January 2024

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 Persons and Prescribed Entities 1

Requirements for Disclosure to Prescribed Persons and Prescribed Entities 1

Purpose of this Manual 1

Other Manuals and Addenda 2

Review Process for Prescribed Persons and Prescribed Entities 3

Initial Review of the Prescribed Persons and Prescribed Entities 3

Three-Year Review of the Prescribed Persons and Prescribed Entities 6

Publication of Three-Year Review Documentation 11

Reviews under other Acts 11

Appendix A: List of Required Policies, Procedures, and Practices 12

Part 1 – Privacy Policies, Procedures, and Practices 12

Part 2 – Information Security Policies, Procedures, and Practices 14

Part 3 – Human Resources Policies, Procedures, and Practices 16

Part 4 – Organizational Policies, Procedures, and Practices 17

Appendix B: Minimum Content of Required Policies, Procedures, and Practices 18

Part 1 – Privacy Policies, Procedures, and Practices 18

General Privacy Policies, Procedures, and Practices 18

1. Privacy Policy in Respect of its Status as a Prescribed Person or Prescribed Entity 18

2. Policy, Procedures, and Practices for Ongoing Review of Privacy Policies, Procedures, and Practices 21

Transparency 23

3. Policy on the Transparency of Privacy Policies, Procedures, and Practices 23

Collection of Personal Health Information and Data Holdings 24

4. Policy, Procedures, and Practices for the Collection of Personal Health Information 24

5. List of Data Holdings Containing Personal Health Information 26

6. Policy, Procedures, and Practices for Maintaining Statements of Purpose for Data Holdings Containing Personal Health Information 27

7. Statements of Purpose for Data Holdings Containing Personal Health Information 28

Access and Use of Personal Health Information 28

8. Policy, Procedures, and Practices for Limiting Agent Access to and Use of Personal Health Information 28

9. Log of Agents Granted Approval to Access and Use Personal Health Information 32

10. Policy, Procedures, and Practices for the Use of Personal Health Information for Research 32

11. Log of Approved Uses of Personal Health Information for Research 37

Disclosure of Personal Health Information for Research 38

12. Policy, Procedures, and Practices for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements 38

13. Template Research Agreement 42

14. Log of Research Agreements 47

Disclosure of Personal Health Information for Purposes Other Than Research 48

15. Policy, Procedures, and Practices for Disclosure of Personal Health Information for Purposes Other Than Research 48

16. Policy, Procedures, and Practices for the Execution of Data Sharing Agreements 52

17. Template Data Sharing Agreement 53

18. Log of Data Sharing Agreements 57

Third-Party Service Provider Agreements 58

19. Policy, Procedures, and Practices for Executing Agreements with Third-Party Service Providers in Respect of Personal Health Information 58

20. Template Agreement for Third-Party Service Providers 61

21. Log of Agreements with Third-Party Service Providers 67

Data Linkage, De-Identification and Aggregation 67

22. Policy, Procedures, and Practices for the Linkage of Records of Personal Health Information 67

23. Log of Approved Linkages of Records of Personal Health Information 70

24. Policy, Procedures, and Practices with Respect to De-Identification and Aggregation 70

Privacy Impact Assessments 73

25. Policy, Procedures, and Practices for Privacy Impact Assessments 73

26. Log of Privacy Impact Assessments 76

Privacy Audit Program 77

27. Policy, Procedures, and Practices in Respect of Privacy Audits....77

28. Log of Privacy Audits 79

Privacy Breaches 79

29. Policy, Procedures, and Practices for Privacy Breach Management 79

30. Log of Privacy Breaches 85

Privacy Complaints and Inquiries....86

31. Policy, Procedures, and Practices for Privacy Complaints 86

32. Log of Privacy Complaints 90

33. Policy, Procedures, and Practices for Privacy Inquiries 91

Part 2 - Information Security Policies, Procedures, and Practices 93

General Information Security Policies, Procedures, and Practices 93

1. Information Security Policy 93

2. Policy, Procedures, and Practices for Ongoing Review of Information Security Policies, Procedures, and Practices....95

Physical Security 97

3. Policy, Procedures, and Practices for Ensuring Physical Security of Personal Health Information 97

4. Policy, Procedures, and Practices with Respect to Access by Agents....97

5. Policy, Procedures, and Practices with Respect to Access by Visitors 101

6. Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity 102

Secure Retention, Transfer, and Disposal 102

7. Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information 102

8. Policy, Procedures, and Practices for Securing Records of Personal Health Information on Mobile Devices and Remotely Accessing Personal Health Information 103

9. Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information 108

10. Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information 110

Information Security 112

11. Policy, Procedures, and Practices Relating to Authentication and Passwords 112

12. Policy, Procedures, and Practices in Respect of Privacy Flags and Notices to Agents....114

13. Policy, Procedures, and Practices for Logging, Monitoring, and Auditing Privacy and Information Security Events 115

14. Policy, Procedures, and Practices for Vulnerability and Patch Management....123

15. Policy, Procedures, and Practices Related to Change Management....129

16. Policy, Procedures, and Practices for Back-Up and Recovery of Records of Personal Health Information 131

17. Policy, Procedures, and Practices on the Acceptable Use of Technology....132

Information Security Audit Program....134

18. Policy, Procedures, and Practices in Respect of Information Security Audits....134

19. Log of Information Security Audits 137

Information Security Breaches 137

20. Policy, Procedures, and Practices for Information Security Breach Management 137

21. Log of Information Security Breaches 143

Part 3 – Human Resources Policies, Procedures, and Practices.... 145

Privacy Training and Awareness....145

1. Policy, Procedures, and Practices for Privacy Training and Awareness 145

2. Log of Completion of Initial and Ongoing Privacy Training 149

Information Security Training and Awareness 149

3. Policy, Procedures, and Practices for Information Security Training and Awareness.....149

4. Log of Completion of Initial and Ongoing Information Security Training.....153

Confidentiality Agreements 153

5. Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Agents 153

6. Template Confidentiality Agreement with Agents.....155

7. Log of Executed Confidentiality Agreements with Agents 157

Privacy and Information Security Leadership.....157

8. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program.....157

9. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Information Security Program.....158

Termination or Cessation.....159

10. Policy, Procedures, and Practices upon Termination or Cessation of the Employment or Contractual Relationship 159

Discipline and Corrective Action.....161

11. Policy, Procedures, and Practices for Discipline and Corrective Action.....161

Part 4 – Organizational Policies, Procedures, and Practices 162

Governance and Accountability.....162

1. Privacy Governance and Accountability Framework.....162

2. Information Security Governance and Accountability Framework.....164

3. Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Information Security Program 166

Risk Management.....166

4. Corporate Risk Management Framework 166

5. Corporate Risk Register.....169

6. Policy, Procedures, and Practices for Maintaining a Consolidated Log of Recommendations 170

7. Consolidated Log of Recommendations 171

Business Continuity and Disaster Recovery.....171

8. Business Continuity and Disaster Recovery Plan 171

Appendix C: Privacy, Information Security, Human Resources, and Organizational Indicators 176

Part 1 – Privacy Indicators..... 176

Part 2 – Information Security Indicators 182

Part 3 – Human Resources Indicators 186

Part 4 – Organizational Indicators 187

Appendix D: Sworn Affidavit..... 188

Appendix E: Glossary 190

Process for the Review and Approval of Prescribed Persons and Prescribed Entities

The ***Personal Health Information Protection Act, 2004*** (PHIPA) is a consent-based statute, meaning that persons or organizations in the health sector defined as **health information custodians** ("custodians") may only collect, use, and disclose **personal health information** ("PHI") with the consent of the individual to whom the PHI relates, subject to limited exceptions where PHIPA permits or requires the collection, use, or disclosure to be made without consent.

One such disclosure that is permitted without consent is the disclosure of PHI to **prescribed persons** ("PPs") that compile or maintain registries of PHI for the purpose of facilitating or improving the provision of health care, or that relate to the storage or donation of body parts or bodily substances pursuant to clause 39(1)(c) of PHIPA. Another such disclosure that is permitted without consent is the disclosure of PHI to **prescribed entities** ("PEs") for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system pursuant to subsection 45(1) of PHIPA.

These disclosures are permitted without consent provided that the PPs and PEs comply with the requirements set out in PHIPA and Regulation 329/04 as well as in any other regulation(s) that may be enacted under PHIPA ("regulations").

Requirements for Disclosure to Prescribed Persons and Prescribed Entities

In order for a **custodian** to be permitted to disclose PHI to a PP or PE without consent, the PP or PE must have in place practices and procedures approved by the Information and Privacy Commissioner of Ontario (the "IPC") to protect the privacy of individuals whose PHI it receives and to maintain the confidentiality of that information. In the case of a PP, this requirement is set out in subsection 13(2) of Regulation 329/04 of PHIPA. In the case of a PE, this requirement is set out in subsection 45(3) of PHIPA.

These practices and procedures must also be reviewed by the IPC every three years from the date of their initial approval in order for a custodian to be able to continue to disclose PHI to a PP or PE without consent, and in order for the PP or PE to be able to continue to collect, use, and disclose PHI without consent as permitted by PHIPA and its regulations. In the case of a PP, this requirement is set out in subsection 13(2) of PHIPA's regulations. In the case of a PE, this requirement is set out in subsection 45(4) of PHIPA.

Purpose of this Manual

The purpose of the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("the Manual") is to outline the process to be followed by the IPC in reviewing the practices and procedures implemented by PPs and PEs to protect the privacy of individuals whose PHI they receive and to maintain the confidentiality of that information. The purpose of the Manual is also to set out the requirements that are reasonably necessary to protect the PHI

that PPs and PEs are permitted to collect, and to assist PPs and PEs in complying with their obligations under PHIPA and its regulations.

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

Please note, throughout the Manual, "**must**" indicates a requirement and "**should**" indicates a recommendation. The IPC may amend the Manual from time to time. It is the responsibility of the PPs and PEs to ensure continued compliance with the Manual.

Other Manuals and Addenda

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

Under the ***Child, Youth and Family Services Act, 2017*** (CYFSA) PEs named under that law may collect personal information without individuals' consent from service providers and use that personal information for analysis and compiling statistics in relation to the planning and management of services for children, youth, and families. Like PPs and PEs under PHIPA, PEs under the CYFSA must have their practices and procedures reviewed by the IPC every three years. The IPC maintains **The *Child, Youth and Family Services Act* Addendum to the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities** that sets out the requirements for review and approval of PEs under the CYFSA.

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

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

Review Process for Prescribed Persons and Prescribed Entities

Each PP and PE is required to have in place practices and procedures to protect the privacy of individuals whose PHI it receives and to maintain the confidentiality of that information. At a minimum, these practices and procedures must:

- include the policies, procedures, practices, agreements, and other documentation set out in **appendix A**, and
- contain the minimum content set out in **appendix B** to the Manual.

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

- nature of the functions performed by the PPs and PEs
- amount and sensitivity of the PHI collected
- number and roles of the individuals with access to the PHI, and
- obligations and duties of the PPs and PEs under PHIPA and its regulations.

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

Initial Review of the Prescribed Persons and Prescribed Entities

Each PP and PE seeking the initial approval of the IPC in respect of the practices and procedures implemented to protect the privacy of individuals whose PHI it receives and to maintain the confidentiality of that information, must submit to the IPC the applicable policies, procedures, and practices described in **appendix A** and containing the minimum content set out in **appendix B** to the Manual. These policies, procedures, and practices must be submitted at least six months prior to the date that the approval of the IPC is requested.

Statements of Requested Exceptions

If there is, or is expected to be, a divergence between the policies, procedures, and practices of the PP or PE and the requirements in **appendix A** or **appendix B** of the Manual, the PP or PE must provide a written **Statement of Requested Exceptions** at the same time they submit their policies, procedures, and practices to the IPC. The Statement of Requested Exceptions must identify each requirement of the Manual from which the PP or PE's policies, procedures, and practices will or currently diverge, together with a rationale.

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

- a detailed plan and timeline for achieving compliance with the requirement, or
- an explanation for why an exception to the requirement in the Manual should be granted by the IPC and how the PP or PE has achieved, or will achieve, an equivalent standard to protect the privacy of the individuals whose PHI it receives and maintain the confidentiality

of the information; where a PP or PE has not yet achieved an equivalent standard, it must provide a detailed plan and timeline for achieving the equivalent standard.

Statements of Inapplicability

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

IPC Review of Submitted Materials

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

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

On-Site Meeting

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

- discuss the policies, procedures, and practices implemented by the PP or PE,
- provide the IPC with an opportunity to ask questions arising from the review of the policies, procedures, and practices implemented, and
- provide the IPC with an opportunity to review the physical security measures put in place to protect PHI.

Approval Process

Following the on-site meeting:

- The PP or PE will be informed of any actions it is required to take prior to the approval of its policies, procedures, and practices.
- Once all necessary actions have been taken, the IPC will prepare and provide to the PP or PE a draft report for review and comment.
- The report, letter of approval, and any approved Statements of Requested Exceptions and Statements of Inapplicability will be finalized.
- The finalized report will be posted on the IPC's website, along with a letter of approval and any approved Statements of Requested Exceptions and Statements of Inapplicability.

- The PP or PE will also be required to have a statement on its website informing the public that this documentation is publicly available on the IPC's website, and must provide a link to the IPC's website where the PP or PE's documentation is made available.

Amending or Withdrawing Statements of Requested Exceptions or Statements of Inapplicability

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

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

Approval Letter

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

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

In Case of No Approval

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

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

Three-Year Review of the Prescribed Persons and Prescribed Entities

Preliminary Information to be Submitted

One year plus three months prior to the date that the continued approval is required pursuant to PHIPA and its regulations, each PP and PE seeking the continued approval of its policies, procedures, and practices must submit its Privacy, Information Security, Human Resources, and Organizational indicators as set out in **appendix C** of the Manual (the "indicators"). Typically, approval is provided by October 31 of the required approval year; therefore, in typical circumstances, PPs and PEs will submit their indicators to the IPC on August 1 of the year prior to the required approval year.

Such indicators must be attached as an exhibit to a sworn affidavit, the template of which is set out in **appendix D** of the Manual (the "sworn affidavit").

The sworn affidavit must be executed by the chief executive officer or the executive director (or equivalent position), as the case may be, who is ultimately accountable for ensuring that the policies, procedures, and practices of the PP or PE comply with PHIPA and its regulations, as elaborated by the requirements in appendices A and B of the Manual, and has taken steps that are reasonable in the circumstances to ensure that these policies, procedures, and practices are implemented.

