy and procedures for executing agreements with third party service providers in respect of personal information	37
	21. Template agreement for all third party service providers	38
	22. Log of agreements with third party service providers	42
Data Linkage and Data De-Identification	23. Policy and procedures for the linkage of records of personal information	42
	24. Log of approved linkages of records of personal information	44
	25. Policy and procedures with respect to de-identification and aggregation	45
Privacy Impact Assessments	26. Privacy impact assessment policy and procedures	46
	27. Log of privacy impact assessments	48
Privacy Audit Program	28. Policy and procedures in respect of privacy audits	48
	29. Log of privacy audits	49
Privacy Breaches, Inquiries, and Complaints	30. Policy and procedures for privacy breach management	50
	31. Log of privacy breaches	52
	32. Policy and procedures for privacy complaints	53
	33. Log of privacy complaints	55
	34. Policy and procedures for privacy inquiries	56

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 DOCUMENTATION

PART 1 - PRIVACY DOCUMENTATION

1. PRIVACY POLICY IN RESPECT OF ITS STATUS AS A PRESCRIBED ENTITY

An overarching privacy policy, or equivalent, must be developed and implemented in relation to personal information received by the organization as a prescribed entity under the *CYFSA* ("the Privacy Policy"). At a minimum, the Privacy Policy must address the matters outlined below.

STATUS UNDER THE *CYFSA*

The Privacy Policy must describe the status of the organization as a 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 and procedures to protect the privacy of individuals whose personal information it receives and to maintain the confidentiality of that information, and that these policies and procedures 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 *CYFSA* and its regulation.

PRIVACY AND SECURITY ACCOUNTABILITY FRAMEWORK

The accountability framework for ensuring compliance with the *CYFSA* and its regulation and for ensuring compliance with the privacy and security policies and procedures implemented by the prescribed entity must also be articulated. In particular, the Privacy Policy must indicate that the Chief Executive Officer or the Executive Director, as the case may be, is ultimately accountable for ensuring compliance with the *CYFSA* and its regulation and for ensuring compliance with the privacy and security policies and procedures implemented.

The Privacy Policy must also identify the position(s) that have been delegated day-to-day authority to manage the privacy program and the security program and to whom these positions report. It must further identify the duties and responsibilities of the position(s) that have been delegated day-to-day authority to manage the privacy program and the security program and some of the key activities of these programs. The Privacy Policy should also identify other positions or committees that support the privacy program and/or the security program and their role in respect of these programs.

COLLECTION OF PERSONAL INFORMATION

The Privacy Policy must identify the specific purposes for which personal information is collected, the types of personal information collected, and the service providers and any other persons or organizations from which personal information is typically collected under the *CYFSA*. In identifying the purposes for which personal information is collected, the prescribed entity must ensure that each collection identified in the Privacy Policy is consistent with the collections of personal information permitted by the *CYFSA* and its regulation.

The Privacy Policy must also 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. In this regard, the Privacy Policy must outline the policies and procedures 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.

The Privacy Policy must also contain a list of the data holdings of personal information maintained by the prescribed entity and must identify where an individual may obtain further information in relation to the purposes, data elements, and data sources for each data holding of personal information.

USE OF PERSONAL INFORMATION

The specific purposes for which the prescribed entity uses personal information must be identified. In identifying these purposes, the prescribed entity must clearly distinguish between the use of personal information and the use of de-identified and/or aggregate information. The prescribed entity must also 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 the regulation. The prescribed entity must also ensure that each use of personal information identified in the Privacy Policy is consistent with the uses of personal information permitted by the *CYFSA* and its regulation.

The Privacy Policy must further 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 and must identify some of the policies and procedures implemented by the prescribed entity in this regard, including limits on the use of personal information by agents.

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

DISCLOSURE OF PERSONAL INFORMATION

The Privacy Policy must identify the 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. The prescribed entity must ensure that each disclosure identified in the Privacy Policy is consistent with the disclosures of personal information permitted by the *CYFSA* and its regulation.

The Privacy Policy must also clearly distinguish between the purposes for which and the circumstances in which personal information is disclosed and the circumstances in which and the purposes for which de-identified and/or aggregate information is disclosed. It must further indicate that the prescribed entity will review all de-identified and/or aggregate information prior to its disclosure in order 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.

Additionally, the Privacy Policy 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 and must identify some of the policies and procedures implemented by the prescribed entity in this regard.

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, and the secure manner in which they are retained. It must also address the manner in which records of personal information in both electronic and paper 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 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 is required to identify the agent(s) to whom and the manner in which individuals may direct inquiries, concerns, or complaints related to the privacy policies and procedures of the prescribed entity and related to the compliance of the prescribed entity with the *CYFSA* and its regulation.

The information provided 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 and the manner and format in which these inquiries, concerns, or complaints may be made. It should also state that individuals may direct complaints regarding the compliance of a prescribed entity with section 293 of the *CYFSA* and its regulation to the IPC and provide the IPC's mailing address and contact information.

TRANSPARENCY OF PRACTICES IN RESPECT OF PERSONAL INFORMATION

The Privacy Policy must identify where individuals may obtain further information in relation to the privacy policies and procedures of the prescribed entity.

2. POLICY AND PROCEDURES FOR ONGOING REVIEW OF PRIVACY POLICIES AND PROCEDURES

A policy and associated procedures must be developed and implemented for the ongoing review of the privacy policies and procedures put in place by the prescribed entity. The purpose of the review is to determine whether amendments are needed or whether new privacy policies and procedures are required.

The policy and procedures must identify the frequency of the review, the agent(s) responsible for undertaking the review, the procedure to be followed in undertaking the review, and the time frame in which the review will be undertaken. At a minimum, the privacy policies and procedures implemented by the prescribed entity must be reviewed on an annual basis. The policy and procedures must also identify the agent(s) responsible and the procedure to be followed in amending and/or drafting new privacy policies and procedures if deemed necessary as a result of the review, and the agent(s) responsible and the procedure that must be followed in obtaining approval of any amended or newly developed privacy policies and procedures.

In undertaking the review and determining whether amendments and/or new privacy policies and procedures are necessary, the prescribed entity must have regard to any orders, guidelines, fact sheets, and best practices issued by the IPC under the *CYFSA* and its regulation; evolving industry privacy standards and best practices; amendments to the *CYFSA* and its regulation relevant to the prescribed entity; and

recommendations arising from privacy and security audits, privacy impact assessments, and investigations into privacy complaints, privacy breaches, and information security breaches. Helpful guidance may also be found in other IPC orders, reports, and decisions.

The policy and procedures must also take into account whether the privacy policies and procedures of the prescribed entity continue to be consistent with its actual practices and whether there is consistency between and among the privacy and security policies and procedures implemented.

The policy and its associated procedures must further identify the agent(s) responsible and the procedure to be followed in communicating the amended or newly developed privacy policies and procedures, including the method and nature of the communication. It shall also identify the agent(s) responsible for and the procedure to be followed in reviewing and amending the communication materials available to the public and other stakeholders as a result of the amended or newly developed privacy policies and procedures.

The prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

3. POLICY ON THE TRANSPARENCY OF PRIVACY POLICIES AND PROCEDURES

A policy must be developed and implemented that identifies the information made available to the public and other stakeholders relating to the privacy policies and procedures implemented by the prescribed entity and that identifies the means by which such information is made available. At a minimum, the policy must require the prescribed entity to make the following information available:

- its Privacy Policy;
- brochures or frequently asked questions related to the privacy policies and procedures implemented by the prescribed entity;
- documentation related to the review by the IPC of the policies and procedures;
- a list of the data holdings of personal information maintained by the prescribed entity; and
- the name and/or title, mailing address, and contact information of the agent(s) to whom inquiries, concerns, or complaints regarding compliance with the privacy policies and procedures implemented and regarding compliance with the *CYFSA* and its regulation may be directed.

We recommend that privacy impact assessments or a summary of the privacy impact assessments conducted also be made available.

The policy must also set out the minimum content of the brochures or frequently asked questions described above. In particular, the brochures or frequently asked questions must describe the status of the prescribed entity under the *CYFSA*, the duties and responsibilities arising from this status, and the privacy policies and procedures implemented in respect of personal information, including:

- the types of personal information collected from service providers;
- the specific purposes for which the personal information is collected;
- the specific purposes for which the personal information is used, and if identifiable information is not routinely used, the nature of the information that is used;
- 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 processes used to link the personal information; and
- the circumstances in which and the specific purposes for which the personal information is disclosed and the persons or organizations to which it is typically disclosed.

The brochures or frequently asked questions must also 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 use or disclosure and to protect records of personal information against unauthorized copying, modification, or disposal.

We also recommend that the brochures or frequently asked questions provide the name and/or title, mailing address, and contact information of the agent(s) to whom inquiries, concerns, or complaints regarding compliance with the privacy policies and procedures, and compliance with the *CYFSA* and its regulation, may be directed.

4. POLICY AND PROCEDURES FOR THE COLLECTION OF PERSONAL INFORMATION

A policy and procedures 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, and the secure manner in which the personal information will be collected.

The policy and procedures must articulate a commitment by the prescribed entity not to collect personal information unless the collection is permitted by the *CYFSA* and its regulation, 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.

The prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

REVIEW AND APPROVAL PROCESS

The policy and procedures must identify the agent(s) responsible for reviewing and determining whether to approve the collection of personal information and the process that must be followed and the requirements that must be satisfied in this regard.

The policy and procedures must further set out the criteria that must be considered by the agent(s) responsible for determining whether to approve the collection of personal information. At a minimum, the criteria must require the agent(s) responsible for determining whether to approve the collection of personal information to ensure that the collection is permitted by the *CYFSA* and its regulation and that any and all conditions or restrictions set out in the *CYFSA* and its regulation have been satisfied.

The criteria must also require the agent(s) responsible for determining whether to approve the collection of personal information to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose and that no more personal information is collected from service providers and retained by the prescribed entity than is reasonably necessary to meet the identified purpose.

The policy and procedures should also set out the manner in which the decision approving or denying the collection of personal information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

CONDITIONS OR RESTRICTIONS ON THE APPROVAL

The policy and procedures must identify the conditions or restrictions that are required to be satisfied prior to the collection of personal information, 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. The conditions or restrictions identified in the policy and procedures, including the documentation and agreements that must be completed, provided, or executed, shall have regard to the requirements of the *CYFSA* and its regulation.

The policy and procedures must also identify the agent(s) responsible for ensuring that any conditions or restrictions have, in fact been satisfied.

SECURE RETENTION

The policy and procedures must require that the records of personal information collected by the prescribed entity be retained in a secure manner in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Information*.

SECURE TRANSFER

If the personal information is being collected by an agent of the prescribed entity, such as a chart abstractor, the policy and procedures shall require the records of personal information to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Information*.

SECURE RETURN OR DISPOSAL

The policy and procedures must identify 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 to be returned to the service provider, the policy and procedures must require the records to be transferred in a secure manner and in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Information*. If the records are to be disposed of, the policy and procedures must require the records to be disposed of in a secure manner and in compliance with the *Policy and Procedures for Secure Disposal of Records of Personal Information.*

5. POLICY AND PROCEDURES FOR THE SEGREGATION OF PERSONAL INFORMATION

A policy and procedures must be developed and implemented with respect to the segregation of personal information collected from service providers under the *CYFSA*. The policy and procedures 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 policy and procedures must also set out 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.

The prescribed entity shall require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

6. LIST OF DATA HOLDINGS CONTAINING PERSONAL INFORMATION

The prescribed entity shall 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 AND PROCEDURES FOR STATEMENTS OF PURPOSE FOR DATA HOLDINGS CONTAINING PERSONAL INFORMATION

A policy and procedures 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 and procedures shall require the statements of purpose to set out 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, and the need for the personal information in relation to the identified purpose.

The policy and procedures must also identify the agent(s) responsible and the process that must be followed in completing the statements of purpose, including the agent(s) or other persons or organizations that must be consulted in completing the statements of purpose and the agent(s) responsible for approving the statements of purpose. The 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 shall also be specified.

The persons and organizations that will be provided with the statements of purpose shall also be identified. At a minimum, this should include the service providers that provided the personal information.

The policy and procedures shall further require that the statements of purpose be reviewed on an ongoing basis in order to ensure their continued accuracy and in order to ensure that the personal information collected for purposes of the data holding is still necessary for the identified purposes. In this regard, the frequency with which and the circumstances in which the statements of purpose are required to be reviewed must be identified.

The agent(s) responsible and the process that must be followed in reviewing the statements of purpose and in amending the statements of purpose, if necessary, shall also be documented. This shall include the agent(s) or other persons or organizations that must be consulted in reviewing, and if necessary, amending the statements of purpose and the agent(s) responsible for approving the amended statements of purpose. The policy and procedures must further identify the persons and organizations 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 prescribed entity shall require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

8. STATEMENTS OF PURPOSE FOR DATA HOLDINGS CONTAINING PERSONAL INFORMATION

For each data holding containing personal information, the prescribed entity must draft 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, and the need for the personal information in relation to the identified purpose.

9. POLICY AND PROCEDURES FOR LIMITING AGENT ACCESS TO AND USE OF PERSONAL INFORMATION

A policy and procedures 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 and its procedures is to ensure that agents of the prescribed entity access and use both 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 and procedures 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. The prescribed entity must 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 and procedures must require agents to access and use de-identified and/or aggregate information, as defined in the *Policy and Procedures with Respect to De-Identification and Aggregation*.

In this regard, the policy and procedures 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 and procedures must also prohibit agents from using de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information, and attempting to identify an individual based on prior knowledge.

REVIEW AND APPROVAL PROCESS

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 shall be set out in the policy and procedures, 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 and procedures 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; the documentation that must be completed, provided, and/or executed; the agent(s) responsible for completing, providing, and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also set out the 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, if the request is approved, the criteria that must be considered in determining the appropriate level of access. At a minimum, the agent(s) responsible for determining whether to approve or deny the request 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 his or her employment, contractual, or other responsibilities;
- the identified purpose for which access to and use of personal information is requested is permitted by the *CYFSA* and its regulation;
- the identified purpose for which access to and use of personal information is requested cannot reasonably be accomplished without personal information;
- de-identified and/or aggregate information will not serve the identified purpose; and
- in approving the request, no more personal information will be accessed and used than is reasonably necessary to meet the identified purpose.

The policy and procedures should also set out the manner in which the decision approving or denying the request for access to and use of personal information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; to whom the decision will be communicated; any documentation that must be completed, provided, and/or executed upon rendering the

decision; the agent(s) responsible for completing, providing, and/or executing the documentation; and the required content of the documentation.

CONDITIONS OR RESTRICTIONS ON THE APPROVAL

The policy and procedures must identify the conditions or restrictions imposed on an agent granted approval to access and use personal information, such as read, create, 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 and procedures 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.

We recommend that all approved accesses and uses of personal information 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 and its procedures. At a minimum, we recommend that the expiry date be one year from the date approval is granted.

The policy and procedures must also prohibit an agent granted approval to access and use personal information from accessing and using personal information except as necessary for his or her 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 regulation.

Further, the policy and procedures 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 regulation.

NOTIFICATION AND TERMINATION OF ACCESS AND USE

The policy and procedures must require an agent granted approval to access and use personal information, as well as his or her supervisor, to notify the prescribed entity when the agent is no longer employed or retained by the prescribed entity or no longer requires access to or use of the personal information.

The procedure to be followed in providing the notification must also be identified. In particular, the policy and procedures must identify the agent(s) to whom this notification must be provided; the time frame within which this notification must be provided; the format of the notification; the documentation that must be completed, provided, and/or executed, if any; the agent(s) responsible for completing, providing, and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also identify the agent(s) responsible for terminating access to and use of the personal information, the procedure to be followed in terminating access to and use of the personal information and the time frame 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 and Procedures for Termination or Cessation of the Employment or Contractual Relationship*.

SECURE RETENTION

The policy and procedures 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 and Procedures for Secure Retention of Records of Personal Information*.

SECURE DISPOSAL

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

TRACKING APPROVED ACCESS TO AND USE OF PERSONAL INFORMATION

The policy and procedures must require that a log be maintained of agents granted approval to access and use personal information and must identify the agent(s) responsible for maintaining such a log. We also recommend that the policy and procedures 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 prescribed entity must also require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.

In the event that there is no automatic expiry date on the approval to access and use personal information, regular audits of agents granted approval to access and use personal information must be conducted in accordance with the *Policy and Procedures in Respect of Privacy Audits*. The purpose of the audit is to ensure that agents granted such approval continue to be employed or retained by the prescribed entity and continue to require access to the same amount and type of personal information. In this regard, the policy and procedures must identify the agent(s) responsible for conducting the audits and for ensuring compliance and the frequency with which the audits must be conducted. At a minimum, audits must be conducted on an annual basis.

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

10. LOG OF AGENTS GRANTED APPROVAL TO ACCESS AND USE PERSONAL INFORMATION

A prescribed entity must maintain a log of agents granted approval to access and use personal information. At a minimum, the log must include the name of the agent granted approval to access and use personal information; the data holdings of personal information to which the agent has been granted approval to access and use; the level or type of access and use granted; the date that access and use was granted; and the termination date or the date of the next audit of access to and use of the personal information.

11. POLICY AND PROCEDURES FOR THE USE OF PERSONAL INFORMATION FOR RESEARCH

A policy and procedures 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.

The policy and procedures 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 prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance.

The policy and procedures must also require agents to notify the prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of the policy or its procedures.

WHERE THE USE OF PERSONAL INFORMATION IS PERMITTED FOR RESEARCH

If the prescribed entity permits personal information to be used for research purposes, the policy and procedures must 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 and its procedures must clearly distinguish between the use of personal information for research purposes and the use of personal information for the purpose of data analysis or the compilation of statistical information under sections 293(1) or (3) of the *CYFSA*. The criteria that must be considered in determining when a use of personal information is for research purposes and when a use is for the purpose of data analysis or the compilation of statistical information, as well as the agent(s) responsible and the procedure to be followed in making this determination, must also be addressed.

REVIEW AND APPROVAL PROCESS

The policy and procedures must also 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 process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided, and/or executed; the agent(s) responsible for completing, providing, and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures 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. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the *CYFSA* and its regulation.

At a minimum, prior to any approval of the use of personal information for research purposes, the policy and procedures must require the agent(s) responsible for determining whether to approve or deny the request to review the written research plan to ensure it complies with the requirements in the *CYFSA* and its regulation, to ensure that the written research plan has been approved by a research ethics board, and to ensure that the prescribed entity is in receipt of a copy of the decision of the research ethics board approving the written research plan. In addition, 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. These requirements are set out in section 4 of the regulation.

In addition, 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 be required to ensure that the personal information being requested is consistent with the personal information identified in the written research plan approved by the research ethics board. The responsible agent(s) must also be required to ensure that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal information is being requested than is reasonably necessary to meet the research purpose.

The policy and procedures should also set out the manner in which the decision approving or denying the request to use personal information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

CONDITIONS OR RESTRICTIONS ON THE APPROVAL

The policy and procedures must identify the conditions or restrictions that will be imposed on the approval to use personal 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. In determining the conditions or restrictions that will be imposed, the policy and procedures shall have regard to the *CYFSA* and its regulation.