The IPC may request that the sworn affidavit be resubmitted during the IPC's three-year review, including where the previously submitted affidavit does not comply with the requirements of appendix D, or the exhibits to that affidavit do not comply with the requirements of the Manual, or where the sworn affidavit is otherwise no longer accurate.

Statements of Requested Exceptions

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

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

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

Statements of Inapplicability

Where one or more of the requirements in **appendix A** or **appendix B** is inapplicable to a PP or PE, the PP or PE need not submit a **Statement of Requested Exceptions** but must instead provide the IPC with a **Statement of Inapplicability** attached as an exhibit to the sworn affidavit. The Statement of Inapplicability must identify each requirement that is inapplicable (if any), together with a rationale.

IPC Review of Submitted Materials

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

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

Selection of Policies, Procedures, and Practices

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

- whether there have been any changes to the PP's or PE's policies, procedures, and practices since the last review by the IPC
- privacy and information security issues (including recommendations) identified during previous reviews of the PP or PE
- whether the policies, procedures, and practices have been recently reviewed by the IPC in following up on the status of recommendations made during the last review

- privacy and information security issues, including any privacy or information security breaches, identified through ongoing, current, or previous IPC consultations with the PP or PE
- results of privacy and information security audits conducted by the PP or PE since the last review
- recent decisions, guidelines, fact sheets, etc. issued by the IPC or other relevant oversight offices
- privacy and information security trends emerging from complaints and privacy and information security breaches reported to the IPC
- privacy and information security trends identified through the IPC's environmental scanning function
- privacy and information security issues recently reported in the media more generally
- privacy and information security issues identified in a Statement of Requested Exceptions or a Statement of Inapplicability
- changes in requirements arising from new or amended laws or regulations
- evolving industry privacy and information security standards and best practices, and
- any other information the IPC and the PP or PE may consider relevant and important for the purposes of the review.

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

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

In its sole discretion, the IPC may expand the scope of its review at any time during the review period to include other policies, procedures, and practices that are the subject of the IPC's review under subsection 45(4) of PHIPA or subsection 13(2) of its regulations, depending on the level of privacy and information security risks revealed in the information and documentation provided by the PP or PE.

Review of Selected Policies, Procedures, and Practices

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

The IPC will review the selected policies, procedures, and practices. The IPC will assess whether the PP's or PE's policies, procedures, and practices protect the privacy of individuals whose PHI the PP or PE receives and maintain the confidentiality of that information, and whether the PP or PE is adhering to these policies, procedures, and practices. At a minimum, the IPC will assess whether the selected policies, procedures, and practices sufficiently address the content set out in **appendix B** of this Manual.

Approval Process

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

Further examination may include one or more of the following:

- a detailed review by the IPC of additional policies, procedures, and practices of the PP or PE
- requests for further details or clarifications regarding the submitted indicators, as may be necessary to assess compliance with the requirements set out in the Manual
- a request for further documentation from the PP or PE with respect to one or more of its policies, procedures, and practices
- interviews with relevant personnel of the PP or PE
- a request for further supporting evidence demonstrating how the PP or PE is implementing or complying with its practices or procedures, or results of recent assessments or audits
- a request to meet with representatives of the PP or PE to discuss the implementation of, and compliance with, its policies, procedures, and practices
- an on-site visit at the premises of the PP or PE to further assess implementation of, and compliance with, its policies, procedures, and practices, and
- an assessment of any other aspect of the PP or PE deemed relevant and appropriate in the sole discretion of the IPC.

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

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

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

Amending or Withdrawing Statements of Requested Exceptions or Statements of Inapplicability

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

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

Approval Letter

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

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

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

In Case of No Approval

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

In the case where the practices and procedures of a PP or PE are not approved for a further three-year period on the date that continued approval is required pursuant to PHIPA and its regulations, the IPC will inform the PP or PE in writing of the reasons why approval was not granted, including the significant divergence(s) that must be addressed by the PP or PE prior to regaining approval.

The PP or PE may resubmit its policies, procedures and practices and any other requested documentation for approval by the IPC, as described in the IPC's letter. Once the significant divergence(s) have been adequately addressed, approval will be provided to resume operating as a PP or PE. To prevent undue delay in resumption of PP or PE activities, this approval may be provided in the intervening time period between typical three-year review periods.

Publication of Three-Year Review Documentation

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

PPs and PEs are also required to have a statement on their respective public-facing websites that informs the public that this documentation is publicly available on the IPC's website and must provide a link to the IPC's website where the PP or PE's documentation is made available.

In Case of Confidential Content

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

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

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

Reviews under other Acts

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

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

Part 1 – Privacy Policies, Procedures, and Practices

Categories	Required Policies, Procedures, and Practices	Page No. Appendix B
General Privacy Policies, Procedures and Practices	1. *Privacy Policy in Respect of its Status as a Prescribed Person or Prescribed Entity*	18
	2. *Policy, Procedures, and Practices for Ongoing Review of Privacy Policies, Procedures, and Practices*	21
Transparency	3. *Policy on the Transparency of Privacy Policies, Procedures, and Practices*	23
Collection of Personal Health Information and Data Holdings	4. *Policy, Procedures, and Practices for the Collection of Personal Health Information*	24
	5. *List of Data Holdings Containing Personal Health Information*	26
	6. *Policy, Procedures, and Practices for Maintaining Statements of Purpose for Data Holdings Containing Personal Health Information*	27
	7. *Statements of Purpose for Data Holdings Containing Personal Health Information*	28
Access and Use of Personal Health Information	8. *Policy, Procedures, and Practices for Limiting Agent Access to and Use of Personal Health Information*	28
	9. *Log of Agents Granted Approval to Access and Use Personal Health Information*	32
	10. *Policy, Procedures, and Practices for the Use of Personal Health Information for Research*	32
	11. *Log of Approved Uses of Personal Health Information for Research*	37
Disclosure of Personal Health Information for Research	12. *Policy, Procedures, and Practices for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements*	38
	13. *Template Research Agreement*	42
	14. *Log of Research Agreements*	47

Categories	Required Policies, Procedures, and Practices	Page No. Appendix B
Disclosure of Personal Health Information for Purposes Other Than Research	15. *Policy, Procedures, and Practices for Disclosure of Personal Health Information for Purposes Other Than Research*	48
	16. *Policy, Procedures, and Practices for the Execution of Data Sharing Agreements*	52
	17. *Template Data Sharing Agreement*	53
	18. *Log of Data Sharing Agreements*	57
Third-Party Service Provider Agreements	19. *Policy, Procedures, and Practices for Executing Agreements with Third-Party Service Providers in Respect of Personal Health Information*	58
	20. *Template Agreement for Third-Party Service Providers*	61
	21. *Log of Agreements with Third-Party Service Providers*	67
Data Linkage, De-Identification and Aggregation	22. *Policy, Procedures, and Practices for the Linkage of Records of Personal Health Information*	67
	23. *Log of Approved Linkages of Records of Personal Health Information*	70
	24. *Policy, Procedures, and Practices with Respect to De-Identification and Aggregation*	70
Privacy Impact Assessments	25. *Policy, Procedures, and Practices for Privacy Impact Assessments*	73
	26. *Log of Privacy Impact Assessments*	76
Privacy Audit Program	27. *Policy, Procedures, and Practices in Respect of Privacy Audits*	77
	28. *Log of Privacy Audits*	79
Privacy Breaches	29. *Policy, Procedures, and Practices for Privacy Breach Management*	79
	30. *Log of Privacy Breaches*	85
Privacy Complaints and Inquiries	31. *Policy, Procedures, and Practices for Privacy Complaints*	86
	32. *Log of Privacy Complaints*	90
	33. *Policy, Procedures, and Practices for Privacy Inquiries*	91

Part 2 – Information Security Policies, Procedures, and Practices

Categories	Required Policies, Procedures, and Practices	Page No. Appendix B
General Information Security Policies, Procedures and Practices	1. ***Information Security Policy***	93
	2. ***Policy, Procedures, and Practices for Ongoing Review of Information Security Policies, Procedures, and Practices***	95
Physical Security	3. ***Policy, Procedures, and Practices for Ensuring Physical Security of Personal Health Information***	97
	4. ***Policy, Procedures, and Practices with Respect to Access by Agents***	97
	5. ***Policy, Procedures, and Practices with Respect to Access by Visitors***	101
	6. ***Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity***	102
Secure Retention, Transfer and Disposal	7. ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information***	102
	8. ***Policy, Procedures, and Practices for Securing Records of Personal Health Information on Mobile Devices and Remotely Accessing Personal Health Information***	103
	9. ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information***	108
	10. ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information***	110
Information Security	11. ***Policy, Procedures, and Practices Relating to Authentication and Passwords***	112
	12. ***Policy, Procedures, and Practices in Respect of Privacy Flags and Notices to Agents***	114
	13. ***Policy, Procedures, and Practices for Logging, Monitoring, and Auditing Privacy and Information Security Events***	115
	14. ***Policy, Procedures, and Practices for Vulnerability and Patch Management***	123
	15. ***Policy, Procedures, and Practices Related to Change Management***	129
	16. ***Policy, Procedures, and Practices for Back-Up and Recovery of Records of Personal Health Information***	131

Categories	Required Policies, Procedures, and Practices	Page No. Appendix B
Information Security (Cont'd)	17. ***Policy, Procedures, and Practices on the Acceptable Use of Technology***	132
Information Security Audit Program	18. ***Policy, Procedures and Practices in Respect of Information Security Audits***	134
	19. ***Log of Information Security Audits***	137
Information Security Breaches	20. ***Policy, Procedures and Practices for Information Security Breach Management***	137
	21. ***Log of Information Security Breaches***	143

Part 3 – Human Resources Policies, Procedures, and Practices

Categories	Required Policies, Procedures, and Practices	Page No. Appendix B
Privacy Training and Awareness	1. ***Policy, Procedures, and Practices for Privacy Training and Awareness***	145
	2. ***Log of Completion of Initial and Ongoing Privacy Training***	149
Information Security Training and Awareness	3. ***Policy, Procedures, and Practices for Information Security Training and Awareness***	149
	4. ***Log of Completion of Initial and Ongoing Information Security Training***	153
Confidentiality Agreements	5. ***Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Agents***	153
	6. ***Template Confidentiality Agreement with Agents***	155
	7. ***Log of Executed Confidentiality Agreements with Agents***	157
Privacy and Information Security Leadership	8. ***Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program***	157
	9. ***Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Information Security Program***	158
Termination or Cessation	10. ***Policy, Procedures, and Practices upon Termination or Cessation of the Employment or Contractual Relationship***	159
Discipline and Corrective Action	11. ***Policy, Procedures, and Practices for Discipline and Corrective Action***	161

Part 4 – Organizational Policies, Procedures, and Practices

Categories	Required Policies, Procedures, and Practices	Page No. Appendix B
Governance and Accountability	1. ***Privacy Governance and Accountability Framework***	162
	2. ***Information Security Governance and Accountability Framework***	164
	3. ***Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Information Security Program***	166
Risk Management	4. ***Corporate Risk Management Framework***	166
	5. ***Corporate Risk Register***	169
	6. ***Policy, Procedures, and Practices for Maintaining a Consolidated Log of Recommendations***	170
	7. ***Consolidated Log of Recommendations***	171
Business Continuity and Disaster Recovery	8. ***Business Continuity and Disaster Recovery Plan***	171

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

Part 1 – Privacy Policies, Procedures, and Practices

General Privacy Policies, Procedures, and Practices

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

Status under the *Personal Health Information Protection Act*

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

The Privacy Policy must also articulate a commitment by the PP or PE to comply with the provisions of PHIPA and its regulations applicable to PPs or PEs, as the case may be.

Privacy and Information Security Accountability Framework

The Privacy Policy must also describe the accountability framework for ensuring compliance with PHIPA and its regulations and for ensuring compliance with the privacy and information security policies, procedures, and practices implemented by the PP or PE.

In particular, the Privacy Policy must:

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

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

Collection of Personal Health Information

The Privacy Policy must:

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

Use of Personal Health Information

The Privacy Policy must identify the purposes for which the PP or PE uses PHI. In identifying these purposes, the Privacy Policy must:

- clearly distinguish between the use of PHI and the use of de-identified and/or aggregate information
- distinguish between the use of PHI for purposes of clause 39(1)I or subsection 45(1) of PHIPA, as the case may be, and the use of PHI for research purposes
- ensure that each use of PHI identified in the Privacy Policy is consistent with the uses of PHI permitted by PHIPA and its regulations
- articulate a commitment by the PP or PE not to use PHI if other information will serve the purpose and not to use more PHI than is reasonably necessary to meet the purpose, and
- identify some of the policies, procedures, and practices implemented by the PP or PE to fulfill these data minimization requirements, including limits on the use of PHI by agents.

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

Disclosure of Personal Health Information

The Privacy Policy of the PP or PE must:

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

Secure Retention, Transfer, and Disposal of Records of Personal Health Information

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

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

Implementation of Administrative, Technical, and Physical Safeguards

The Privacy Policy must outline some of the administrative, technical, and physical safeguards implemented to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information, including the steps taken to protect PHI against theft, loss, and unauthorized collection, use, or disclosure, and to protect records of PHI against unauthorized copying, modification, or disposal.

Inquiries, Concerns, or Complaints Related to Information Practices

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

Specifically, the Privacy Policy must:

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

Compliance, Audit, and Enforcement

The Privacy Policy must:

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

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

A policy, procedures, and practices must be developed and implemented for the ongoing review of the PP's or PE's privacy policies, procedures, and practices ("policy, procedures, and practices for ongoing review"). The purpose of this ongoing review is to determine on a regular basis whether amendments are needed or whether new privacy policies, procedures, and practices are required.

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

- frequency of the review of the privacy policies, procedures, and practices, which at minimum must be reviewed at least once prior to each three-year review by the IPC
- agent(s) responsible and the procedure for undertaking the review
- timeframe in which the review will be undertaken

- agent(s) responsible and the procedure for amending and/or drafting new privacy policies, procedures, and practices
- agent(s) responsible, and the procedure, for seeking and providing approval of any amendments or newly-developed privacy policies, procedures, and practices, if deemed necessary as a result of the review
- agent(s) responsible and the procedure for communicating the amended or newly developed privacy policies, procedures, and practices, and
- method and nature of the communication to agents, the public, and other stakeholders, as may be relevant, depending on the nature of the subject matter.

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

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

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

Transparency

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

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

At a minimum, the Transparency Policy must require the PP or PE to make the following information publicly available:

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

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

Brochures, Frequently Asked Questions, and Other Plain Language Tools

The Transparency Policy must set out the minimum content of the brochures, frequently asked questions, and/or other plain language tools and in particular, such content must:

- describe the status of the PP or PE under PHIPA, the duties and responsibilities arising from this status, and the privacy policies, procedures, and practices implemented in respect of PHI, including the:
    - types of PHI collected and the persons or organizations from which this PHI is typically collected
    - purposes for which PHI is collected
    - purposes for which PHI is used, and if identifiable information is not routinely used, the nature of the information that is used, and
    - circumstances in which and the purposes for which PHI is disclosed, and the persons or organizations to which it is typically disclosed

- identify some of the administrative, technical, and physical safeguards implemented to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information, including the steps taken to protect PHI against theft, loss, and unauthorized collection, use, or disclosure, and to protect records of PHI against unauthorized copying, modification, or disposal, and
- provide the name and/or title, mailing address, and contact information of the agent(s) to whom inquiries, concerns, or complaints may be directed regarding the PP's or PE's compliance with the privacy policies, procedures, and practices.

Statement on Public Website

The PP or PE must have a statement on its website informing the public of the IPC's:

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

Collection of Personal Health Information and Data Holdings

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

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

- the purposes for which PHI will be collected by the PP or PE
- the nature of the PHI that will be collected
- from whom the PHI will typically be collected, and
- the secure manner in which PHI will be collected.

The policy, procedures, and practices must articulate a commitment by the PP or PE not to collect:

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

Review and Approval Process for Collection of Personal Health Information

The policy, procedures, and practices must identify the:

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

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

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

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

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

Conditions or Restrictions on the Approval to Collect Personal Health Information

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

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

Secure Retention, Transfer, Return, or Disposal of Personal Health Information

The policy, procedures, and practices must require that:

- records of PHI collected by the PP or PE be retained in a secure manner in compliance with the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information***
- records of PHI collected by an agent of the PP or PE be transferred in a secure manner in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information***, and
- identification of the agent(s) responsible for ensuring that the records of PHI 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 be set out in any documentation and/or agreements and executed prior to the collection of the PHI.

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

5. List of Data Holdings Containing Personal Health Information

The PP or PE must develop and retain an up-to-date list and brief description of the data holdings of PHI maintained by the PP or PE.

6. Policy, Procedures, and Practices for Maintaining Statements of Purpose for Data Holdings Containing Personal Health Information

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

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

- set out the purpose of the data holding
- describe the PHI contained in the data holding
- identify the source(s) of the PHI
- explain the need for the PHI in relation to the identified purpose, and
- explain why de-identified and/or aggregate information will not serve the identified purpose.

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

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

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

7. Statements of Purpose for Data Holdings Containing Personal Health Information

For each data holding containing PHI, the PP or PE must complete a statement identifying the purpose of the data holding, the PHI contained in the data holding, the source(s) of the PHI, the need for the PHI in relation to the identified purpose, and why de-identified and/or aggregate information will not serve the identified purpose.

Access and Use of Personal Health Information

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

A policy, procedures, and practices must be developed and implemented to limit access to and use of PHI by agents based on the "need to know" principle. The purpose of this policy, procedures, and practices is to ensure that agents of the PP or PE access and use the least identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual, or other responsibilities.

The policy, procedures, and practices must:

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

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

The policy, procedures, and practices must explicitly prohibit access to and use of PHI 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 PHI than is reasonably necessary to meet the identified purpose.

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

Review and Approval Process for Allowing Access and Use by Agents

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

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

- requirements to be satisfied in requesting, reviewing, and determining whether to approve or deny a request by an agent for access to and use of PHI
- 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 PHI and the criteria for determining the appropriate level of access
- manner of documenting the decision approving or denying the request for access to and use of PHI and the reasons for the decision
- method and format in which the decision will be communicated and to whom
- documentation that must be completed, provided, and/or executed upon rendering the decision
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom the documentation must be provided, and
- required content of the documentation.

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

- the agent making the request routinely requires access to and use of PHI 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 PHI is being requested is permitted by PHIPA and its regulations
- the identified purpose for which access to and use of PHI is being requested cannot reasonably be accomplished without PHI
- de-identified and/or aggregate information will not serve the identified purpose, and
- no more PHI will be accessed and used than is reasonably necessary to meet the identified purpose.

Conditions or Restrictions on the Approval

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

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

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

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

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

Notification and Termination of Access and Use by Agents

The policy, procedures, and practices must require an agent granted approval to access and use PHI, or his or her supervisor, to notify the PP or PE when the agent is no longer employed or retained by the PP or PE or no longer requires such access. In this regard, the policy, procedures, and practices must:

- set out the procedure to be followed in providing the notification
- identify the agent(s) to whom this notification must be provided
- stipulate the timeframe within which this notification must be provided
- specify the nature and format of the notification

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

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

Secure Retention and Disposal

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

Tracking Approved Access to and Use of Personal Health Information

The policy, procedures, and practices must:

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the PP or PE at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an agent breaches or believes there may have been breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices

- address how and by whom compliance will be enforced and the consequences of breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***, and
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices In Respect of Privacy Audits***.

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

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

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

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

A policy, procedures, and practices must be developed and implemented to identify whether and in what circumstances, if any, the PP or PE permits PHI to be used for research purposes. If the PP or PE does not permit PHI to be used for research purposes, the policy, procedures, and practices must explicitly prohibit the use of PHI for research purposes. If the PP or PE does not permit **de-identified and/or aggregate information** to be used for research purposes, the policy, procedures, and practices must explicitly prohibit such use as well.

Where the Use of Personal Health Information is Permitted for Research

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

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

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

The policy, procedures, and practices must:

- clearly distinguish between the use of PHI for research purposes and the use of PHI for purposes of compiling or maintaining a registry of PHI under clause 39(1) or for purposes of analysis or compiling statistical information with respect to managing, evaluating,

monitoring, planning for, or allocating resources to, the health system under subsection 45(1) of PHIPA, as the case may be, and

- identify the criteria that must be considered in distinguishing between these uses, as well as the agent(s) responsible and the procedure to be followed in making this determination.

Review and Approval Process for Research Purposes

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

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

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

- requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request to use PHI for research purposes, having regard to PHIPA and its regulations
- manner of documenting the decision approving or denying the request to use PHI for research purposes and the reasons for the decision, and
- method and format in which the decision will be communicated, and to whom.

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

- the written **research plan** complies with the requirements in PHIPA and its regulations
- the written research plan has been approved by a research ethics board
- the PP or PE is in receipt of a copy of the decision of the research ethics board approving the written research plan
- the PHI being requested is consistent with the PHI identified in the written research plan approved by the research ethics board
- other information, namely de-identified and/or aggregate information, will not serve the research purpose, and
- no more PHI is being requested than is reasonably necessary to meet the research purpose.

Conditions or Restrictions on the Approval for Research Purposes

Having regard to PHIPA and its regulations, the policy, procedures, and practices must identify the conditions or restrictions that will be imposed on the approval to use PHI for research

purposes. At a minimum, the agent(s) granted approval to use PHI for research purposes must be required to comply with clauses 44(6) (a) to (f) of PHIPA.

The policy, procedures, and practices must also:

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

Secure Return of Records of Personal Health Information

If the records of PHI are required to be securely returned to the PP or PE, the policy, procedures, and practices must require the records to be transferred in a secure manner and in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of PHI***.

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

Secure Disposal of Records of Personal Health Information

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

Certificate of Destruction

The policy, procedures, and practices must identify the:

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

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

- identify the records of PHI securely disposed of
- indicate the date, time, and method of secure disposal employed, and
- bear the name and signature of the agent who performed the secure disposal.

De-Identification of Records of Personal Health Information

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

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

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

Tracking Approved Uses of Personal Health Information for Research

The policy, procedures, and practices must:

- require that a log be maintained of the approved uses of PHI for research purposes
- identify the agent(s) responsible for maintaining such a log
- 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 PHI for research purposes will be retained, and
- identify the agent(s) responsible for retaining this documentation.

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

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

Review and Approval Process

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

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

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

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

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

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

Conditions or Restrictions on the Approval

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

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

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

11. Log of Approved Uses of Personal Health Information for Research

A PP or PE that permits the use of PHI 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 date that the approval to use PHI for research purposes was granted by the PP or PE
- the date that the PHI was provided to the agent(s)
- the nature of the PHI provided to the agent(s)
- the retention period for the records of PHI identified in the written research plan approved by the research ethics board
- whether the records of PHI will be securely returned, securely disposed of, or **de-identified** and retained following the retention period, and
- the date the records of PHI were securely returned or a **certificate of destruction** was received or the date by which the records of PHI must be returned or disposed of, if applicable.

Disclosure of Personal Health Information for Research

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

A policy, procedures, and practices must be developed and implemented to identify whether and in what circumstances, if any, the PP or PE permits PHI to be disclosed for research purposes. If the PP or PE does not permit PHI to be disclosed for research purposes, the policy, procedures, and practices must explicitly prohibit the disclosure of PHI for research purposes and indicate whether or not de-identified and/or aggregate information may be disclosed for research purposes.

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

Where the Disclosure of Personal Health Information is Permitted for Research

Where the PP or PE permits the disclosure of PHI for research purposes, the policy, procedures, and practices must:

- articulate a commitment by the PP or PE not to disclose PHI for research purposes if other information will serve the research purpose and not to disclose more PHI than is reasonably necessary to meet the research purpose, and
- set out the circumstances in which PHI is permitted to be disclosed for research purposes.

Review and Approval Process

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

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

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

At a minimum, prior to any approval of the disclosure of PHI for research purposes, the policy, procedures, and practices must require the agent(s) responsible for determining whether to approve or deny the request to ensure that:

- the PP or PE is in receipt of a written application accompanied by a written **research plan** and a copy of the decision of the research ethics board approving the written research plan
- the written research plan complies with the requirements in PHIPA and its regulations
- the PHI being requested is consistent with the PHI identified in the written research plan approved by the research ethics board
- other information, namely **de-identified and/or aggregate information**, will not serve the research purpose, and
- no more PHI is being requested than reasonably necessary to meet the research purpose.

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

- the manner of documenting the decision approving or denying the request for the disclosure of PHI for research purposes and the reasons for the decision
- 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, procedures, and practices must identify the conditions or restrictions that are required to be satisfied prior to the approval of disclosure of PHI for research purposes, including any documentation and/or agreements that must be completed, provided, or executed and the agent(s) or researcher responsible for completing, providing, or executing the documentation and/or agreements. At a minimum, the policy, procedures, and practices must:

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

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

The policy, procedures, and practices must:

- identify the agent(s) responsible for ensuring that records of PHI disclosed to a researcher for research purposes are either securely returned, securely disposed of, or de-identified in compliance with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***, as the case may be, within a specific timeframe following the retention period set out in the Research Agreement, and

- address the process to be followed by the responsible agent(s) where records of PHI are not securely returned, a **certificate of destruction** is not received, or written confirmation of de-identification is not received within the time set out in the Research Agreement.

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

The policy, procedures, and practices must also:

- address where documentation related to the receipt, review, approval, or denial of requests for the disclosure of PHI for research purposes will be retained, including written applications, written **research plans**, copies of the decisions of research ethics boards, **Research Agreements**, and **certificates of destruction**, and
- identify the agent(s) responsible for retaining this documentation.

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

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

Review and Approval Process

The policy, procedures, and practices must identify 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, and the request process that must be followed. At a minimum, the request process must set out the:

- documentation that must be completed, provided, and/or executed by agent(s) of the PP or PE or by a researcher, having regard to PHIPA and its regulations
- agent(s) to whom this documentation must be provided
- required content of the documentation
- manner of documenting the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for research purposes and the reasons for the decision, and
- method and format in which the decision will be communicated, and to whom.

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

The policy, procedures, and practices must also address the requirements that must be satisfied and the criteria that must be considered by the 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, procedures, and practices must:

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

Conditions or Restrictions on the Approval

The policy, procedures, and practices must:

- comply with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***, and
- 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 PP or PE must require the researcher to whom the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the researcher will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is permitted by PHIPA or another law and is in accordance with the written **research plan** approved by the research ethics board. This must include prohibiting any attempt to decrypt information that is encrypted or identifying an individual based on unencrypted information and/or prior knowledge.

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

The policy, procedures, and practices must also:

- identify the documentation and/or agreements that must be completed, provided, or executed and the agent(s) or researcher responsible for completing, providing, or executing the documentation and/or agreements
- identify 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 and agreement,

- require the responsible agent(s) to track receipt of the executed written acknowledgements and agreements, and
- set out the procedure that must be followed and related documentation that must be maintained.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

13. Template Research Agreement

A **Research Agreement** must be executed with the researchers to whom PHI will be disclosed prior to the disclosure of the PHI for research purposes. At a minimum, the Research Agreement must address the matters set out below.

General Provisions

The **Research Agreement** must:

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

Purposes of Collection, Use and Disclosure

The **Research Agreement** must:

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

In identifying the purposes for which the PHI may be used, the Research Agreement must explicitly:

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

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

- the PHI that is being disclosed pursuant to the Research Agreement is necessary for the identified research purpose(s) and that other information, namely **de-identified and/or aggregate information**, will not serve the research purpose, and
- no more PHI 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 PHI. At a minimum, the Research Agreement must require the researcher to acknowledge and agree not to:

- disclose the PHI except as required by law and subject to the exceptions and additional requirements prescribed in PHIPA's regulations
- publish the PHI in a form that could reasonably enable a person to ascertain the identity of the individual, or
- make contact or attempt to make contact with the individual to whom the PHI relates, directly or indirectly, unless the consent of the individual to being contacted is first obtained in accordance with subsection 44(6) of PHIPA.

Compliance with the Statutory Requirements for the Disclosure for Research Purposes

The **Research Agreement** must require:

- the researcher and the PP or PE to acknowledge and agree that the researcher has submitted an application in writing, a written research plan, and a copy of the decision of the research ethics board approving the written **research plan**, that meets the requirements of PHIPA and its regulations, and
- the researcher to also acknowledge and agree that the researcher will comply with the:
    - Research Agreement
    - written research plan approved by the research ethics board, and

- conditions, if any, specified by the research ethics board in respect of the written research plan.