At a minimum, the policy and procedures must require that agent(s) granted approval to use personal information for research purposes 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, and
- notify the prescribed entity immediately in writing if the agent fails to fulfill any of the above-listed requirements.

The policy and procedures must also 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.

SECURE RETENTION

The policy and procedures must require the agent 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 the *Policy and Procedures for Secure Retention of Records of Personal Information*.

SECURE RETURN OR DISPOSAL

The policy and procedures must address whether an agent 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.

If the records of personal information are required to be securely returned to prescribed entity, the policy and procedures must stipulate the time frame 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.

If the records of personal information are required to be disposed of in a secure manner, the policy and procedures must require the records to be disposed of in accordance with the *Policy and Procedures for Secure Disposal of Records of Personal Information*. The policy and procedures must further stipulate the time frame following the retention period in the written research plan within which the records must be securely disposed of, must require a certificate of destruction to be provided, must identify the agent of the prescribed entity to whom the certificate of destruction must be provided, and must identify the time frame following secure disposal within which the certificate of destruction must be provided. The certificate of destruction confirming the secure disposal must be required to identify the records of personal information securely disposed of and the date, time, and method of secure disposal employed and must be required to bear the name and signature of the agent who performed the secure disposal.

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 and procedures shall require the records of personal information to be de-identified in compliance with the *Policy and Procedures With Respect to De-Identification and Aggregation*. The policy and procedures must further stipulate the time frame following the retention period set out in the written research plan within which the records must be de-identified.

The policy and procedures 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 time frame following the retention period set out in the written research plan and the process to be followed in the event that the records of personal information are not securely returned, a certificate of destruction is not received, or the records of personal information are not de-identified within the time frame identified.

TRACKING APPROVED USES OF PERSONAL INFORMATION FOR RESEARCH

The policy and procedures must require that a log be maintained of the approved uses of personal information for research purposes and must identify the agent(s) responsible for maintaining such a log. We also recommend that the policy and procedures address where written research plans, copies of the 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 and the agent(s) responsible for retaining this documentation.

WHERE THE USE OF PERSONAL INFORMATION IS NOT PERMITTED FOR RESEARCH

If the prescribed entity does not permit personal information to be used for research purposes, the policy and procedures must expressly prohibit the use of personal information for research purposes and must indicate whether or not de-identified and/or aggregate information may be used for research purposes.

REVIEW AND APPROVAL PROCESS

If the prescribed entity permits de-identified and/or aggregate information to be used for research purposes, the policy and procedures 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 process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided, and/or executed; the agent(s) responsible for completing, providing, and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures 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. At a minimum, the policy and procedures 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. The agent(s) responsible for undertaking this review shall also be identified.

The policy and procedures should also set out the manner in which 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 are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

CONDITIONS OR RESTRICTIONS ON THE APPROVAL

The policy and procedures 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 and procedures must prohibit an agent 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. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information, and attempting to identify an individual based on prior knowledge.

The policy and procedures 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.

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; and
- the date the records of personal information were securely returned or a certificate of destruction was received or the date by which they must be returned or disposed of, if applicable.

13. POLICY AND PROCEDURES FOR DISCLOSURE OF PERSONAL INFORMATION FOR PURPOSES OTHER THAN RESEARCH

A policy and procedures must be developed and implemented that limit the disclosure of personal information 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 and procedures must prohibit all other disclosures of personal information for non-research purposes.

The policy and procedures 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.

The prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

WHERE THE DISCLOSURE OF PERSONAL INFORMATION IS PERMITTED

The policy and procedures must set out the purposes for which and the circumstances in which the disclosure of personal information is permitted. The policy and procedures must further require that all disclosures of personal information comply with the *CYFSA* and its regulation.

REVIEW AND APPROVAL PROCESS

The policy and procedures 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 in this regard. This shall include a discussion of the

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

The policy and procedures 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. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the *CYFSA* and its regulation.

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 regulation and that any and all conditions or restrictions set out in the *CYFSA* and its regulation have been satisfied

The criteria must also require the agent(s) responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose of the disclosure and that no more personal information is being requested than is reasonably necessary to meet the identified purpose.

The policy and procedures should also set out the manner in which the decision approving or denying the request for the disclosure of personal information for purposes other than research and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

CONDITIONS OR RESTRICTIONS ON THE APPROVAL

The policy and procedures 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 and procedures must require a Data Sharing Agreement to be executed in accordance with the *Policy and Procedures 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.

The policy and procedures must also 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.

SECURE TRANSFER

The policy and procedures shall require records of personal information to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Information*.

SECURE RETURN OR DISPOSAL

The policy and procedures 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.

The policy and procedures must further 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. This shall include the agent(s) responsible for implementing this process and the stipulated time frame 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 may apply.

DOCUMENTATION RELATED TO APPROVED DISCLOSURES OF PERSONAL INFORMATION

We recommend that the policy and procedures 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.

WHERE THE DISCLOSURE OF PERSONAL INFORMATION IS NOT PERMITTED

The policy and procedures must expressly prohibit the disclosure of personal information for non-research purposes, except where the disclosure is required by law. The policy and procedures must indicate whether or not de-identified and/or aggregate information may be disclosed.

REVIEW AND APPROVAL PROCESS

If the prescribed entity permits de-identified and/or aggregate information to be disclosed for non-research purposes, the policy and procedures 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 in this regard. This shall include a discussion of the documentation that must be completed, provided, and/or executed; the agent(s) or other persons or organizations responsible for completing, providing, and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures 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 and procedures must require the de-identified and/or aggregate information to be reviewed prior to the 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. The agent(s) responsible for undertaking this review shall also be identified.

The policy and procedures should also set out the manner in which 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 are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

CONDITIONS OR RESTRICTIONS ON THE APPROVAL

The policy and procedures must also identify the conditions or restrictions that are required to be satisfied prior to the 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. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information, and attempting to identify an individual based on prior knowledge.

The policy and procedures 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 and procedures shall require the responsible agent(s) to track receipt of the executed written acknowledgments and shall set out the procedure that must be followed and the documentation that must be maintained in this regard.

14. POLICY AND PROCEDURES FOR DISCLOSURE OF PERSONAL INFORMATION FOR RESEARCH PURPOSES AND THE EXECUTION OF RESEARCH AGREEMENTS

A policy and procedures 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(1)(b) of the regulation.

The policy and procedures 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.

The prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

WHERE THE DISCLOSURE OF PERSONAL INFORMATION IS PERMITTED FOR RESEARCH

If the prescribed entity permits personal information to be disclosed for research purposes in accordance with section 6(1)(b) of the regulation, the policy and procedures must set out the circumstances in which personal information is permitted to be disclosed for research purposes.

REVIEW AND APPROVAL PROCESS

The policy and procedures 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 research purposes, as well as the process that must be followed in this regard. This shall include a discussion of the documentation

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

The policy and procedures 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 research purposes. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the *CYFSA* and its regulation.

At a minimum, prior to any approval of the disclosure of personal information for research purposes, the policy and procedures must require the agent(s) responsible for determining whether to approve or deny the request to ensure that the prescribed entity is in receipt of a written research plan and a copy of the decision of the research ethics board approving the written research plan and that the written research plan complies with the requirements in the *CYFSA* and its regulation. In addition, the prescribed entity must ensure that the researcher 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.

In addition, prior to any approval of the disclosure of personal information for research purposes, the agent(s) responsible for determining whether to approve or deny the request must be required to ensure that the personal information being requested is consistent with the personal information identified in the written research plan approved by the research ethics board. The responsible agent(s) must also be required to ensure that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal information is being requested than is reasonably necessary to meet the research purpose.

The policy and procedures should also set out the manner in which the decision approving or denying the request for the disclosure of personal information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

CONDITIONS OR RESTRICTIONS ON THE APPROVAL

The policy and procedures must identify the conditions or restrictions that are required to be satisfied prior to the 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 and procedures 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. In addition, the prescribed entity must be satisfied that the researcher will comply with the requirements set out in section 6(2)(c) of the regulation.

The policy and procedures must also identify the agent(s) responsible for ensuring that any conditions or restrictions 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.

SECURE TRANSFER

The policy and procedures shall require the records of personal information disclosed for research purposes to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Information*.

SECURE RETURN OR DISPOSAL

The policy and procedures 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, as the case may be, following the retention period set out in the Research Agreement. The policy and procedures must further 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 PERSONAL INFORMATION FOR RESEARCH

We recommend that the policy and procedures also address where written research plans, copies of the decisions of research ethics boards, Research Agreements, certificates of destruction, and other documentation related to the receipt, review, approval, or denial of requests for the disclosure of personal information for research purposes will be retained and the agent(s) responsible for retaining this documentation.

WHERE THE DISCLOSURE OF PERSONAL INFORMATION IS NOT PERMITTED FOR RESEARCH

If the prescribed entity does not permit personal information to be disclosed for research purposes, the policy and procedures must expressly prohibit the disclosure of personal information for research purposes and must indicate whether or not de-identified and/or aggregate information may be disclosed for research purposes.

REVIEW AND APPROVAL PROCESS

If the prescribed entity permits de-identified and/or aggregate information to be disclosed for research purposes, the policy and procedures 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 for research purposes, as well as the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided, and/or executed by agent(s) of the prescribed entity or by a researcher; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

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

The policy and procedures 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 research purposes. At a minimum, the policy and procedures must require the de-identified and/or aggregate information to be reviewed prior to the approval and 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. The agent(s) responsible for undertaking this review shall also be identified.

The policy and procedures should also set out the manner in which 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 are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

CONDITIONS OR RESTRICTIONS ON THE APPROVAL

The policy and procedures must also identify the conditions or restrictions 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 and 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. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information, and attempting to identify an individual based on prior knowledge.