Secure Transfer of Records of Personal Health Information

The **Research Agreement** must:

- require the secure transfer of records of PHI that will be disclosed pursuant to the Research Agreement, and
- set out the secure manner in which records of PHI 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 PHI are transferred in a secure manner; in identifying the secure manner in which the records of PHI will be transferred, the Research Agreement must have regard to the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information*** implemented by the PP or PE.

Secure Retention of Records of Personal Health Information

The **Research Agreement** must:

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

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

Secure Return of Records of Personal Health Information

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

- timeframe following the retention period within which the records must be securely returned
- secure manner in which the records must be returned, and
- agent of the PP or PE to whom the records must be securely returned.

In identifying the secure manner in which the records of PHI will be returned, regard may be had to the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information*** implemented by the PP or PE.

Secure Disposal of Records of Personal Health Information

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

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

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

- **PHIPA** and its **regulations**
- orders and decisions issued by the IPC under PHIPA and its regulations, including **Order HO-001** and **Order HO-006**
- guidelines, fact sheets, and best practices issued by the IPC pursuant to PHIPA and its regulations, including **Fact Sheet 10: Secure Destruction of Personal Information**, and
- policies, procedures, and practices implemented by the PP or PE, such as the **Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information**.

Certificate of Destruction

The **Research Agreement** must identify the:

- agent of the PP or PE to whom the **certificate of destruction** must be provided
- timeframe following secure disposal within which the certificate of destruction must be provided, and
- required content of the certificate of destruction.

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

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

Where Records Are De-identified and Retained

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

- require the researcher to submit written confirmation that the records were de-identified
- stipulate the timeframe following the retention period set out in the Research Agreement within which the written confirmation must be provided, and
- specify the agent of the PP or PE to whom the written confirmation must be provided.

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

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

Breach Notification to PP or PE

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

- of a breach or suspected breach of the Research Agreement
- of a breach or suspected breach of subsection 44(6) of PHIPA; or
- that PHI subject to the Research Agreement is stolen, lost, or collected, used, or disclosed without authority or is believed to have been stolen, lost, or collected, used, or disclosed without authority.

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

Consequences of Breach and Monitoring Compliance

The **Research Agreement** must also:

- provide the PP or PE with the right to audit the researcher's compliance with the agreement
- set out the manner and circumstances in which compliance will be audited and the notice, if any, that will be provided to the researcher of the audit
- require the researcher to ensure that all persons who will have access to the PHI, 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 PHI
- 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; and
- outline the consequences of breach of the agreement.

14. Log of Research Agreements

A PP or PE must maintain a log of executed **Research Agreements**. At a minimum, the log must include:

- the name of the research study
- the name of the principal researcher to whom the PHI was disclosed pursuant to the Research Agreement
- the date(s) of receipt of the written application, the written **research plan**, and the written decision of the research ethics board approving the research plan
- the date that the approval to disclose the PHI for research purposes was granted by the PP or PE
- the date that the Research Agreement was executed
- the date that the PHI was disclosed
- the nature of the PHI disclosed
- the retention period for the records of PHI as set out in the Research Agreement
- whether the records of PHI 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 PHI were securely returned, a **certificate of destruction** was received or written confirmation of de-identification was received or the date by which they must be returned, disposed of, or de-identified.

Disclosure of Personal Health Information for Purposes Other Than Research

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

A policy, procedures, and practices must be developed and implemented to identify whether and in what circumstances, if any, PHI is permitted to be disclosed for purposes other than research. If the PP or PE does not permit PHI to be disclosed for purposes other than research, the policy, procedures, and practices must explicitly prohibit the disclosure of PHI for non-research purposes, except where required by law. If the PP or PE does *not* permit **de-identified and/or aggregate information** to be disclosed for purposes other than research, the policy, procedures, and practices must explicitly prohibit such disclosure as well.

Where the Disclosure of Personal Health Information is Permitted

Where the PP or PE permits PHI to be disclosed for purposes other than research, the policy, procedures, and practices must:

- articulate a commitment by the PP or PE not to disclose PHI if other information will serve the purpose and not to disclose more PHI than is reasonably necessary to meet the purpose
- set out the purposes other than research for which and the circumstances in which the disclosure of PHI is permitted, and
- require that all such disclosures comply with PHIPA and its regulations.

Review and Approval Process

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

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

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

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

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

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

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

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

Secure Return or Disposal of Records of Personal Health Information

The policy, procedures, and practices must:

- identify the agent(s) responsible for ensuring that records of PHI disclosed to a person or organization for purposes other than research are either securely returned or securely

disposed of, as the case may be, following the retention period in the **Data Sharing Agreement** or the date of termination of the Data Sharing Agreement

- address the process to be followed where records of PHI 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, and
- identify the agent(s) responsible for implementing this process and the stipulated timeframe following the retention period or the date of termination within which this process must be implemented.

Documentation Related to Approved Disclosures of Personal Health Information

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

Disclosure of De-identified and/or Aggregate Information

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

Review and Approval Process

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

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

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

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

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

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

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

Conditions or Restrictions on the Approval

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

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

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

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

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

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

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

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

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

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

collection of PHI for purposes other than research, the agent(s) responsible for ensuring that a Data Sharing Agreement is executed must be satisfied that the collection was approved in accordance with the ***Policy, Procedures, and Practices for the Collection of Personal Health Information***.

The policy, procedures, and practices must also:

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

17. Template Data Sharing Agreement

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

General Provisions

The **Data Sharing Agreement** must:

- describe the status of the PP or PE under PHIPA and the duties and responsibilities arising from this status
- provide a definition of PHI that is consistent with PHIPA and its regulations
- specify the precise nature of the PHI subject to the Data Sharing Agreement. Where it is not reasonably possible for a PP or PE to list or itemize every data element or variable, the PP or PE may identify categories of data elements or variables, and

- identify the person or organization that is collecting PHI or disclosing PHI pursuant to the Data Sharing Agreement.

Purposes of Collection, Use, and Disclosure

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

In identifying these purposes, the Data Sharing Agreement must explicitly state whether or not the PHI collected pursuant to the Data Sharing Agreement will be linked to other information. If the PHI will be linked to other information, the Data Sharing Agreement must identify and describe:

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

The Data Sharing Agreement must also:

- contain an acknowledgement that:
    - the PHI collected pursuant to the Data Sharing Agreement is necessary for the purpose for which it was collected
    - other information, namely **de-identified and/or aggregate information**, will not serve the purpose, and
    - no more PHI is being collected and will be used than is reasonably necessary to meet the purpose
- identify the purposes, if any, for which the PHI subject to the Data Sharing Agreement may be further disclosed and any limitations, conditions, or restrictions imposed thereon
- require the collection, use, and disclosure of PHI subject to the Data Sharing Agreement to comply with PHIPA and its regulations
- set out the specific statutory authority for each collection, use, and disclosure contemplated in the Data Sharing Agreement, and
- set out any restrictions with respect to small cell-sizes (e.g. less than five), having regard for the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation*** implemented by the PP or PE.

Secure Transfer of Records of Personal Health Information

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

- secure manner in which the records of PHI will be transferred, including under what conditions and to whom the records will be transferred, and

- 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 PHI will be transferred, regard should be had to the ***Policy, Procedures, and Practices for Secure Transfer of Records of PHI*** implemented by the PP or PE.

Secure Retention of Records of Personal Health Information

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

The Data Sharing Agreement must:

- require the records of PHI to be retained in a secure manner
- specify the manner in which the records of PHI 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 PHI will be retained, the Data Sharing Agreement should have regard for the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information*** implemented by the PP or PE
- require reasonable steps to be taken to ensure that the records of PHI subject to the Data Sharing Agreement are protected against:
    - theft, loss, and unauthorized collection, use, or disclosure, and
    - unauthorized copying, modification, or disposal, and
- detail the reasonable steps that are required to be taken.

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

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

Secure Return of Records of Personal Health Information

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

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

Secure Disposal of Records of Personal Health Information

If the records of PHI 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 PHIPA and its regulations
- specify the manner in which the records of PHI subject to the Data Sharing Agreement must be securely disposed of
- stipulate the timeframe following the retention period or following the date of termination of the Data Sharing Agreement within which the records of PHI must be securely disposed of, and
- specify the timeframe within which a **certificate of destruction** must be provided.

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

- **PHIPA** and its **regulations**
- orders and decisions issued by the IPC under PHIPA and its regulations, including **Order HO-001** and **Order HO-006**;
- guidelines, fact sheets, and best practices issued by the IPC pursuant to PHIPA and its regulations, including **Fact Sheet 10: Secure Destruction of Personal Information**, and
- The ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information*** implemented by the PP or PE.

Certificate of Destruction

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

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

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

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

Breach Notification to PP or PE

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

- the Data Sharing Agreement has been breached or is suspected to have been breached, or

- the PHI subject to the Data Sharing Agreement is stolen, lost, or collected, used, or disclosed without authority or is believed to have been stolen, lost, or collected, used, or disclosed without authority.

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

Consequences of Breach and Monitoring Compliance

The **Data Sharing Agreement** must:

- provide the PP or PE with the right to audit compliance with the agreement
- set out the manner and circumstances in which compliance will be audited and the notice, if any, that will be provided of the audit
- require that all persons who will have access to the PHI are aware of and agree to comply with the terms and conditions of the Data Sharing Agreement prior to being given access to the PHI
- set out the method by which this will be ensured; this may include requiring the persons who will have access to the PHI 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, and
- outline the consequences of breach of the agreement.

18. Log of Data Sharing Agreements

A PP or PE 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 PHI was collected or to whom the PHI was disclosed
- the date that the collection or disclosure of PHI was approved, as the case may be
- the date that the Data Sharing Agreement was executed
- the date the PHI was collected or disclosed, as the case may be
- the nature of the PHI subject to the Data Sharing Agreement
- the retention period for the records of PHI set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement
- whether the records of PHI 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 PHI were securely returned or a **certificate of destruction** was provided or the timeframes by which they must be returned or disposed of.

Third-Party Service Provider Agreements

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

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

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

Limitations on Access to and Use of PHI

The policy, procedures, and practices with respect to **TPSP Agreements** must require the PP or PE to:

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

Vulnerability Management Practices

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

Secure Transfer, Retention, Back-Up, and Disposal

The policy, procedures, and practices must also:

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

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

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

The policy, procedures, and practices must:

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

- the agent(s) responsible for ensuring that records of PHI provided to a TPSP are either securely returned to the PP or PE or are securely disposed of, as the case may be, following the termination of the agreement.

Where a TPSP is contracted to securely retain or securely dispose of records of PHI of the PP or PE, the policy, procedures, and practices must further:

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

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

Tracking Agreements

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

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices;

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

20. Template Agreement for Third-Party Service Providers

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

General Provisions

The **TPSP Agreement** must:

- describe the status of the PP or PE under PHIPA and the duties and responsibilities arising from this status, and
- state whether or not the TPSP is an agent of the PP or PE in providing services pursuant to the agreement.

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

If the TPSP is an agent of the PP or PE, the TPSP Agreement must require the TPSP to comply with the provisions of PHIPA and its regulations relating to PPs or PEs, as the case may be, and to comply with the privacy and information security policies, procedures, and practices implemented by the PP or PE in providing services pursuant to the agreement.

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

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

Obligations with Respect to Access and Use

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

In the case of a TPSP that is not an agent of the PP or PE, the TPSP Agreement must prohibit TPSPs from using PHI except:

- as permitted in the TPSP Agreement
- for the purposes for which the PP or PE is permitted to use PHI under PHIPA and its regulations, and
- as necessary in the course of providing services pursuant to the agreement or as required by law.

In the case of a TPSP that is also an agent of the PP or PE, the TPSP Agreement must further:

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

Obligations with Respect to Disclosure

The **TPSP Agreement** must identify the purposes, if any, for which the TPSP is permitted to disclose the PHI of the PP or PE and any limitations, conditions, or restrictions imposed thereon.

In identifying the limited and narrowly defined purposes for which the TPSP is permitted to disclose PHI, the PP or PE must ensure that each disclosure identified in the TPSP Agreement is consistent with, and reasonably necessary for, the disclosures of PHI permitted by PHIPA and its regulations and is not contrary to PHIPA, its regulations, or another law.

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

In the case of a TPSP that is also an agent of the PP or PE, the TPSP Agreement must further prohibit the TPSP from disclosing PHI:

- except as permitted in the TPSP Agreement
- except for the purposes for which the PP or PE is permitted to disclose PHI under PHIPA and its regulations
- if other information will serve the purposes identified in the TPSP Agreement, and
- if the disclosure includes more PHI than is reasonably necessary to meet the purposes identified in the agreement.

Secure Transfer

The **TPSP Agreement** must identify the purposes for which and the circumstances in which records of PHI of the PP or PE may be transferred to the TPSP and transferred from the TPSP back to the PP or PE, if any.

Where it is necessary to transfer records of PHI to or from the PP or PE, the TPSP Agreement must require the TPSP and the PP or PE to transfer the records of PHI in a secure manner and must set out the responsibilities of the TPSP and PP or PE in this regard.

In particular, the TPSP Agreement must specify:

- the secure manner in which the records will be transferred
- the conditions pursuant to which the records will be transferred
- to whom the records will be transferred, 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 records of PHI must be transferred, the TPSP Agreement must have regard to the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information*** implemented by the PP or PE.

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

Secure Retention and Back-Up

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

The TPSP Agreement must further outline the responsibilities of the TPSP in securely retaining the records of PHI having regard to the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information*** implemented by the PP or PE.

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

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

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

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

- a detailed inventory of the records of PHI or backed-up records of PHI being retained on behalf of the PP or PE, and
- a method to track the records being retained.

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

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

Secure Return or Disposal of records of Personal Health Information

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

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

- timeframe within which the records of PHI must be securely returned
- secure manner in which the records must be returned, and
- agent of the PP or PE to whom the records must be securely returned.

In identifying the secure manner in which the records of PHI will be returned, the TPSP Agreement must have regard to the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information*** implemented by the PP or PE.

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

- **PHIPA** and its **regulations**
- orders and decisions issued by the IPC under PHIPA and its regulations, including **Order HO-001** and **Order HO-006**
- guidelines, fact sheets, and best practices issued by the IPC pursuant to PHIPA and its regulations, including **Fact Sheet 10: Secure Destruction of Personal Information**, and
- the ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information*** implemented by the PP or PE.