The policy and procedures 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 and procedures shall require the responsible agent(s) to track receipt of the executed written acknowledgments and shall set out the procedure that must be followed and the documentation that must be maintained in this regard.

15. 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(1)(b) of the regulation. At a minimum, the Research Agreement must address the matters set out below.

GENERAL PROVISIONS

The Research Agreement must describe the status of the prescribed entity under the *CYFSA* and the duties and responsibilities arising from this status. It must also specify the precise nature of the personal information that will be disclosed by the prescribed entity for research purposes and must provide a definition of personal information that is consistent with *FIPPA*.

PURPOSES OF COLLECTION, USE, AND DISCLOSURE

The research purpose for which the personal information is being disclosed by the prescribed entity and the purposes for which the personal information may be used or disclosed by the researcher must be identified in the Research Agreement, as must the statutory authority for each collection, use, and disclosure identified.

In particular, 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. The Research Agreement must also prohibit the researcher from permitting persons to access and use the personal information except those persons described in the written research plan approved by the research ethics board.

In identifying the purposes for which the personal information may be used, the Research Agreement shall explicitly state whether or not the personal information may be linked to other information and must prohibit the personal information from being linked except in accordance with the written research plan approved by the research ethics board.

The Research Agreement shall 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 and that other information, namely de-identified and/or aggregate information, will not serve the research purpose. The researcher must also be required to acknowledge that 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 regulation; not to publish the personal information in a form that could reasonably enable a person to ascertain the identity of the individual; and not to 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 that meets the requirements of the *CYFSA* and its regulation, and a copy of the decision of the research ethics board approving the written research plan.

The researcher must also be required to acknowledge and agree that the researcher will comply with the Research Agreement, with the written research plan approved by the research ethics board, and with the conditions, if any, specified by the research ethics board in respect of the written research plan.

SECURE TRANSFER

The Research Agreement shall require the secure transfer of records of personal information that will be disclosed pursuant to the Research Agreement. The Research Agreement shall 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, and 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 shall have regard to the *Policy and Procedures for Secure Transfer of Records of Personal Information* implemented by the prescribed entity.

SECURE RETENTION

The retention period for the records of personal information subject to the Research Agreement must also be identified, 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.

The Research Agreement shall require the researcher to ensure that the records of personal information are retained in a secure manner and shall 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 and Procedures for Secure Retention of Records of Personal Information* and shall have regard to the written research plan approved by the research ethics board.

The Research Agreement must also require the researcher to take steps that are reasonable in the circumstances to ensure that the personal information subject to the Research Agreement is protected

against theft, loss, and unauthorized use or disclosure and to ensure that the records of personal information subject to the Research Agreement are protected against unauthorized copying, modification, or disposal. The reasonable steps that are required to be taken by the researcher must be detailed in the Research Agreement and, at a minimum, shall include those set out in the written research plan approved by the research ethics board.

SECURE RETURN OR DISPOSAL

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 shall be consistent with the written research plan approved by the research ethics board.

If the records of personal information are required to be returned in a secure manner, the Research Agreement must stipulate the time frame following the retention period within which the records must be securely returned, the secure manner in which the records must be returned, and the 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 and Procedures 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 Research Agreement must provide a definition of secure disposal that is consistent with the *CYFSA* and its regulation and must identify the precise manner in which the records of personal information subject to the Research Agreement must be securely disposed of. The Research Agreement must also stipulate the time frame following the retention period set out in the Research Agreement within which the records of personal information must be securely disposed of and 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 must be consistent with the *CYFSA* and its regulation and with orders, guidelines, fact sheets, and best practices issued by the IPC under the *CYFSA* and its regulation. Helpful guidance may be found in other orders, reports, and decisions issued by the IPC. In addition, regard may be had to the *Policy and Procedures for Secure Disposal of Records of Personal Information* implemented by the prescribed entity.

Further, the Research Agreement must identify the agent of the prescribed entity to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided, and the required content of the certificate of destruction. At a minimum, the certificate of destruction must be required to identify the records of personal information securely disposed of; to stipulate the date, time, location, and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.

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 and Procedures 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 and shall stipulate the time frame following the retention period set out in the

Research Agreement within which the written confirmation must be provided and the agent of the prescribed entity to whom the written confirmation must be provided.

NOTIFICATION

At a minimum, the Research Agreement must require the researcher to immediately notify the prescribed entity, in writing, if the researcher becomes aware of a breach or suspected breach of the Research Agreement, in the circumstances set out in section 6(2)(c)(vi) of the regulation, or if personal information subject to the Research Agreement is stolen, lost, or used or disclosed without authority or is believed to have been stolen, lost, or 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 and to contain the theft, loss, or unauthorized use or disclosure.

CONSEQUENCES OF BREACH AND MONITORING COMPLIANCE

The Research Agreement must outline the consequences of breach of the agreement and must indicate whether compliance with the Research Agreement will be audited by the prescribed entity and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.

The Research Agreement must also 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. The Research Agreement must 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.

16. LOG OF RESEARCH AGREEMENTS

A prescribed entity must maintain a log of executed Research Agreements under section 6(1)(b) of the regulation. 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 written decision of the research ethics board approving the research plan;
- 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; and
- 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.

17. POLICY AND PROCEDURES FOR THE EXECUTION OF DATA SHARING AGREEMENTS

A policy and procedures must be developed and implemented to identify the circumstances requiring the execution of a Data Sharing Agreement and the process that must be followed and the requirements that must be satisfied prior to the execution of a Data Sharing Agreement.

The policy and procedures 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 and must require the execution of a Data Sharing Agreement prior to any disclosure of personal information for purposes other than research.

The policy and procedures must further identify the agent(s) responsible for ensuring that a Data Sharing Agreement is executed, as well as the process that must be followed and the requirements that must be satisfied in this regard. This shall include a discussion of the documentation that must be completed, provided, and/or executed; the agent(s) or other persons or organizations responsible for completing, providing, and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the 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 and Procedures 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 and Procedures for the Collection of Personal Information*.

The policy and procedures must also require that a log of Data Sharing Agreements be maintained and must identify the agent(s) responsible for maintaining such a log. In addition, we recommend that the policy and procedures address where documentation related to the execution of Data Sharing Agreements will be retained and the agent(s) responsible for retention.

The prescribed entity must also require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

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 and Procedures 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. It must also specify the precise nature of the personal information subject to the Data Sharing Agreement and must provide a definition of personal information that is consistent with *FIPPA*. The Data Sharing Agreement shall also identify the person or organization that is collecting personal information and the person or organization that is disclosing personal information pursuant to the Data Sharing Agreement.

PURPOSES OF COLLECTION, USE, AND DISCLOSURE

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

In identifying these purposes, the Data Sharing Agreement shall 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, the Data Sharing Agreement must identify 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, and why the linkage is required for the identified purposes.

The Data Sharing Agreement shall 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 and that other information, namely de-identified and/or aggregate information, will not serve the purpose, and that no more personal information is being collected and will be used than is reasonably necessary to meet the purpose.

The Data Sharing Agreement must also identify the purposes, if any, for which the personal information subject to the Data Sharing Agreement may be disclosed and any limitations, conditions, or restrictions imposed thereon.

The Data Sharing Agreement must also require the collection, use, and disclosure of personal information subject to the Data Sharing Agreement to comply with the *CYFSA* and its regulation and must set out the specific statutory authority for each collection, use, and disclosure contemplated in the Data Sharing Agreement.

SECURE TRANSFER

The Data Sharing Agreement shall require the secure transfer of the records of personal information subject to the Data Sharing Agreement. The Data Sharing Agreement shall 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, and the 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 may be had to the *Policy and Procedures for Secure Transfer of Records of Personal Information* implemented by the prescribed entity.

SECURE RETENTION

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

The Data Sharing Agreement shall also require the records of personal information to be retained in a secure manner and shall identify the precise 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 may have regard to the *Policy and Procedures for Secure Retention of Records of Personal Information* implemented by the prescribed entity.

The Data Sharing Agreement must also require reasonable steps to be taken to ensure that the personal information subject to the Data Sharing Agreement is protected against theft, loss, and unauthorized use or disclosure and to ensure that the records of personal information are protected against unauthorized copying, modification, or disposal. The reasonable steps that are required to be taken shall also be detailed in the Data Sharing Agreement.

SECURE RETURN OR DISPOSAL

The Data Sharing Agreement must also address whether the records of personal information subject to the Data Sharing Agreement will be returned in a secure manner or will be disposed of in a secure manner following the retention period set out in the Data Sharing Agreement or following the date of termination of the Data Sharing Agreement, as the case may be.

If the records of personal information are required to be returned in a secure manner, the Data Sharing Agreement must stipulate the time frame 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, the secure manner in which the records must be returned, and the person 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 and Procedures 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 Data Sharing Agreement must provide a definition of secure disposal that is consistent with the *CYFSA* and its regulation and must identify the precise manner in which the records of personal information subject to the Data Sharing Agreement must be securely disposed of. The Data Sharing Agreement must also stipulate the time frame 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 and 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, prescribed entities must ensure that the method of secure disposal identified is consistent with the *CYFSA* and its regulation and with orders, guidelines, fact sheets, and best practices issued by the IPC under the *CYFSA* and its regulation. Helpful guidance may be found in other orders, reports, and decisions issued by the IPC. In addition, regard may be had to the *Policy and Procedures for Secure Disposal of Records of Personal Information* implemented by the prescribed entity.

Further, the Data Sharing Agreement must identify the person to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided, and the required content of the certificate of destruction. At a minimum, the certificate of destruction must be required to identify the records of personal information securely disposed of; to stipulate the date, time, location, and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.

NOTIFICATION

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 if the personal information subject to the Data Sharing Agreement is stolen, lost, or used or disclosed without authority or is believed to have been stolen, lost, or used or disclosed without authority. It should also identify whether the notification must be verbal 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 of the Data Sharing Agreement and to contain the theft, loss, or unauthorized use or disclosure.

CONSEQUENCES OF BREACH AND MONITORING COMPLIANCE

The Data Sharing Agreement must outline the consequences of breach of the agreement and must indicate whether compliance with the Data Sharing Agreement will be audited and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.

The Data Sharing Agreement must also 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. The Data Sharing Agreement must set out the method by which this will be ensured. This may include requiring the persons that 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.

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; and
- the date the records of personal information were securely returned or a certificate of destruction was provided or the date by which they must be returned or disposed of.

20. POLICY AND PROCEDURES FOR EXECUTING AGREEMENTS WITH THIRD PARTY SERVICE PROVIDERS IN RESPECT OF PERSONAL INFORMATION

A policy and procedures must be developed and implemented requiring written agreements to be entered into with third party service providers prior to permitting third party service providers to access and use the personal information of the prescribed entity. The policy and procedures must further require the written agreements to contain the relevant language from the *Template Agreement for All Third Party Service Providers*.

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 such an agreement, must also be identified in the policy and procedures.

The policy and procedures must also state that the prescribed entity shall not provide personal information to a third party service provider if other information, namely de-identified and/or aggregate information, will serve the purpose and will not provide more personal information than is reasonably necessary to meet the purpose. The agent responsible for making this determination must also be identified in the policy and procedures.

The policy and procedures must further identify the agent(s) responsible for ensuring that records of personal information provided to a third party service provider are either securely returned to the prescribed entity or are securely disposed of, as the case may be, following the termination of the agreement. They must further address 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 and the time frame following termination within which this process must be implemented.

The policy and procedures must require that a log be maintained of all agreements executed with third party service providers and must identify the agent(s) responsible for maintaining such a log. In addition, we recommend that the policy and procedures address where documentation related to the execution of agreements with third party service providers will be retained and the agent(s) responsible for retaining this documentation.

The prescribed entity must also require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

21. TEMPLATE AGREEMENT FOR ALL THIRD PARTY SERVICE PROVIDERS

A written agreement must be entered into with third party service providers that will be permitted to access and use personal information of the prescribed entity, including those that are contracted to retain, transfer, or dispose of records of personal information and those that are contracted to provide services for the purpose of enabling the prescribed entity to use electronic means to collect, use, modify, disclose, retain, or dispose of personal information ("electronic service providers"). At a minimum, the written agreement must address the matters set out below.

GENERAL PROVISIONS

The agreement must describe the status of the prescribed entity under the *CYFSA* and the duties and responsibilities arising from this status. The agreement must also state whether or not the third party service provider is an agent of the prescribed entity in providing services pursuant to the agreement.

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

If the third party service provider is an agent of the prescribed entity, the agreement must require the third party service provider to comply with the provisions of the *CYFSA* and its regulation relating to prescribed entities and to comply with the privacy and security policies and procedures implemented by the prescribed entity in providing services pursuant to the agreement.

We also recommend that the agreement provide a definition of personal information and that the definition provided be consistent with *FIPPA*. Where appropriate, the agreement should also specify the precise nature of the personal information that the third party service provider will be permitted to access and use in the course of providing services pursuant to the agreement.

The agreement must also require that the services provided by the third party service provider pursuant to the agreement be performed in a professional manner, in accordance with industry standards and practices, and by properly trained agents of the third party service provider.

OBLIGATIONS WITH RESPECT TO ACCESS AND USE

The agreement shall identify the purposes for which the third party service provider is permitted to access and use the personal information of the prescribed entity and any limitations, conditions, or restrictions imposed thereon.

In identifying the purposes for which the third party service provider is permitted to use personal information, the prescribed entity must ensure that each use identified in the agreement is consistent with the uses of personal information permitted by the *CYFSA* and its regulation. The agreement must also prohibit the third party service provider from using personal information except as permitted in the agreement.

In the case of an electronic service provider that is not an agent of the prescribed entity, the agreement must explicitly prohibit the electronic service provider from using personal information except as necessary in the course of providing services pursuant to the agreement.

Further, the agreement must prohibit the third party service provider from using personal information if other information will serve the purpose and from using more personal information than is reasonably necessary to meet the purpose.

OBLIGATIONS WITH RESPECT TO DISCLOSURE

The agreement must identify the purposes, if any, for which the third party service provider is permitted to disclose the personal information of the prescribed entity and any limitations, conditions, or restrictions imposed thereon.

In identifying the purposes for which the third party service provider is permitted to disclose personal information, the prescribed entity must ensure that each disclosure identified in the agreement is consistent with the disclosures of personal information permitted by the *CYFSA* and its regulation. In this regard, the agreement must prohibit the third party service provider from disclosing personal information except as permitted in the agreement or as required by law, from disclosing personal information if other information will serve the purpose, and from disclosing more personal information than is reasonably necessary to meet the purpose.

In the case of an electronic service provider that is not an agent of the prescribed entity, the agreement must prohibit the electronic service provider from disclosing personal information to which it has access in the course of providing services except as required by law.

SECURE TRANSFER

Where it is necessary to transfer records of personal information to or from the prescribed entity, the agreement must require the third party service provider to securely transfer the records of personal information and must set out the responsibilities of the third party service provider in this regard. In particular, the agreement must specify the secure manner in which the records will be transferred by the third party service provider, the conditions pursuant to which the records will be transferred by the third party service provider, to whom the records will be transferred, and the procedure that must be followed by the third party service provider 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 agreement shall have regard to the *Policy and Procedures for Secure Transfer of Records of Personal Information* implemented by the prescribed entity.

In addition, where the retention of records of personal information or where the disposal of records of personal information outside the premises of the prescribed entity is the primary service provided to the prescribed entity, the agreement shall require the third party service provider 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 of the records of personal information by the third party service provider. In these circumstances, the agreement must also obligate the third party service provider to maintain a detailed inventory of the records of personal information transferred.

SECURE RETENTION

The agreement shall require the third party service provider to retain the records of personal information, where applicable, in a secure manner and shall identify the precise methods by which records of personal information in paper and electronic format will be securely retained by the third party service provider, including records of personal information retained on various media.

The agreement must further outline the responsibilities of the third party service provider in securely retaining the records of personal information. In identifying the secure manner in which the records of personal information will be retained, and the methods by which the records of personal information will be securely retained, the agreement shall have regard to the *Policy and Procedures for Secure Retention of Records of Personal Information* implemented by the prescribed entity.

In addition, the agreement must require the third party service provider 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 and Procedures for the Segregation of Personal Information* implemented by the prescribed entity.

Where the retention of records of personal information is the primary service provided to the prescribed entity by the third party service provider, the agreement must also obligate the third party service provider to maintain a detailed inventory of the records of personal information being retained on behalf of the prescribed entity as well as a method to track the records being retained.

SECURE RETURN OR DISPOSAL FOLLOWING TERMINATION OF THE AGREEMENT

The agreement must address, where applicable, whether records of personal information will be securely returned to the prescribed entity or will be 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 agreement must stipulate the time frame following the date of termination of the agreement within which the records of personal information must be securely returned, the secure manner in which the records must be returned, and the 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 agreement shall have regard to the *Policy and Procedures 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 agreement must provide a definition of secure disposal that is consistent with the *CYFSA* and its regulation and must identify the precise manner in which the records of personal information are to be securely disposed of.

In identifying the secure manner in which the records of personal information will be disposed of, prescribed entities must ensure that the method of secure disposal identified is consistent with the *CYFSA* and its regulation and with orders, guidelines, fact sheets, and best practices issued by the IPC under the *CYFSA* and its regulation. Helpful guidance may be found in other IPC orders, reports, and decisions. In addition, regard may be had to the *Policy and Procedures for Secure Disposal of Records of Personal Information* implemented by the prescribed entity.

The agreement must also stipulate the time frame following termination of the agreement within which the records of personal information must be securely disposed of and within which a certificate of destruction must be provided to the prescribed entity. The agreement must further identify the agent of the prescribed entity to whom the certificate of destruction must be provided and must identify the required content of the certificate of destruction. At a minimum, the certificate of destruction must be required to identify the records of personal information securely disposed of; to stipulate the date, time, and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.

SECURE DISPOSAL AS A CONTRACTED SERVICE

Where the disposal of records of personal information is the primary service provided to the prescribed entity by the third party service provider, in addition to the requirements set out above in relation to secure disposal, the agreement must further set out the responsibilities of the third party service provider in securely disposing of the records of personal information, including:

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

The agreement should also enable the prescribed entity, at its discretion, to witness the secure disposal of the records of personal information subject to such reasonable terms or conditions as may be required in the circumstances.

IMPLEMENTATION OF SAFEGUARDS

The agreement shall require the third party service provider to take steps that are reasonable in the circumstances to ensure that the personal information accessed and used in the course of providing services pursuant to the agreement is protected against theft, loss, and unauthorized use or disclosure and to ensure that the records of personal information subject to the agreement are protected against unauthorized copying, modification, or disposal. The reasonable steps that are required to be implemented by the third party service provider must be detailed in the agreement.

TRAINING OF AGENTS OF THE THIRD PARTY SERVICE PROVIDER

The agreement shall require the third party service provider 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 and on the consequences that may arise in the event of a breach of these obligations.