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

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

Certificate of Destruction

The **TPSP Agreement** must identify the:

- agent of the PP or PE to whom the **certificate of destruction** must be provided
- timeframe following secure disposal within which the certificate of destruction must be provided, and
- required content of the certificate of destruction.

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

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

Implementation of Safeguards

The **TPSP Agreement** must require the TPSP to take steps that are reasonable in the circumstances to ensure that the records of PHI subject to the agreement are accessed and used in the course of providing services pursuant to the agreement are protected against

theft, loss, and unauthorized collection, use, or disclosure and protected against unauthorized copying, modification, or disposal.

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

Training of Agents of the Third-Party Service Provider

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

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

Subcontracting of the Services

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

- acknowledge and agree that it will provide the PP or PE with advance notice of its intention to do so
- enter into a written agreement with the subcontractor on terms consistent with its obligations to the PP or PE, and
- provide the PP or PE with a right to obtain a copy of the written subcontracting agreement, upon request.

Breach Notification to PP or PE

At a minimum, the **TPSP Agreement** must require the TPSP to notify the PP or PE at the first reasonable opportunity if:

- there has been a breach or suspected breach of the TPSP Agreement
- PHI handled by the TPSP on behalf of the PP or PE is stolen, lost, or collected, used, or disclosed without authority, or
- PHI handled by the TPSP on behalf of the PP or PE is believed to have been stolen, lost, or collected, used, or disclosed without authority.

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

Consequences of Breach and Monitoring Compliance

The **TPSP Agreement** must provide the PP or PE with the right to audit the TPSP's compliance with the agreement and must also set out the manner and circumstances in which compliance will be audited and the notice, if any, that will be provided to the TPSP of the audit. The TPSP Agreement should also allow the PP or PE to request and obtain a copy of any independent audit of the TPSP's privacy and information security policies, procedures, and practices.

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

21. Log of Agreements with Third-Party Service Providers

A PP or PE must maintain a log of executed agreements with TPSPs that are permitted to access and use PHI. At a minimum, the log must include:

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

Data Linkage, De-Identification and Aggregation

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

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

The policy, procedures, and practices must identify whether or not the PP or PE permits the linkage of records of PHI and, if it is not permitted, the policy, procedures, and practices must explicitly prohibit the linkage of records of PHI. If the linkage of records of PHI 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 PHI is permitted, regard must be had to the sources of the records of PHI that are requested to be linked and the identity of the person or organization that will ultimately make use of the linked records of PHI, including where the linkage of records of PHI is:

- solely in the custody of the PP or PE for the exclusive use by the PP or PE
- in the custody of the PP or PE with records of PHI to be collected from another person or organization for the exclusive use by the PP or PE
- solely in the custody of the PP or PE for purposes of disclosure of the linked records of PHI to another person or organization, and
- in the custody of the PP or PE with records of PHI to be collected from another person or organization for purposes of disclosure of the linked records of PHI to that other person or organization.

Reviewing and Approving Requests to Link Records of Personal Health Information

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

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

The policy, procedures, and practices must also address:

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

Conditions or Restrictions on the Approval

Where the linked records of PHI will be disclosed by the PP or PE to another person or organization, the policy, procedures, and practices must require that the disclosure be approved

pursuant to the ***Policy, Procedures, and Practices for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements*** or the ***Policy, Procedures, and Practices for Disclosure of Personal Health Information For Purposes Other Than Research***, as applicable.

Where the linked records of PHI will be used by the PP or PE, the policy, procedures, and practices must require that the:

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

Process for the Linkage of Records of Personal Health Information

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

Secure Retention

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

Secure Disposal

The policy, procedures, and practices must address the secure disposal of records of PHI linked by the PP or PE and, in particular, must require that the records of PHI be securely disposed of in compliance with the ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information***.

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

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

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

Tracking Approved Linkages of Records of Personal Health Information

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

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

23. Log of Approved Linkages of Records of Personal Health Information

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

- name of the agent, person, or organization who requested the linkage
- date that the linkage of records of PHI was approved, and
- nature of the records of PHI linked.

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

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

- requires that PHI not be used or disclosed if other information, namely de-identified and/or aggregate information, will serve the identified purpose
- provides a definition of de-identified information and aggregate information which must have regard to small cell-sizes (e.g. less than five), and be consistent with the meaning of "**identifying information**" in subsection 4(2) of PHIPA and the meaning of "**de-identify**" in section 2 of PHIPA

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

Different Release Models

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

Small Cell Sizes

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

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

Re-Identification

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

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

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

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

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

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

The policy, procedures, and practices must also identify the mechanisms implemented to ensure that the persons or organizations to whom de-identified and/or aggregate information is disclosed will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual, unless such re-identification is permitted by PHIPA or another law.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

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

Privacy Impact Assessments

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

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

Circumstances in which Privacy Impact Assessments are Required to be Conducted

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

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

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

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

Circumstances in which Privacy Impact Assessments are Not Required

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

- require documentation of the rationale for why a privacy impact assessment is not required
- set out the documentation that must be completed, provided, and/or executed
- identify the agent(s) responsible for completing, providing, and/or executing the documentation

- identify the agent(s) to whom this documentation must be provided, and
- set out the required content of the documentation, including the criteria that must be used in making the determination that a privacy impact assessment is not to be conducted.

Timing of Conducting and Reviewing Privacy Impact Assessments

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

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

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

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

Required Content of Privacy Impact Assessments

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

- the data holding, information system, technology, or program at issue
- the nature and type of PHI collected, used, or disclosed or that is proposed to be collected, used, or disclosed
- the sources of the PHI
- the purposes for which the PHI is collected, used, or disclosed or is proposed to be collected, used, or disclosed
- the reason that the PHI is required for the purposes identified

- the flows of the PHI
- the statutory authority for each collection, use, and disclosure of PHI identified
- the limitations imposed on the collection, use, and disclosure of the PHI
- whether or not the PHI is or will be linked to other information
- whether or not the PHI will be **de-identified and/or aggregated** and the specific purposes for which, and circumstances in which, the de-identified and/or aggregate information will be re-identified, if any, and the conditions or restrictions imposed
- the retention period for the records of PHI
- the secure manner in which the records of PHI are or will be retained, transferred, and disposed of
- the functionality for logging access, use, modification, and disclosure of the PHI and the functionality to audit logs for unauthorized use or disclosure
- the risks to the privacy of individuals whose PHI 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 PHI.

Privacy Impact Assessment Findings and Recommendations

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

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

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

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

Relationship to the Privacy Impact Assessment Guidelines for the Ontario *Personal Health Information Protection Act*

In developing the policy, procedures, and practices, regard should be given to the **Privacy Impact Assessment Guidelines for the Ontario *Personal Health Information Protection Act***, published by the IPC.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

26. Log of Privacy Impact Assessments

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

- data holding, information system, technology, or program involving PHI that is at issue
- date that the privacy impact assessment was completed or is expected to be completed
- agent(s) responsible for completing or ensuring the completion of the privacy impact assessment
- findings, mitigations, and any other recommendations arising from the privacy impact assessment
- agent(s) responsible for addressing each mitigation and any other recommendation, the date that each mitigation or recommendation was or is expected to be addressed, and
- manner in which each recommendation was or is expected to be addressed.

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

- reasons that a privacy impact assessment will not be undertaken

- agent(s) responsible for making this determination, and
- date the determination was made.

Privacy Audit Program

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

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

- audits to assess compliance with the privacy policies, procedures, and practices implemented by the PP or PE, and
- audits of the agent(s) permitted to access and use PHI pursuant to the ***Policy, Procedures, and Practices for Limiting Agent Access to and Use of Personal Health Information***.

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

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

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

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

- criteria that must be considered in selecting the subject matter of the audit, 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, procedures, and practices must also set out the process that must be followed in reviewing and addressing the mitigations and any other recommendations resulting from privacy audits, including the agent(s) responsible for:

- assigning other agent(s) to address the mitigations and any other recommendations as required

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

Required Documentation

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

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

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

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

Privacy Audit Findings

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

- identifying the agent(s) responsible for communicating the findings of the privacy audit
- the mechanism and format for communicating the findings of the privacy audit, including the level of detail for communicating the findings
- the timeframe within which the findings of the privacy audit must be communicated, and
- to whom the findings of the privacy audit will be communicated, including whether the findings must be communicated to the chief executive officer or the executive director (or equivalent position).

The policy, procedures, and practices must:

- require that a log be maintained of privacy audits
- identify the agent(s) responsible for maintaining the log of findings, mitigations, and other recommendations and for tracking that the mitigations/recommendations arising from the privacy audits are addressed within the identified timeframe

- address where documentation related to privacy audits will be retained, and
- identify the agent(s) responsible for retaining this documentation.

Compliance, Audit, and Enforcement

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

28. Log of Privacy Audits

A PP or PE must maintain a log of privacy audits that have been completed. The log must set out the:

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

Privacy Breaches

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

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

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

- the collection, use, and disclosure of PHI that is not in compliance with PHIPA or its regulations
- a contravention of the privacy policies, procedures, or practices implemented by the PP or PE, related to the requirements of the Manual
- a contravention of written acknowledgments, **Data Sharing Agreements, Research Agreements, Confidentiality Agreements**, and **TPSP Agreements**, related to the requirements of the Manual, and

- circumstances where PHI is stolen, lost, or collected, used, or disclosed without authority or where records of PHI are subject to unauthorized copying, modification, or disposal.

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

In developing the policy, procedures, and practices, the PP or PE must have regard to the IPC's **Responding to a Health Privacy Breach: Guidelines for the Health Sector**.

Identification of Privacy Breaches

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

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

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

Determination of Whether a Privacy Breach Occurred

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

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

Prioritization Framework

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

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

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

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

Breach Notification to Senior Management

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

- identifying the agent(s) responsible for notifying senior management
- the timeframe within which notification must be provided
- the manner in which this notification must be provided, and
- the nature of the information that must be provided to senior management upon notification, including the level of detail that must be provided.

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

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

Containment

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

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

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

- no copies of the records of PHI have been made, and
- the records of PHI are either retrieved or disposed of in a secure manner.

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

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

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

- process to be followed in reviewing the containment measures implemented and determining whether the privacy breach has been effectively contained or whether further containment measures are necessary
- agent(s) responsible for reviewing the containment measures
- documentation that must be completed, provided, and/or executed in reviewing the containment measures
- agent(s) responsible for completing, providing, and/executing the documentation
- agent(s) to whom this documentation must be provided, and
- required content of the documentation.

Breach Notification to Custodians or Other Organizations

The policy, procedures, and practices must require the PP or PE to notify, at the first reasonable opportunity, the custodian or other organization that disclosed the PHI to the PP or PE whenever PHI has been or is believed to be stolen, lost or collected, used or disclosed without authority and whenever required pursuant to the agreement with the custodian or other organization.

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

- agent(s) responsible for notifying the custodian or other organization
- format of the notification, and
- nature of the information that must be provided upon notification.

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

- the extent of the privacy breach
- the nature of the PHI 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.

Breach Notification to the IPC

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

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

The PP or PE must notify the IPC, at the first reasonable opportunity, of privacy breaches in the circumstances set out in subsections 6.3(1) and 18.3(1) of PHIPA's regulations, as if the PP or PE were a custodian.

Breach Notification to Affected Individuals

However, as a secondary collector of PHI, a PP or PE should not directly notify the individual to whom the PHI relates of a **privacy breach**. Where applicable, the required notification to individuals must be provided by the relevant custodian(s), unless an alternative decision regarding breach notification to affected individuals is approved by the IPC.

Investigation of Breach

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

- agent(s) responsible for investigating the **privacy breach**
- nature and scope of the investigation (i.e., document reviews, interviews, site visits, inspections)

- process that must be followed in investigating the privacy breach. This process must set out the:
    - documentation that must be completed, provided, and/or executed in undertaking the investigation
    - agent(s) responsible for completing, providing, and/or executing the documentation
    - agent(s) to whom this documentation must be provided, and
    - required content of the documentation.

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

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

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

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

Communication of Findings of Investigation and Recommendations

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

- the agent(s) responsible for communicating the findings of the investigation
- the mechanism and format for communicating the findings of the investigation, including the level of detail for communicating the findings
- the timeframe within which the findings of the investigation must be communicated, and
- to whom the findings of the investigation must be communicated, including whether the findings must be communicated to the chief executive officer or the executive director (or equivalent position).

Tracking Privacy Breaches

The policy, procedures, and practices must:

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

30. Log of Privacy Breaches

A PP or PE must maintain a log of **privacy breaches** and suspected privacy breaches. At a minimum, the log must set out:

- the date of the privacy breach or suspected privacy breach
- the date that the privacy breach was identified or suspected
- the nature of the PHI, if any, that was the subject matter of the privacy breach and the nature and extent of the privacy breach or suspected privacy breach
- a description of the privacy breach or suspected privacy breach and who identified the privacy breach or suspected privacy breach
- the cause of the privacy breach or suspected privacy breach
- whether an unauthorized person who is not an agent or **electronic service provider** caused the privacy breach or suspected privacy breach and the name or a description of the unauthorized person, if applicable

- the date that the chief executive officer or executive director (or equivalent position) and senior management were notified of the privacy breach or suspected privacy breach, if applicable
- the date that the privacy breach or suspected privacy breach was contained and the nature of the containment measures
- the name of the agent(s) responsible for containing the privacy breach or suspected privacy breach
- the date that the investigation was commenced
- the date that the investigation was completed
- the agent(s) responsible for conducting the investigation
- the findings, mitigations, and other relevant recommendations arising from the investigation
- the agent(s) responsible for addressing each recommendation
- the manner in which each recommendation was or is expected to be addressed
- the date by which each recommendation was or is expected to be addressed
- the date that the chief executive officer or executive director (or equivalent position) and senior management were notified of the findings, mitigations, and other relevant recommendations arising from the investigation, if applicable
- the date that the custodian or other organization that disclosed the PHI to the PP or PE was notified, if applicable
- the date that notification was provided to the IPC, if applicable, and
- the date that notification was provided to individuals, if applicable.

Privacy Complaints and Inquiries

31. Policy, Procedures, and Practices for Privacy Complaints

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

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

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

- the name and/or title, mailing address, and contact information of the agent(s) to whom concerns or complaints may be directed

- information related to the manner in which and format in which privacy concerns or complaints may be directed to the PP or PE
- information advising individuals that they may make a complaint to the IPC regarding the PP's or PE's compliance with PHIPA and its regulations, and
- the mailing address and contact information for the IPC.