The agreement must also require the third party service provider to 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 agreement must set out the method by which this will be ensured. This may include requiring agents 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 agreement permits the third party service provider to subcontract the services provided under the agreement, the third party service provider must be required to acknowledge and agree that it will provide the prescribed entity with advance notice of its intention to do so, that the third party service provider will enter into a written agreement with the subcontractor on terms consistent with its obligations to the prescribed entity, and that a copy of the written agreement will be provided to the prescribed entity.

NOTIFICATION

At a minimum, the agreement must require the third party service provider to notify the prescribed entity at the first reasonable opportunity if there has been a breach or suspected breach of the agreement or if personal information handled by the third party service provider on behalf of the prescribed entity is stolen, lost, or used or disclosed without authority or is believed to have been stolen, lost, or used or disclosed without authority. The agreement should also identify whether the notification must be verbal, written, or both and to whom the notification must be provided. The third party service provider must also be required to take steps that are reasonable in the circumstances to contain the breach and to contain the theft, loss, or unauthorized use or disclosure.

CONSEQUENCES OF BREACH AND MONITORING COMPLIANCE

The agreement must outline the consequences of breach of the agreement and must indicate whether the prescribed entity will be auditing compliance with the agreement and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided to the third party service provider of the audit.

22. LOG OF AGREEMENTS WITH THIRD PARTY SERVICE PROVIDERS

A prescribed entity must maintain a log of executed agreements with third party service providers. At a minimum, the log must include:

- the name of the third party service provider;
- the nature of the services provided by the third party service provider;
- the date that the agreement with the third party service provider was executed;
- the date that the records of personal information or access to the records of personal information, if any, was provided;
- the nature of the personal information provided or to which access was provided;
- the date of termination of the agreement with the third party service provider;
- whether the records of personal information, if any, will be securely returned or will be securely disposed of following the date of termination of the agreement; and
- 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.

23. POLICY AND PROCEDURES FOR THE LINKAGE OF RECORDS OF PERSONAL INFORMATION

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

The policy and procedures must identify whether or not the prescribed entity permits the linkage of records of personal information and if it is not permitted, the policy and procedures must expressly 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:

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

REVIEW AND APPROVAL PROCESS

The policy and procedures 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 in this regard. This shall include a discussion of the documentation that must be completed, provided, and/or executed; the agent(s) or other persons or organizations responsible for completing, providing, and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures 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. In addition, the policy and procedures must require agent(s) to document the legal authority for linking the records of personal information.

The policy and procedures should also set out the manner in which the decision approving or denying the request to link records of personal information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

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 and procedures must require that the disclosure be approved pursuant to the *Policy and Procedures for Disclosure of Personal Information for Research Purposes and the Execution of Research Agreements* or the *Policy and Procedures for Disclosure of Personal Information for Purposes Other Than Research*, as may be applicable.

Where the linked records of personal information will be used by the prescribed entity, the policy and procedures must require that the use be approved pursuant to the *Policy and Procedures for the Use of Personal Information for Research* or the *Policy and Procedures for Limiting Agent Access to and Use of Personal Information*, as may be applicable. The policy and procedures must further require that the linked

records of personal information be de-identified and/or aggregated as soon as practicable pursuant to the *Policy and Procedures 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 and procedures 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 and its procedures.

RETENTION

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

SECURE DISPOSAL

The policy and procedures 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 and Procedures for Secure Disposal of Records of Personal Information*.

COMPLIANCE, AUDIT, AND ENFORCEMENT

The prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

TRACKING APPROVED LINKAGES OF RECORDS OF PERSONAL INFORMATION

The policy and procedures must require that a log be maintained of the linkages of records of personal information approved by the prescribed entity and must identify the agent(s) responsible for maintaining such a log. We also recommend that the policy and procedures address where documentation related to the receipt, review, approval, or denial of requests to link records of personal information will be retained and the agent(s) responsible for retaining this documentation.

24. LOG OF APPROVED LINKAGES OF RECORDS OF PERSONAL INFORMATION

A prescribed entity must maintain a log of linkages of records of personal information approved by the prescribed entity. At a minimum, the log must include the name of the agent, person, or organization who

requested the linkage; the date that the linkage of records of personal information was approved; and the nature of the records of personal information linked.

25. POLICY AND PROCEDURES WITH RESPECT TO DE-IDENTIFICATION AND AGGREGATION

A policy and procedures must be developed and implemented with respect to de-identification and aggregation. The policy and procedures must require that personal information not be used or disclosed if other information, namely de-identified and/or aggregate information, will serve the identified purpose.

The policy of the prescribed entity with respect to cell-sizes of less than five and the exceptions thereto must also be articulated. In articulating the policy with respect to cell-sizes of less than five, regard must be had to the restrictions related to cell-sizes of less than five contained in Agreements, Research Agreements, and written research plans pursuant to which the personal information was collected by the prescribed entity.

The policy and procedures must provide a definition of de-identified information and aggregate information. The definitions adopted and the policy of the prescribed entity with respect to cell-sizes of less than five shall have regard to, and must be consistent with, the meaning of "personal information" in *FIPPA*.

The information that must be removed, encrypted, and/or truncated in order to constitute de-identified information and the manner in which the information must be grouped, collapsed, or averaged in order to constitute aggregate information must also be identified. The policy and procedures shall also address the agent(s) responsible for de-identifying and/or aggregating information and the procedure to be followed in this regard.

Further, the policy and procedures must require de-identified and/or aggregate information, including information of cell-sizes of 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. The agent(s) responsible for conducting this review shall also be identified.

The process to be followed in reviewing the de-identified and/or aggregate information and the criteria to be used in assessing the risk of re-identification shall also be set out. In establishing the criteria to be used in assessing the risk of re-identification, the prescribed entity shall 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).

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

The policy and procedures must also prohibit agents from using de-identified and/or aggregate information, including information in cell-sizes of less than five, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information, and attempting to identify an individual based on prior knowledge. The policy and procedures 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.

The prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures

must also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

26. PRIVACY IMPACT ASSESSMENT POLICY AND PROCEDURES

A policy and procedures must be developed and implemented to identify the 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, we recommend that the policy and procedures ensure that prescribed entities conduct privacy impact assessments on existing and proposed data holdings involving personal information and whenever a new information system or a change to an existing information system, technology, or program involving personal information is contemplated.

If there are limited and specific circumstances in which privacy impact assessments are not required to be conducted on existing and proposed data holdings involving personal information and whenever a new information system or a change to an existing information system, technology, or program involving personal information is contemplated, these shall be outlined in the policy and procedures along with a rationale for why privacy impact assessments are not required. The policy and procedures must further identify the agent(s) responsible for making this determination and must require the determination and the reasons for the determination to be documented.

The policy and procedures must also address the timing of privacy impact assessments. With respect to proposed data holdings involving personal information and new or changes to existing information systems, technologies, or programs involving personal information, the policy and procedures must require that privacy impact assessments be conducted at the conceptual design stage and that they be reviewed and amended, if necessary, during the detailed design and implementation stage. With respect to existing data holdings involving personal information, the policy and procedures must require that a timetable be developed to ensure privacy impact assessments are conducted, and the policy and procedures must identify the agent(s) responsible for developing the timetable.

Once privacy impact assessments have been completed, the policy and procedures shall require that they be reviewed on an ongoing basis in order to ensure that they continue to be accurate and continue to be consistent with the information practices of the prescribed entity. The policy and procedures must also identify the circumstances in which and the frequency with which privacy impact assessments are required to be reviewed.

The policy and procedures must also identify the agent(s) responsible and the process that must be followed in identifying when privacy impact assessments are required; in identifying when privacy impact assessments are required to be reviewed in accordance with the policy and procedures; in ensuring that privacy impact assessments are conducted and completed; and in ensuring that privacy impact assessments are reviewed and amended, if necessary. The role of agent(s) that have been delegated day-to-

day authority to manage the privacy program and the security program shall also be identified in respect of privacy impact assessments.

The policy and procedures 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 specific 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;
- 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; and
- the administrative, technical, and physical safeguards implemented or proposed to be implemented to protect the personal information.

The process for addressing the recommendations arising from privacy impact assessments, including the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations, and for monitoring and ensuring the implementation of the recommendations, is also required to be outlined.

The policy and procedures must require that a log be maintained of privacy impact assessments that have been completed; that have been undertaken but that have not been completed; and that have not been undertaken. The policy and procedures must also identify the agent(s) responsible for maintaining such a log.

The prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and*

Procedures in Respect of Privacy Audits, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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

In developing the policy and procedures, we recommend that regard be had to the various guidelines produced by the IPC and available at **www.ipc.on.ca**.

27. LOG OF PRIVACY IMPACT ASSESSMENTS

A prescribed entity shall maintain a log of privacy impact assessments that have been completed and of privacy impact assessments that have been undertaken but that have not been completed. The log shall describe the data holding, information system, technology, or program involving personal information that is at issue; the date that the privacy impact assessment was completed or is expected to be completed; the agent(s) responsible for completing or ensuring the completion of the privacy impact assessment; the recommendations arising from the privacy impact assessment; the agent(s) responsible for addressing each recommendation, the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.

A prescribed entity shall 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 shall either set out the reason that a privacy impact assessment will not be undertaken and the agent(s) responsible for making this determination or set out the date that the privacy impact assessment is expected to be completed and the agent(s) responsible for completing or ensuring the completion of the privacy impact assessment.

28. POLICY AND PROCEDURES IN RESPECT OF PRIVACY AUDITS

A policy and procedures 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 shall include audits to assess compliance with the privacy policies and procedures implemented by the prescribed entity and audits of the agent(s) permitted to access and use personal information pursuant to the *Policy and Procedures for Limiting Agent Access to and Use of Personal Information*.