Process for Receiving Complaints

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

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

Determination of Whether to Investigate a Complaint

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

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

Where Complaint Will Not Be Investigated

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

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

Where Complaint Will Be Investigated

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

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

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

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

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

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

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

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

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

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

- identifying the agent(s) responsible for communicating the findings of the investigation
- the mechanism and format for communicating the findings of the investigation, including the level of detail for communicating the findings
- the timeframe within which the findings of the investigation must be communicated, and
- to whom the findings must be communicated, including whether the findings must be communicated to the chief executive officer or the executive director (or equivalent position).

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

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

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

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

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

Tracking Privacy Complaints

The policy, procedures, and practices must:

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

Relationship to Other Policies, Procedures, and Practices

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

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

32. Log of Privacy Complaints

A PP or PE must maintain a log of **privacy complaints** received that, at a minimum, sets out:

- the date that the privacy complaint was received and the nature of the privacy complaint
- the determination as to whether the privacy complaint will be investigated and the date that the determination was made
- the agent(s) who made the determination as to whether the privacy complaint would be investigated

- where the determination was made that the privacy complaint will not be investigated, the date that the complainant was advised that the complaint will not be investigated and informed of their right to file their complaint with the IPC, and
- where the determination is made that the privacy complaint will be investigated:
    - the date that the complainant was advised that the complaint will be investigated
    - the agent(s) responsible for conducting the investigation
    - the dates that the investigation was commenced and completed
    - the findings and other relevant recommendations arising from the investigation
    - the date that the chief executive officer or executive director (or equivalent position) and senior management were notified of the findings and other relevant recommendations arising from the investigation, if applicable
    - the agent(s) responsible for addressing each recommendation
    - the date that each recommendation was or is expected to be addressed
    - the manner in which each recommendation was or is expected to be addressed, and
    - the date that the complainant was advised of the findings of the investigation, of the measures taken, if any, in response to the privacy complaint and of their right to file their complaint with the IPC.

33. Policy, Procedures, and Practices for Privacy Inquiries

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

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

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

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

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

Relationship to Policy, Procedures, and Practices for Privacy Complaints

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

Part 2 - Information Security Policies, Procedures, and Practices

PPs and PEs must take steps that are reasonable in the circumstances to ensure that PHI is protected against theft, loss, and unauthorized collection, use, or disclosure and that the records of PHI are protected against unauthorized copying, modification, or disposal. The policies, procedures, and practices required throughout this Part, related to PHI, must be read as including policies, procedures, and practices that are reasonable in the circumstances to protect **de-identified** and/or aggregate information from unauthorized re-identification (i.e., re-identification that is contrary to the **Policy, Procedures, and Practices with Respect to De-Identification and Aggregation** or is not permitted by PHIPA or another law).

General Information Security Policies, Procedures, and Practices

1. Information Security Policy

An overarching information security policy, or equivalent, must be developed and implemented in relation to PHI received by the PP or PE under PHIPA. The information security policy must require that steps be taken that are reasonable in the circumstances to ensure that the PHI is protected against theft, loss, and unauthorized collection, use, or disclosure and to ensure that the records of PHI are protected against unauthorized copying, modification, or disposal.

Threat and Risk Assessment

The information security policy must also:

- require the PP or PE to undertake comprehensive and organization-wide threat and risk assessments of all **information security components** relating to PHI, as well as appropriate project specific threat and risk assessments, and
- establish and document a methodology for identifying, assessing, and remediating threats and risks and for prioritizing all threats and risks identified for remedial action.

Information Security Program

The information security policy must further require a comprehensive information security program to be developed and implemented consisting of administrative, technical, and physical safeguards that are consistent with evolving industry information security standards and best practices. The information security program must:

- be required to effectively address the threats and risks identified
- be amenable to independent verification
- be consistent with established information security frameworks and control objectives, and
- address the duties and responsibilities of agents in respect of the information security program and of the administrative, technical, and physical safeguards.

The information security policy must also require the information security program to consist of the following control objectives and information security policies, procedures, and practices:

- an ***Information Security Governance and Accountability Framework*** for the implementation of the information security program, including information security training and awareness
- ***Policy, Procedures, and Practices for the Ongoing Review of the Information Security Policies, Procedures, and Practices*** implemented
- ***Policies, Procedures, and Practices for Ensuring the Physical Security of Personal Health Information*** and ensuring the premises and locations within the premises where records of PHI are retained
- policies, procedures, and practices for the secure retention, transfer, and disposal of records of PHI, including policies, procedures, and practices related to mobile devices remotely accessing PHI, and secure transfer and retention of records of PHI
- policies, procedures, and practices to establish access control and authorization (e.g., identity, access, and privileged account management) including business requirements, user access management, user responsibilities, network access control, operating system access control, and application and information access control
- policies, procedures, and practices for information systems acquisition, development, and maintenance including the security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development, and support procedures
- policies, procedures, and practices for logging, monitoring, and auditing privacy and information security events as well as other types of information security audits
- policies, procedures, and practices for infrastructure security management, including system hardening, network segregation and segmentation, vulnerability and patch management and change management
- policies, procedures, and practices related to the acceptable use of information technology
- policies, procedures, and practices for back-up and recovery
- policies, procedures, and practices for **information security breach** management
- policies, procedures, and practices to establish protection against network intrusions, phishing attacks, and malicious code, and
- policies, procedures, and practices governing third-party or supply chain risk management.

The information security policy should also refer to more detailed policies, procedures, and practices developed and implemented to address the above-noted matters. The required content of some of these more detailed policies, procedures, and practices are set out in this Manual.

Information Security Infrastructure

The information security infrastructure implemented by the PP or PE, including networks, servers, components, technologies, applications, software, and configurations applied to protect and keep PHI secure, must:

- be documented within the information security policy
- be in accordance with evolving industry information security standards and best practices, and
- ensure requirements under this Part are addressed.

Regular Assessment and Verification of the Information Security Program

In addition, the information security policy must require a robust program to be implemented for regular assessment and verification of the effectiveness of the information security program in order to deal with threats and risks to data holdings containing PHI. Specifically, the policy, procedures, and practices must identify the frequency with which and the circumstances in which the information security program is required to be assessed.

Compliance, Audit and Enforcement

The policy, procedures, and practices must:

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

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

A policy, procedures, and practices must be developed and implemented for the ongoing review of the information security policies, procedures, and practices put in place by the PP or PE. The purpose of the review is to determine whether amendments are needed or whether new information security policies, procedures, and practices are required.

The policy, procedures, and practices must identify the:

- frequency of the review of information security policies, procedures, and practices, which at minimum must be reviewed at least once prior to each three-year review by the IPC
- agent(s) responsible, and the procedure, for undertaking the review

- timeframe in which the review will be undertaken
- agent(s) responsible and the procedure for amending and/or drafting new information security policies, procedures, and practices, if deemed necessary as a result of the review
- agent(s) responsible and the procedure for seeking and obtaining approval of any amendments or newly developed information security policies, procedures, and practices, if deemed necessary as a result of the review
- agent(s) responsible and the procedure for communicating the amended or newly developed information security policies, procedures, and practices, and
- method and nature of the communication to agents, the public, and other stakeholders, as may be relevant, depending on the nature of the subject matter.

In undertaking the review and determining whether amendments and/or new information security policies, procedures, and practices are necessary, the PP or PE must have regard to:

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the PP or PE at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if an agent breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices

- address how and by whom compliance will be enforced and the consequences of breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***, and
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Information Security Audits***.

Physical Security

3. Policy, Procedures, and Practices for Ensuring Physical Security of Personal Health Information

A policy, procedures, and practices must be developed and implemented to address the physical safeguards implemented by the PP or PE to protect PHI against theft, loss, and unauthorized collection, use, or disclosure and to protect records of PHI against unauthorized copying, modification, or disposal.

At a minimum, the physical safeguards implemented must include controlled access to the premises and to locations within the premises where records of PHI are retained such as locked, alarmed, restricted, and/or monitored access.

Not all parts of the premises of a PP or PE are required to adhere to the same physical safeguards. The policy, procedures, and practices should ensure that the premises of the PP or PE are divided into varying levels of physical security with each successive level being more secure and restricted to fewer individuals. The levels of physical security should be determined in accordance with risk analyses, such as privacy impact assessments and threat and risk assessments.

4. Policy, Procedures, and Practices with Respect to Access by Agents

The policy, procedures, and practices must:

- set out the various levels of access that may be granted to the premises and to locations within the premises where records of PHI are retained
- require individuals to pass through multiple levels of physical security before they can access locations within the premises where records of PHI are retained
- identify the agent(s) responsible and procedure for receiving, reviewing, and granting initial requests for access to locations within the premises where records of PHI are retained, including the levels of access that may be granted
- set out the process to be followed and the requirements that must be satisfied to grant access
- specify any documentation that must be completed, provided, and/or executed, including the manner in which the determination relating to access and the level of access is documented
- identify the agent(s) responsible and procedure for the ongoing review of agents granted access to locations within the premises where records of PHI are retained

- identify the agent(s) responsible and procedure for terminating access, including a review of whether access to locations within the premises where records of PHI are retained continues to be needed, and
- set out the process and content of any documentation that must be completed, provided, and/or executed related to reviewing, granting, changing, or terminating access to locations within the premises where records of PHI are retained, including the agent(s) to whom the documentation must be provided.

The policy, procedures, and practices must address the criteria that must be considered by the agent(s) responsible for approving and determining the appropriate level of access. The criteria must be based on the "need to know" principle and must ensure that access is only provided to agents who routinely require such access for their employment, contractual, or other responsibilities.

At a minimum, the criteria considered by the agent(s) must ensure that access is only provided to agents acting on behalf of the PP or PE:

- who are employed, contracted, or otherwise engaged to provide services to the PP or PE
- who are required to use PHI retained on the premises of the PP or PE for the purpose of performing their duties as agents of the PP or PE, and
- whose use of is permitted by PHIPA and its regulations and by the ***Policy, Procedures, and Practices for Limiting Agent Access to and Use of PHI***.

In the event that an agent only requires such access for a specified period, the policy, procedures, and practices must establish a process for ensuring that access is permitted only for that specified period.

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

- agent(s) responsible and the process to be followed in providing identification cards, access cards, and/or keys to the premises and to locations within the premises, and
- documentation that must be completed, provided, and/or executed, including the:
    - agent(s) responsible for completing, providing, and/or executing the documentation, and
    - required content of the documentation.

Theft, Loss, and Misplacement of Identification Cards, Access Cards, and Keys

The policy, procedures, and practices must require agents to notify the PP or PE at the first reasonable opportunity of the theft, loss, or misplacement of identification cards, access cards, and/or keys and must set out the process that must be followed in such cases. The process must specify the:

- agent(s) to whom the notification must be provided
- nature and format of the notification

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

With regard to the theft, loss, or misplacement of identification cards, access cards, and/or keys, the policy, procedures, and practices must also:

- outline the safeguards that are required to be implemented as a result of the theft, loss, or misplacement of identification cards, access cards, and/or keys
- identify the agent(s) responsible for implementing these safeguards
- address the circumstances that warrant issuing temporary or replacement identification cards, access cards, and/or keys
- detail the process that must be followed and the agent(s) responsible for their issuance
- set out any documentation that must be completed, provided, and/or executed
- identify the agent(s) responsible for completing, providing, and/or executing the documentation
- identify the agent to whom the documentation must be provided
- set out the required content of the documentation
- identify the agent(s) to whom temporary identification cards, access cards, and/or keys must be returned
- specify the timeframe for return
- set out the process to be followed in the event that temporary identification cards, access cards, and/or keys are not returned
- identify the agent(s) responsible for implementing the process to be followed in the event of non-return, and
- the timeframe within which this process must be implemented.

Termination of the Employment, Contractual, or Other Relationship

The policy, procedures, and practices must require agents, as well as their supervisors, to:

- notify the PP or PE of the termination of their employment, contractual, or other relationship with the PP or PE
- return their identification cards, access cards, and/or keys to the PP or PE on or before the date of termination of their employment, contractual, or other relationship in accordance with the ***Policy, Procedures, and Practices upon Termination or Cessation of the Employment or Contractual Relationship***, and

- ensure access to the premises is terminated upon the cessation of the employment, contractual or other relationship in accordance with the ***Policy, Procedures, and Practices upon Termination or Cessation of the Employment or Contractual Relationship***.

Notification When Access is No Longer Required

The policy, procedures, and practices must require the agent granted approval to access location(s) where records of PHI are retained, or his or her supervisor, to notify the PP or PE when the agent no longer requires such access. In this regard, the policy, procedures, and practices must:

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

Audits of Agents with Access to the Premises

Audits must be conducted of agents with access to the premises of the PP or PE and to locations within the premises where records of PHI are retained in accordance with the ***Policy, Procedures, and Practices in Respect of Information Security Audits***. The purpose of the audit is to ensure that agents granted access to the premises and to locations within the premises where records of PHI are retained continue to:

- be employed, contracted, or otherwise engaged to provide services to the PP or PE
- be routinely required to use PHI received by the PP or PE for the purpose of performing their duties as agents of the PP or PE, and
- require the same level of access to the PHI.

In this regard, the policy, procedures, and practices must identify the agent(s) responsible for conducting the audits and for ensuring compliance with the policy, procedures, and practices and the frequency with which the audits must be conducted.

Tracking and Retention of Documentation Related to Access to the Premises

The policy, procedures, and practices must:

- require that a log be maintained of agents granted approval to access the premises of the PP or PE and to locations within the premises where records of PHI are retained, and identify the agent(s) responsible for maintaining such a log, and
- address where documentation related to the receipt, review, approval, and termination of access to the premises and to locations within the premises where PHI is retained will be maintained, and identify the agent(s) responsible for maintaining this documentation.

5. Policy, Procedures, and Practices with Respect to Access by Visitors

The policy, procedures, and practices must address the agent(s) responsible and the process to be followed in identifying, screening, and supervising visitors to the premises of the PP or PE. At a minimum, the policy, procedures, and practices must set out:

- the identification that is required to be worn by visitors
- the documentation that must be completed, provided, and/or executed by agent(s) responsible for identifying, screening, and supervising visitors, and
- the documentation that must be completed, provided, and/or executed by visitors.