With respect to each privacy audit that is required to be conducted, the policy and procedures must set out the purposes of the privacy audit; the nature and scope of the privacy audit (i.e. document reviews, interviews, site visits, inspections); the agent(s) responsible for conducting the privacy audit; and the frequency with which and the circumstances in which each privacy audit is required to be conducted. In this regard, the policy and procedures shall require a privacy audit schedule to be developed and shall identify the agent(s) responsible for developing the privacy audit schedule.

For each type of privacy audit that is required to be conducted, the policy and procedures shall also set out the process to be followed in conducting the audit. This is to include the criteria that must be considered in selecting the subject matter of the audit and 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 and

procedures must further discuss the documentation that must be completed, provided, and/or executed in undertaking each privacy audit; the agent(s) responsible for completing, providing, and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The role of agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The policy and procedures shall also set out the process that must be followed in addressing the recommendations arising from privacy audits, including the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations, and for monitoring and ensuring the implementation of the recommendations.

The policy and procedures 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, the agent(s) to whom the documentation must be provided, and the required content of the documentation.

The policy and procedures must also address the manner and format in which the findings of privacy audits, including the recommendations arising from the privacy audits and the status of addressing the recommendations, are communicated. This shall include a discussion of the agent(s) responsible for communicating the findings of the privacy audit; the mechanism and format for communicating the findings of the privacy audit; the time frame within which the findings of the privacy audit must be communicated; and to whom the findings of the privacy audit will be communicated, including the Chief Executive Officer or the Executive Director.

The policy and procedures must further require that a log be maintained of privacy audits and must identify the agent(s) responsible for maintaining the log and for tracking that the recommendations arising from the privacy audits are addressed within the identified time frame. They should further address where documentation related to privacy audits will be retained and the agent(s) responsible for retaining this documentation.

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

29. LOG OF PRIVACY AUDITS

A prescribed entity shall maintain a log of privacy audits that have been completed. The log shall set out the nature and type of the privacy audit conducted; the date that the privacy audit was completed; the agent(s) responsible for completing the privacy audit; the recommendations arising from the privacy audit; the agent(s) responsible for addressing each recommendation; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.

30. POLICY AND PROCEDURES FOR PRIVACY BREACH MANAGEMENT

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

The policy and procedures must provide a definition of the term "privacy breach." At a minimum, a privacy breach shall be defined to include:

- the collection, use, and disclosure of personal information that is not in compliance with the *CYFSA* or its regulation;
- a contravention of the privacy policies and procedures implemented by the prescribed entity;
- a contravention of a Data Sharing Agreement, Research Agreement, Confidentiality Agreement, or an Agreement with a Third Party Service Provider retained by the prescribed entity; and
- circumstances where personal information is stolen, lost, or subject to unauthorized use or disclosure or where records of personal information are subject to unauthorized copying, modification, or disposal.

The policy and procedures shall impose a mandatory requirement on agents to notify the prescribed entity of a privacy breach or suspected privacy breach.

In this regard, the policy and procedures shall identify the agent(s) who must be notified of the privacy breach or suspected privacy breach and shall provide contact information for the agent(s) who must be notified. The policy and procedures shall further stipulate the time frame within which notification must be provided, whether the notification must be provided verbally and/or in writing, and the nature of the information that must be provided upon notification. The policy and procedures shall also address the documentation that must be completed, provided, and/or executed with respect to notification; the agent(s) responsible for completing, providing, and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

Upon notification, the policy and procedures shall require a determination to be made of whether a privacy breach has in fact occurred and if so, what, if any, personal information has been breached. The agent(s) responsible for making this determination must also be identified.

The policy and procedures must further address when senior management, including the Chief Executive Officer or the Executive Director, will be notified. This shall include a discussion of the agent(s) responsible for notifying senior management; the time frame within which notification must be provided; the manner in which this notification must be provided; and the nature of the information that must be provided to senior management upon notification.

The policy and procedures shall also require that containment be initiated immediately and shall identify the agent(s) responsible for containment and the procedure that must be followed in this regard, including any documentation that must be completed, provided, and/or executed by the agent(s) responsible for containing the breach and the required content of the documentation.

In undertaking containment, the policy and procedures must ensure that reasonable steps are taken in the circumstances to protect personal information from further theft, loss, or unauthorized use or disclosure and to protect records of personal information from further unauthorized copying, modification, or disposal. At a minimum, these steps shall include ensuring that no copies of the records of personal information have been

made and ensuring that 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 related to the date, time, and method of secure disposal. These steps shall also include ensuring that additional privacy breaches cannot occur through the same means and determining whether the privacy breach would allow unauthorized access to any other information and, if necessary, taking further action to prevent additional privacy breaches.

The agent(s) responsible and 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, must be identified in the policy and procedures. The policy and procedures shall also address the documentation that must be completed, provided, and/or executed by the agent(s) responsible for reviewing the containment measures; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

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

In particular, the policy and procedures shall set out the agent(s) responsible for notifying the service provider or other person or organization, the format of the notification, and the nature of the information that must be provided upon notification. At a minimum, the policy and procedures 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, and further actions that will be undertaken with respect to the privacy breach, including investigation and remediation. 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. The required notification shall be provided by the service provider, if applicable.

The policy and procedures shall also set out whether any other persons or organizations must be notified of the privacy breach and shall set out the agent(s) responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification, and the time frame for notification.

In particular, the policy and procedures 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 the regulation. 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, and further actions that will be undertaken with respect to the privacy breach, including investigation and remediation.

The policy and procedures must further identify the agent(s) responsible for investigating the privacy breach, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections), and the process that must be followed in investigating the privacy breach. This shall include a discussion of the documentation that must be completed, provided, and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing, and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. The role of agent(s)

that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The policy and procedures shall also identify the agent(s) responsible for assigning other agent(s) to address the recommendations; for establishing timelines to address the recommendations; for addressing the recommendations; and for monitoring and ensuring that the recommendations are implemented within the stated timelines. The policy and procedures shall 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; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also address the manner and format in which the findings of the investigation of the privacy breach, including the recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This shall include a discussion of the agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings of the investigation must be communicated, including the Chief Executive Officer or the Executive Director.

In addition, the policy and procedures shall address whether the process to be followed in identifying, reporting, containing, notifying, investigating, and remediating a privacy breach is different where the breach is both a privacy breach or suspected privacy breach, as well as an information security breach or suspected information security breach.

Further, the policy and procedures must require that a log be maintained of privacy breaches and must identify the agent(s) responsible for maintaining the log and for tracking that the recommendations arising from the investigation of privacy breaches are addressed within the identified timelines. They should further address where documentation related to the identification, reporting, containment, notification, investigation, and remediation of privacy breaches will be retained and the agent(s) responsible for retaining this documentation.

The prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

In developing the policy and procedures, we recommend that the prescribed entity have regard to the various guidelines produced by the IPC and available at **www.ipc.on.ca**.

31. LOG OF PRIVACY BREACHES

A prescribed entity shall maintain a log of privacy breaches setting out:

- the date of the privacy breach;
- the date that the privacy breach was identified or suspected;
- whether the privacy breach was internal or external;

- the nature of the personal information that was the subject matter of the privacy breach and the nature and extent of the privacy breach;
- the date that the privacy breach was contained and the nature of the containment measures;
- the date that the service provider that disclosed the personal information to the prescribed entity was notified;
- the date that the IPC was notified of the breach, if applicable;
- the date that the investigation of the privacy breach was completed;
- the agent(s) responsible for conducting the investigation;
- the recommendations arising from the investigation;
- the agent(s) responsible for addressing each recommendation;
- the date each recommendation was or is expected to be addressed; and
- the manner in which each recommendation was or is expected to be addressed.

32. POLICY AND PROCEDURES FOR PRIVACY COMPLAINTS

A policy and procedures 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" shall be provided that, at a minimum, includes concerns or complaints relating to the privacy policies and procedures implemented by the prescribed entity and relating to the compliance of the prescribed entity with the *CYFSA* and its regulation.

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 shall also be identified. At a minimum, the name and/or title, mailing address, and contact information of the agent(s) to whom concerns or complaints may be directed and information related to the manner in which and format in which privacy concerns or complaints may be directed to the prescribed entity should be made publicly available. We also recommend that individuals be advised that they may make a complaint to the IPC and be provided with the IPC's mailing address and contact information.

The policy and procedures must further establish the process to be followed in receiving privacy complaints. This shall include any documentation that must be completed, provided, and/or executed by the individual making the privacy complaint; the agent(s) responsible for receiving the privacy complaint; the required content of the documentation, if any; and the nature of the information to be requested from the individual making the privacy complaint.

Upon receipt of a privacy complaint, the policy and procedures shall require a determination to be made of whether or not the privacy complaint will be investigated. In this regard, the policy and procedures shall identify the agent(s) responsible for making this determination, the time frame within which this determination must be made, and the process that must be followed and the criteria that must be used in making the determination, including any documentation that must be completed, provided, and/or executed and the required content of the documentation.

In the event that it is determined that an investigation will not be undertaken, the policy and procedures must require that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; providing a response to the privacy complaint; advising that an investigation of the privacy complaint will not be undertaken; advising the individual that he or she may make a complaint to the IPC; and providing the IPC's contact information.

In the event that it is determined that an investigation will be undertaken, the policy and procedures must require that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; advising that an investigation of the privacy complaint will be undertaken; explaining the privacy complaint investigation procedure; indicating whether the individual will be contacted for further information concerning the privacy complaint; setting out the projected time frame for completion of the investigation; and identifying the nature of the documentation that will be provided to the individual following the investigation.

The policy and procedures must identify the agent(s) responsible for sending the above noted letters to the individuals making privacy complaints and the time frame within which the letters will be sent to the individuals.