At a minimum, visitors must also be required to record:

- their name, date and time of arrival, time of departure, and
- the name of the agent(s) with whom the visitors are meeting.

The duties of agent(s) responsible for identifying, screening, and supervising visitors must also be addressed to ensure that:

- visitors are accompanied at all times
- visitors are wearing the identification issued by the PP or PE
- the identification is returned prior to departure, and
- visitors complete the appropriate documentation upon arrival and departure.

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

- process to be followed when the visitor does not return the identification provided
- process to be followed when the visitor does not document his or her date and time of departure
- agent(s) responsible for implementing and maintaining the identified process
- location where documentation related to the identification, screening, and supervision of visitors will be retained, and
- agent(s) responsible for retaining this documentation.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

6. Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity

A log must be maintained of agents granted approval to access the premises of the PP or PE and the level of access granted. At a minimum, the log must include the name of the agent granted approval to access the premises, and for each agent the:

- level and nature of the access granted
- locations within the premises to which access is granted
- date that the access was granted
- date(s) that identification cards, access cards, and/or keys were provided to the agent
- identification numbers on the identification cards, access cards, and/or keys, if any
- date of the next audit of access, and
- date that the identification cards, access cards, and/or keys were returned to the PP or PE, if applicable.

Secure Retention, Transfer, and Disposal

7. Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information

A policy, procedures, and practices must be developed and implemented with respect to the secure retention of records of PHI in paper and electronic format.

Retention Period

The policy, procedures, and practices must identify the retention period for records of PHI in both paper and electronic format, including the various categories of each, if applicable. The policy, procedures, and practices must require that records used for research purposes are not retained for a period longer than that set out in the written **research plan** approved by a research ethics board and that records collected pursuant to a **Data Sharing Agreement** not be retained for a period longer than that set out in the Data Sharing Agreement.

In any event, the policy, procedures, and practices must mandate that records of PHI be retained for only as long as necessary to fulfill the purposes for which the PHI was collected.

Secure Retention

The policy, procedures, and practices must also:

- require the records of PHI to be retained in a secure manner consistent with evolving industry information security standards and best practices
- identify the agent(s) responsible for ensuring the secure retention of these records
- set out the precise methods by which records of PHI in paper and electronic format are to be securely retained, including records retained on various media
- require agents of the PP or PE to take steps that are reasonable in the circumstances to ensure that records of PHI are protected against theft, loss, and unauthorized collection, use, or disclosure and against unauthorized copying, modification, or disposal, and
- outline the reasonable steps that must be taken by the agents of the PP or PE.

Third-Party Service Providers

If a TPSP is contracted to retain records of PHI on behalf of the PP or PE, the policy, procedures, and practices must incorporate those additional requirements set out in the ***Policy, Procedures, and Practices for Executing Agreements with Third-Party Service Providers***, including the ***Template Agreement for Third-Party Service Providers***.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

8. Policy, Procedures, and Practices for Securing Records of Personal Health Information on Mobile Devices and Remotely Accessing Personal Health Information

A policy, procedures, and practices must be developed and implemented to identify whether and in what circumstances, if any, the PP or PE permits PHI to be collected, used, disclosed,

retained, transferred, and/or disposed of on a mobile device. The policy, procedures, and practices must, at minimum, define the term mobile device to include mobile computing devices and portable storage devices.

If the PP or PE does not permit PHI to be collected, used, disclosed, retained, transferred, and/or disposed of on a mobile device, the policy and procedures must:

- explicitly prohibit such collection, use, disclosure, retention, transfer, and/or disposal
- indicate whether or not PHI may be accessed remotely through a secure connection or virtual private network, and
- explicitly prohibit such remote access if the PP or PE does not permit PHI to be accessed remotely through a secure connection or virtual private network.

At a minimum, this policy, procedures, and practices must be consistent with:

- **PHIPA** and its **regulations**
- orders and decisions issued by the IPC under PHIPA and its regulations, including but not limited to **Order HO-004**, **Order HO-007** and **Order HO-008**
- guidelines, fact sheets, and best practices issued by the IPC pursuant to PHIPA and its regulations, including ***Safeguarding Privacy on Mobile Devices*** and ***Working from Home During the COVID-19 Pandemic***, and
- evolving privacy and information security standards and best practices.

Where PHI is Permitted to be Collected, Used, Disclosed, Retained, Transferred, and/or Disposed of on a Mobile Device

If the PP or PE permits PHI to be collected, used, disclosed, retained, transferred, and/or disposed of on a mobile device, the policy, procedures, and practices must set out the purposes for which and the circumstances in which this is permitted, including where a mobile device is not under the administrative control of the PP or PE.

Approval Process

The policy, procedures, and practices must state whether approval is required prior to collecting, using, disclosing, retaining, transferring, and/or disposing of PHI on a mobile device. If prior approval is required, the policy, procedures, and practices must:

- identify the process that must be followed
- identify the agent(s) responsible for receiving, reviewing, and determining whether to approve or deny a request for the collection, use, disclosure, retention, transfer, and/or disposal of PHI on a mobile device
- set out the documentation that must be completed, provided, and/or executed
- set out the required content of the documentation

- identify the agent(s) responsible for completing, providing, and/or executing the documentation
- set out the manner of documenting decisions approving or denying the requests, and
- specify the method and format in which the decision will be communicated, and to whom.

The policy, procedures, and practices must further 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 a request for the collection, use, disclosure, retention, transfer and/or disposal of PHI on a mobile device.

At a minimum, prior to any approval of a request to collect, use, disclose, retain, transfer, and/or dispose of PHI on a mobile device, the policy, procedures, and practices must 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
- no more PHI will be collected, used, disclosed, retained, transferred, and/or disposed of on the mobile device than is reasonably necessary to meet the identified purpose, and
- the use of the PHI has been approved pursuant to the ***Policy, Procedures, and Practices for Limiting Agent Access to and Use of Personal Health Information***.

Conditions or Restrictions on the Collection, Use, Disclosure, Retention, Transfer, and/or Disposal of PHI on a Mobile Device

The policy, procedures, and practices must:

- require the PHI to be encrypted during transmission and when retained on mobile devices
- require access to the mobile device and to PHI retained on a mobile device to be protected by strong access controls that are in compliance with the ***Policy, Procedures, and Practices Relating to Authentication and Passwords***
- require a mandatory standardized password-protected device lock-out be enabled after a defined period of inactivity
- identify the agent(s) responsible for encrypting mobile devices and for ensuring that the mandatory standardized password-protected device lock-out is enabled, and
- describe the technical administration of mobile devices that collect, use, disclose, retain, transfer, and/or dispose of PHI (e.g., configuration of password policies, remote wipe capabilities, and virtual private network settings), including where such devices are not under the administrative control of the PP/PE.

Where a mobile device is not under the PP or PE's administrative control, PPs and PEs must, through contractual or licensing or other user requirements or mechanisms, ensure that these technical administration specifications are set out as necessary pre-conditions for others to collect, use, disclose, retain, transfer, or dispose of PHI.

The policy, procedures, and practices must further identify the conditions or restrictions with which agents granted approval to collect, use, disclose, retain, transfer, and/or dispose of PHI on a mobile device must comply. At a minimum, the agents must:

- be prohibited from collecting, using, disclosing, retaining, transferring, and/or disposing of PHI on a mobile device if other information, such as de-identified and/or aggregate information, will serve the purpose
- de-identify the PHI to the fullest extent possible
- be prohibited from collecting, using, disclosing, retaining, transferring, and/or disposing of more PHI on a mobile device than is reasonably necessary for the identified purpose
- be prohibited from retaining PHI on a mobile device for longer than necessary to meet the identified purpose; and
- ensure that device-level encryption and file-level encryption use different, strong passwords and are supported by "defence in depth" security measures.

The policy, procedures, and practices must also detail the steps that must be taken by agents to protect the PHI collected, used, disclosed, retained, transferred, and/or disposed of on a mobile device against theft, loss, and unauthorized collection, use, or disclosure and to protect the records of PHI retained on a mobile device against unauthorized copying, modification, or disposal.

The policy, procedures, and practices must also require agents to:

- retain the PHI on a mobile device in compliance with the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information***
- securely dispose of PHI retained on a mobile device in accordance with the process and in compliance with the timeframe outlined in the policy, procedures, and practices and the ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information***, and
- where records of PHI are to be transferred using a mobile device, transfer them in a secure manner, and in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information***.

Accessing PHI Through a Secure Connection or Virtual Private Network

If the PP or PE permits PHI to be accessed remotely, the policy, procedures, and practices must set out the purposes for which and the circumstances in which this is permitted.

Approval Process

The policy, procedures, and practices must identify whether approval is required prior to accessing PHI remotely through a secure connection or virtual private network.

If prior approval is required, the policy, procedures, and practices must:

- identify the process that must be followed

- identify the agent(s) responsible for receiving, reviewing, and determining whether to approve or deny a request for remote access to PHI
- 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 remote access
- set out the documentation that must be completed, provided, and/or executed
- set out the required content of the documentation
- identify the agent(s) responsible for completing, providing, and/or executing the documentation
- set out the manner of documenting the decision approving or denying the request, and
- specify the method and format in which the decision will be communicated, and to whom.

At a minimum, prior to any approval of a request to remotely access PHI, the policy, procedures, and practices must 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
- no more PHI will be accessed than is reasonably necessary to meet the identified purpose, and
- the use of the PHI has been approved pursuant to the ***Policy, Procedures, and Practices for Limiting Agent Access to and Use of Personal Health Information***.

Conditions or Restrictions on the Remote Access to Personal Health Information

The policy, procedures, and practices must identify the conditions or restrictions with which agents granted approval to access PHI remotely must comply, including in mobile and remote environments. At a minimum, the policy, procedures, and practices must:

- prohibit agents from remotely accessing PHI if other information, such as de-identified and/or aggregate information, will serve the purpose
- prohibit agents from remotely accessing more PHI than is reasonably necessary for the identified purpose, and
- set out the administrative, technical, and physical safeguards a PP or PE must implement to reduce risks to a level consistent with the risks associated with non-remote access before its agents are permitted to access PHI remotely.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices

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

9. Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information

A policy, procedures, and practices must be developed and implemented with respect to the secure transfer of records of PHI in paper and electronic format.

Approved Method(s) of Secure Transfer

The policy, procedures, and practices must:

- require records of PHI to be transferred in a secure manner
- set out the secure methods of transferring records of PHI in paper and electronic format that have been approved by the PP or PE
- require agents to use the approved method(s) of transferring records of PHI, and
- prohibit all other methods of transferring records of PHI.

Process of Secure Transfer

The procedures that must be followed in securely transferring records of PHI through each of the approved method(s) must also be outlined. This must include specifying:

- the conditions pursuant to which records of PHI will be transferred
- the agent(s) responsible for ensuring the secure transfer
- any documentation that is required to be completed, provided, and/or executed in relation to the secure transfer, including the:
    - agent(s) responsible for completing, providing, and/or executing the documentation, and
    - required content of the documentation
- whether and in what circumstances the agent transferring records of PHI is required to document the date, time, and mode of transfer
- the recipient of the records of PHI
- the nature of the records of PHI transferred, and

- whether and in what circumstances confirmation of receipt of the records of PHI is required from the recipient, and if so:
    - the manner of obtaining and recording acknowledgement of receipt of the records of PHI, and
    - the agent(s) responsible for obtaining and recording acknowledgement of receipt of the records of PHI.

In addressing whether and in what circumstances an agent is required to document the transfer and confirm receipt, regard must be had to the other privacy and information security policies, procedures, and practices put in place, including the:

- ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information***
- ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information***
- ***Policy, Procedures, and Practices for Back-Up and Recovery of Records of Personal Health Information***, and
- ***Policy, Procedures, and Practices for Executing Agreements with TPSPs in Respect of Personal Health Information***.

Administrative, Technical, and Physical Safeguards to Ensure Secure Transfer

The policy, procedures, and practices must outline the administrative, technical, and physical safeguards that agents must implement in transferring records of PHI through each of the approved method(s) to ensure that the records of PHI are transferred in a secure manner.

At a minimum, the PP or PE must ensure that the approved method(s) of securely transferring records of PHI and the procedures and safeguards that are required to be implemented in respect of the secure transfer of records of PHI are consistent with:

- **PHIPA** and its **regulations**
- orders and decisions issued by the IPC under PHIPA and its regulations, including but not limited to **Order HO-004**, **Order HO-007**, **Order HO-008** and **Order HO-011**
- guidelines, fact sheets, and best practices issued by the IPC, including **Fact Sheet: Communicating Personal Health Information by Email, Fact Sheet 18: The Secure Transfer of Personal Health Information**, and
- evolving privacy and information security standards and best practices.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the PP or PE at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if

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

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

10. Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information

A policy, procedures, and practices must be developed and implemented with respect to the secure disposal of records of PHI in both paper and electronic format in order to ensure that reconstruction of these records is not reasonably foreseeable in the circumstances.

The policy, procedures, and practices must:

- where a determination is made to dispose of records of PHI, require the records to be disposed of in a secure manner
- provide a definition of secure disposal that is consistent with **PHIPA** and its **regulations**, and
- outline the circumstances in which and the conditions pursuant to which the records of PHI must be securely disposed of.

Methods of Secure Disposal

The policy, procedures, and practices must further identify the precise method(s) by which records of PHI in paper or electronic format, including records retained on various media, are required to be securely disposed of. At a minimum, these methods must be consistent with:

- **PHIPA** and its **regulations**
- orders and decisions issued by the IPC under PHIPA and its regulations, including but not limited to **Order HO-001** and **Order HO-006**
- guidelines, fact sheets, and best practices issued by the IPC pursuant to PHIPA and its regulations, including **Fact Sheet 10: Secure Destruction of Personal Information**, and
- evolving privacy and information security standards and best practices.

Secure Retention Pending Disposal

The policy, procedures, and practices must further address the secure retention of records of PHI pending their secure disposal in accordance with the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information***. At a minimum, the policy, procedures, and practices must require:

- the physical segregation of records of PHI intended for secure disposal from other records intended for recycling
- that an area be designated for the secure retention of records of PHI pending their secure disposal
- that records of PHI be retained in a clearly marked and locked container pending their secure disposal, and
- the identification of the agent(s) responsible for ensuring the secure retention of records of PHI pending their secure disposal.