Where an investigation of a privacy complaint will be undertaken, the policy and procedures must identify the agent(s) responsible for investigating the privacy complaint, the nature and scope of the investigation (e.g., document reviews, interviews, site visits, inspections), and the process that must be followed in investigating the privacy complaint. This shall include a discussion of the documentation that must be completed, provided, and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing, and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified in the policy and procedures.

The process for addressing the recommendations arising from the investigation of privacy complaints and the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, and for monitoring and ensuring the implementation of the recommendations shall also be addressed in the policy and procedures. The policy and procedures 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; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also address the manner 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 shall include a discussion of the agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings must be communicated, including the Chief Executive Officer or the Executive Director.

The policy and procedures shall further require the individual making the privacy complaint to be notified, in writing, of the nature and findings of the investigation and of the measures taken, if any, in response to the privacy complaint. The individual making the privacy complaint shall also be advised that he or she may make a complaint to the IPC. The IPC's contact information shall also be provided. The agent(s) responsible

for providing the written notification to the individual making the privacy complaint and the time frame within which the written notification must be provided, shall also be addressed.

The policy and procedures should also address whether 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 by which, the format in which, and the time frame within which the notification must be provided and the agent(s) responsible for providing the notification.

Further, the policy and procedures must require that a log be maintained of privacy complaints and must identify the agent(s) responsible for maintaining the log and for tracking whether the recommendations arising from the investigation of privacy complaints are addressed within the identified timelines. They should further address where documentation related to the receipt, investigation, notification, and remediation of privacy complaints will be retained and the agent(s) responsible for retaining this documentation.

The prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of Privacy Audits,* must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures. The relationship between this policy and its procedures and the *Policy and Procedures for Privacy Breach Management* shall also be addressed.

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

33. LOG OF PRIVACY COMPLAINTS

A prescribed entity shall 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 or not the privacy complaint will be investigated and the date that the determination was made;
- the date that the individual making the complaint was advised that the complaint will not be investigated and was provided a response to the complaint;
- the date that the individual making the complaint 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 recommendations arising from the investigation;
- the agent(s) responsible for addressing each recommendation;
- the date each recommendation was or is expected to be addressed;
- the manner in which each recommendation was or is expected to be addressed; and
- the date that the individual making the privacy complaint was advised of the findings of the investigation and the measures taken, if any, in response to the privacy complaint.

34. POLICY AND PROCEDURES FOR PRIVACY INQUIRIES

A policy and procedures 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" shall be provided that, at a minimum, includes inquiries relating to the privacy policies and procedures implemented by the prescribed entity and related to the compliance of the prescribed entity with the *CYFSA* and its regulation.

The information that must be communicated to the public relating to the manner in which, to whom and where individuals may direct privacy inquiries shall also be identified. At a minimum, the information communicated to the public shall 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; and information as to where individuals may obtain further information about the privacy policies and procedures implemented by the prescribed entity.

The policy and procedures must further establish the process to be followed in receiving and responding to privacy inquiries. This shall include the agent(s) responsible for receiving and responding to privacy inquiries; any documentation that must be completed, provided, and/or executed; the required content of the documentation; and the format and content of the response to the privacy inquiry. The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures in Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited, and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures. The relationship between this policy and its procedures and the *Policy and Procedures for Privacy Complaints* and the *Policy and Procedures for Privacy Breach Management* shall also be addressed.

This policy and its associated procedures may either be a stand-alone document or may be combined with the *Policy and Procedures 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 "the Act" must be read as "the *CYFSA*"
- references to "personal health information" must be read as "personal information"
- references to "prescribed person or prescribed entity" must be read as "prescribed entity"
- references to "health information custodian" must be read as "service provider"
- special regard must be given to the breach notification requirements in section 6(3) of the regulation to the *CYFSA*

To comply with Part 2 of Appendix "B" to the *CYFSA* Addendum, stand-alone *CYFSA* policies and procedures may not be necessary. Instead, a prescribed entity may create *CYFSA* addenda to policies and procedures developed in accordance with parts 2, 3, and 4 of Appendix "B" of the *PHIPA* Manual.

Whichever approach is taken, a prescribed entity must have the necessary policies and procedures in place to ensure compliance.

APPENDIX "C"

PRIVACY, SECURITY, AND OTHER INDICATORS

PART 1 - PRIVACY INDICATORS

Categories	Privacy Indicators
General Privacy Policies and Procedures	• The dates that the privacy policies and procedures were reviewed by the prescribed entity since the prior review of the IPC. • Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure amended, a brief description of the amendments made. • Whether new privacy policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented. • The date that each amended and newly developed privacy policy and procedure was communicated to agents and, for each amended and newly developed privacy policy and procedure 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	• 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.
Use	• The number of agents granted approval to access and use personal information for purposes other than research. • 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.

Categories	Privacy Indicators
Disclosure	• 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 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. • 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.
Data Sharing Agreements	• 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.
Agreements with Third Party Service Providers	• The number of agreements executed with third party service providers with access to personal information since the prior review by the IPC.
Data Linkage	• The number and a list of data linkages of personal information approved since the prior review by the IPC.

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 recommendation,
	  ○ the date each recommendation was addressed or is proposed to be addressed, and
	  ○ the manner in which each recommendation was addressed or is proposed 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.

Categories	Privacy Indicators

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 proposed to be addressed, and
	  ○ the manner in which each recommendation was addressed or is proposed to be addressed.
	• 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 proposed to be addressed, and
	  ○ the manner in which each recommendation was addressed or is proposed to be addressed.

Privacy Breaches	• The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed entity since the prior review by the IPC.
	• With respect to each privacy breach or suspected privacy breach:
	  ○ the date that the notification was received,
	  ○ the extent of the privacy breach or suspected privacy breach,
	  ○ whether it was internal or external,
	  ○ the nature and extent of personal information at issue,
	  ○ the date that senior management was notified,
	  ○ the containment measures implemented,
	  ○ the date(s) that the containment measures were implemented,
	  ○ the date(s) that notification was provided to the service provider or any other persons or organizations, if applicable,
	  ○ the date that notification was provided to the IPC, if applicable,
	  ○ the date that the investigation was commenced,
	  ○ the date that the investigation was completed,
	  ○ a brief description of each recommendation made,
	  ○ the date each recommendation was addressed or is proposed to be addressed, and
	  ○ the manner in which each recommendation was addressed or is proposed to be addressed.

Categories	Privacy Indicators

Privacy Complaints	• 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 recommendation made,
	  ○ the date each recommendation was addressed or is proposed to be addressed,
	  ○ the manner in which each recommendation was addressed or is proposed to be addressed, and
	  ○ 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, and
	  ○ 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 - SECURITY INDICATORS

Categories	Security Indicators
General Security Policies and Procedures	• The dates that the security policies and procedures were reviewed by the prescribed entity since the prior review of the IPC. • Whether amendments were made to existing security policies and procedures as a result of the review and, if so, a list of the amended security policies and procedures and, for each policy and procedure amended, a brief description of the amendments made. • Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented. • The dates that each amended and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and procedure 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: o a brief description of each recommendation made, o the date each recommendation was addressed or is proposed to be addressed, and o the manner in which each recommendation was addressed or is proposed to be addressed.
Security Audit Program	• The dates of the review of system control and audit logs since the prior review by the IPC and a general description of the findings, if any, arising from the review of system control and audit logs. • The number and a list of security audits completed since the prior review by the IPC and for each audit: o a description of the nature and type of audit conducted, o the date of completion of the audit, o a brief description of each recommendation made, o the date that each recommendation was addressed or is proposed to be addressed, and o the manner in which each recommendation was addressed or is expected to be addressed.

Categories	Security Indicators

Information Security Breaches	• The number of notifications of information security breaches or suspected information security breaches received by the prescribed entity since the prior review by the IPC.
	• With respect to each information security breach or suspected information security breach:
	  ○ the date that the notification was received,
	  ○ the extent of the information security breach or suspected information security breach,
	  ○ the nature and extent of personal information at issue,
	  ○ the date that senior management was notified,
	  ○ the containment measures implemented,
	  ○ the date(s) that the containment measures were implemented,
	  ○ the date(s) that notification was provided to the service provider or to any other persons or organizations,
	  ○ the date that the investigation was commenced,
	  ○ the date that the investigation was completed,
	  ○ a brief description of each recommendation made,
	  ○ the date each recommendation was addressed or is proposed to be addressed, and
	  ○ the manner in which each recommendation was addressed or is proposed to be addressed.

PART 3 - HUMAN RESOURCES INDICATORS

Categories	Human Resources Indicators
Privacy Training and Awareness	• The number of agents who have received and who have not received initial privacy orientation since the prior review by the IPC. • The date of commencement of the employment, contractual, or other relationship for agents that have yet to receive initial privacy orientation and the scheduled date of the initial privacy orientation. • The number of agents who have attended and who have not attended 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.
Security Training and Awareness	• The number of agents who have received and who have not received initial security orientation since the prior review by the IPC. • The date of commencement of the employment, contractual, or other relationship for agents that have yet to receive initial security orientation and the scheduled date of the initial security orientation. • The number of agents who have attended and who have not attended ongoing 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 that 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 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], the [INSERT TITLE] of [INSERT NAME OF PRESCRIBED ENTITY], MAKE OATH AND SAY:

> [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.

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], the [INSERT TITLE] of [INSERT NAME OF PRESCRIBED ENTITY], MAKE OATH AND SAY:

1. [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.

2. The policies, procedures, and practices implemented by [INSERT NAME OF PRESCRIBED ENTITY] comply with the *Child, Youth and Family Services Act* 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.

4. [INSERT NAME OF PRESCRIBED ENTITY] has submitted a written report to the Information and Privacy Commissioner of Ontario 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 received is protected against theft, loss, and unauthorized 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

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

April 2020