Process of Secure Disposal

In the event that records of PHI or certain categories of records of PHI will be securely disposed of by a designated agent, the policy, procedures, and practices must:

- identify the designated agent responsible for securely disposing of the records of PHI
- outline the circumstances in which and the conditions pursuant to which the records of PHI must be securely disposed of, and
- set out the responsibilities of the designated agent in securely disposing of the records.

The policy, procedures, and practices must also outline the process to be followed:

- in tracking the dates that records of PHI are transferred for secure disposal and certificates of destruction are received from the designated agent, and the agent(s) responsible for conducting such tracking, and
- where a certificate of destruction is not received within the timeframe set out in the policy, procedures, and practices, and the agent(s) responsible for implementing this process.

In the event that records of PHI or certain categories of records of PHI will be securely disposed of by an agent that is a TPSP, the policy, procedures, and practices must incorporate those additional requirements set out in the ***Policy, Procedures, and Practices for Executing Agreements with Third-Party Service Providers in Respect of Personal Health Information***, including the ***Template Agreement for Third-Party Service Providers***.

Certificate of Destruction

The policy, procedures, and practices must identify the:

- agent of the PP or PE to whom the certificate of destruction must be provided
- timeframe following secure disposal within which the certificate of destruction must be provided, and
- required content of the certificate of destruction.

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

- identify the records of PHI securely disposed of
- indicate the date, time, and method of secure disposal employed, and

- bear the name and signature of the agent who performed the secure disposal.

The policy, procedures, and practices must also address where **certificates of destruction** will be retained, and the agent(s) responsible for retaining the certificates of destruction.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

Information Security

11. Policy, Procedures, and Practices Relating to Authentication and Passwords

A policy, procedures, and practices must be developed and implemented with respect to authentication and passwords for access to information systems, technologies, equipment, resources, applications, and programs regardless of whether they are owned, leased, or operated by the PP or PE.

With regard to passwords, the policy, procedures, and practices must address:

- the required minimum length of passwords
- composition and complexity requirements
- any restrictions on passwords, such as re-use of prior passwords, the use of passwords that resemble prior passwords, and the use of well-known weak passwords
- the timeframe within which passwords will automatically expire
- the frequency with which passwords must be changed
- the process for resetting passwords
- the consequences arising from a defined number of failed log-in attempts
- the imposition of a mandatory system-wide password-protected device lock-out after a defined period of inactivity

- whether and how passwords are stored locally on devices, and
- whether and how passwords are managed by software applications, such as password managers.

The PP or PE must require additional levels of identity assurance in proportion to the sensitivity of the **information security components** within the **information environment** that an agent seeks to access. In this regard, the policies, procedures, and practices must address other factors of authentication supplementing or replacing passwords (e.g. multi-factor authentication), and when these factors will be required.

The policy, procedures, and practices must further identify the administrative, technical, and physical safeguards that must be implemented by agents in respect of authentication and passwords in order to ensure that the PHI is protected against theft, loss, and unauthorized collection, use, or disclosure and that the records of PHI are protected against unauthorized copying, modification, or disposal. At a minimum, agents must be:

- required to keep their passwords private and secure
- required to change their passwords immediately if they suspect that the password has become known to any other individual, including another agent, and
- prohibited from writing down, displaying, revealing, hinting at, providing, sharing, or otherwise making their password known to any other individual, including another agent of the PP or PE.

The PP or PE must also ensure that the policy, procedures, and practices it has developed in this regard are, at a minimum, consistent with:

- orders and decisions issued by the IPC under PHIPA and its regulations
- guidelines, fact sheets, and best practices issued by the IPC, and
- evolving privacy and information security standards and best practices.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

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

12. Policy, Procedures, and Practices in Respect of Privacy Flags and Notices to Agents

A policy, procedures, and practices must be developed and implemented requiring privacy flags and notices to be displayed:

- to each user, at a minimum, once daily, and
- upon the user's initial daily log-in to the PP's or PE's information environment or at the first reasonable opportunity thereafter.

The policy, procedures, and practices must also set out the required content of the privacy flag and notice, and must require the privacy flag and notice to be prominently displayed on components within the information environment on which PHI is retained or that are capable of displaying PHI, and must require agents to acknowledge and agree to certain statements prior to accessing PHI. At a minimum, the privacy flag and notice must:

- indicate that all instances in which PHI is collected, used, and disclosed will be logged, audited and monitored
- require agents to acknowledge and agree that they:
    - will only collect, use, or disclose PHI for the purposes necessary for carrying out their employment, contractual, or other responsibilities
    - will comply with PHIPA and its regulations, and
    - have read and understood, and will comply with, the privacy and information security policies, procedures, and practices put in place, and
- set out the consequences for collecting, using, or disclosing PHI for other purposes, and for failing to comply with PHIPA and its regulations and with the privacy and information security policies, procedures, and practices put in place by the PP or PE.

The policy, procedures, and practices and the privacy flag and notice developed must, at a minimum, be consistent with:

- orders and decisions issued by the IPC under PHIPA and its regulations, including **Order HO-013**, and
- guidelines, fact sheets, and best practices issued by the IPC, including **Detecting and Deterring Unauthorized Access to Personal Health Information**.

The policy, procedures, and practices must:

- identify the agent(s) responsible for developing and displaying privacy flags and notices on components within the information environment on which PHI is retained or that are capable of displaying PHI, and

- set out the documentation that must be completed, provided, and/or executed in respect of the privacy flags and notices, including the:
    - agent(s) responsible for completing, providing, and/or executing the documentation
    - agent(s) to whom this documentation must be provided, and
    - required content of the documentation.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

13. Policy, Procedures, and Practices for Logging, Monitoring, and Auditing Privacy and Information Security Events

Each PP or PE must develop and implement a policy, procedures, and practices with respect to the logging, monitoring, and auditing of privacy and information security events. The policy, procedures, and practices that is applied must also be commensurate with the:

- amount and sensitivity of the PHI maintained
- number and roles of agents with access to PHI, and
- threats and risks associated with the PHI.

In developing the policy, procedures, and practices, the PP or PE must, at a minimum, have regard to:

- findings, mitigations, and other relevant recommendations of information security audits conducted in accordance with the ***Policy, Procedures, and Practices in Respect of Information Security Audits***
- findings, mitigations, and other relevant recommendations arising from investigations of privacy breaches and/or information security breaches
- trends and systemic issues arising from privacy complaints

- orders and decisions issued by the IPC under PHIPA and its regulations, including orders **HO-010** and **HO-013**
- guidelines, fact sheets, and best practices issued by the IPC, including **Detecting and Deterring Unauthorized Access to Personal Health Information**
- requirements of PHIPA and its regulations, including obligations of custodians under sections 12 and 13 of PHIPA
- findings, mitigations, and other recommendations arising from prior three-year reviews, and
- evolving privacy and information security standards and best practices.

Logging of Privacy and Information Security Events

The policy, procedures, and practices must require the PP or PE to determine which privacy and information security events are mandatory to be logged, ensure that the **information environment** has the functionality to log the required content for all mandatory privacy and information security events, and validate that the mandatory privacy and information security events are in fact logged.

The policy, procedures, and practices must further set out the processes to be followed and the agent(s) responsible for:

- determining, reviewing, and approving which privacy and information security events are mandatory to be logged
- the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny privacy and information security events to log
- determining what information must be contained in the log for each privacy and information security event, and
- ensuring the information environment has the functionality to log the required privacy and information security events and that the required privacy and information security events are in fact logged, along with the required content of each log entry.

The policy, procedures, and practices must further set out the:

- documentation that must be completed, provided, and/or executed in determining which privacy and information security events to log
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom this documentation must be provided, and
- required content of the documentation.

Mandatory Events to Log

At a minimum, the policy, procedures, and practices must require the following privacy and information security events to be logged in the information environment:

- all events to collect, create, access, use, modify, transmit, disclose, dispose of, or otherwise deal with PHI
- authentication and authorization events (e.g., log in, log out, deny access, etc.)
- user account management events (e.g., password change, role assignment)
- changes to system software and configuration
- alerts and events generated by information security controls, and
- other events in accordance with evolving privacy and information security standards and best practices.

Required Content of Log Entries

At a minimum, the policy, procedures, and practices must require the privacy and information security event logs to include:

- the types of events that are required to be logged and audited
- the nature and scope of the information that must be contained in system control and audit logs
- the date and time of the event
- the name of the user or unique identifier associated with the individual performing the event
- where applicable, the network name, network address, and other identifying information about the computer with which the action being logged is performed, and
- any additional information in accordance with evolving privacy and information security standards and best practices.

With respect to events to collect, create, access, use, modify, transmit, disclose, dispose of, handle or otherwise deal with PHI, the privacy and information security event log entries must, where reasonable in the circumstances, also include:

- the type of information that was collected, created, accessed, used, modified, transmitted, disclosed, disposed of, and/or otherwise dealt with
- any changes to values, and
- the name or unique identifier associated with the individual to whom PHI relates.

Retention of Logs

The policy, procedures, and practices must identify:

- the length of time that privacy and information security event logs are required to be retained
- the agent(s) responsible for retaining the privacy and information security event logs, and
- where the privacy and information security event logs will be retained.

The policy, procedures, and practices must also require the privacy and information security event logs to be secure and immutable, that is, the PP or PE must ensure that the privacy and information security event logs cannot be amended by anyone, cannot be accessed without authority, and cannot be disposed of except in accordance with the conditions and retention periods specified in the policy, procedures, and practices.

Monitoring of Privacy and Information Security Events

The policy, procedures, and practices must require that the information environment and other information sources be systematically monitored to:

- identify and assess real-time evidence of a privacy breach or suspected privacy breach and/or information security breach or information security incident, and
- assist with the notification of the responsible agent(s) of the PP or PE, at the first reasonable opportunity, of:
    - a **privacy breach** or suspected privacy breach in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, or
    - an **information security breach** or information security incident in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***.

The policy, procedures, and practices must require that this monitoring be conducted in a continuous manner, or as close to continuous as is reasonable in the circumstances, in order to support identification, analysis, and investigation of a suspected privacy breach and/or information security incident, and assist with the confirmation of an actual privacy breach and/or an information security breach in a timely fashion.

The policy, procedures, and practices must further set out processes to be followed and the agent(s) responsible for:

- identifying the information sources to be monitored (i.e., as set out under “Monitoring Scope” below)
- establishing the criteria that must be considered in identifying the information sources to be monitored
- developing, reviewing, approving, and implementing monitoring tools and mechanisms (including developing detailed procedures for reviewing, assessing, and responding to the outputs of the monitoring tools and mechanisms)
- establishing the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny monitoring tools and mechanisms, and
- ensuring the monitoring is conducted on a continuous basis or as close to continuous as possible.

With regard to the monitoring that is conducted, the policy, procedures, and practices must also set out the documentation that must be completed, provided, and/or executed including the:

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

Monitoring Scope

The policy, procedures, and practices must identify the information sources subject to monitoring. At a minimum, the policy, procedures, and practices must require monitoring of the following information sources:

- logs of privacy and information security events retained by the PP or PE (e.g., those listed under "Mandatory Events to Log" above)
- information security data sources (e.g., network traffic, incoming/outgoing emails, device status monitoring, alerts)
- physical security data sources (e.g., security card activity, motion sensors, temperature, and humidity measurements), and
- human resources data sources (e.g., employee hiring and termination records, role changes).

Monitoring Tools and Mechanisms

The policy, procedures, and practices must require the use of tools and mechanisms to support real-time analysis of the information sources subject to monitoring for evidence of actual or potential **privacy** and/or **information security breaches**. These tools and mechanisms:

- should be automated (e.g., by using a security information and event management (SIEM) tool), and
- must be configured to detect a reasonably comprehensive range of privacy and information security threat scenarios, including to detect:
    - unauthorized actions with respect to PHI by otherwise authorized users, and
    - intrusions from unauthorized individuals into systems that process and/or retain PHI.

The policy, procedures, and practices must require that the monitoring tools and mechanisms be regularly updated to:

- address any findings, mitigations, and other relevant recommendations arising from privacy and information security audits
- address the investigations of privacy breaches, information security breaches, and privacy complaints, and
- reflect evolving privacy and information security best practices with respect to monitoring.

Further, the policy, procedures, and practices must require that a method to identify, assess, and remediate problems with the monitoring be implemented, including if:

- privacy or information security event logs are rendered inaccessible to monitoring tools or mechanisms, and
- monitoring tools or mechanisms are offline or suffer degradations in performance.

The policy, procedures, and practices must require that a record be kept of every instance in which the monitoring tools and mechanisms were unavailable, unattended or there was otherwise a failure to monitor in accordance with the policy, procedures, and practices, describing the:

- time and date of the monitoring failure
- nature of the failure
- reason for the failure, and
- time and date at which monitoring resumed.

Procedures for Reviewing, Assessing, and Responding to Outputs of Monitoring Tools and Mechanisms

The policy, procedures, and practices must require the development of procedures for reviewing, assessing, and responding to the outputs of the monitoring tools and mechanisms to determine if the circumstances warrant the triggering of an alert that would lead to further investigation and/or notification of a **privacy breach** or suspected privacy breach and/or of an **information security breach** or information security incident. At a minimum, the circumstances must include situations where the agent(s) responsible for responding to the outputs of the monitoring tools and mechanisms has either confirmed, or has reasonable grounds to suspect that, one of the monitored threat scenarios has occurred or may occur.

The policy, procedures, and practices must set out the following detail with respect to outputs of monitoring tools and mechanisms:

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

Auditing of Privacy and Information Security Event Logs

The policy, procedures, and practices must require that regular audits of privacy and information security event logs be conducted in accordance with the ***Policy, Procedures, and Practices in Respect of Information Security Audits*** and identify the agent(s) responsible for conducting the audits.

At a minimum, the policies, procedures, and practices must require auditing of privacy and information security event logs:

- as necessary, in response to privacy inquiries and privacy complaints from individuals regarding the collection, use, or disclosure of their PHI

- whenever a privacy or information security breach or suspected privacy or information security breach is identified
- of instances, or a randomized representative sample of instances, where PHI is collected, created, accessed, used, modified, transmitted, disclosed, disposed of, or otherwise handled by an agent of the PP or PE
- to review user entitlements such as roles, permissions, elevated privileges
- as necessary, to investigate if an identified vulnerability was exploited
- in the event of suspected failures of information security controls, including monitoring, and
- to detect and deter potential privacy and information security breaches in accordance with threat and risk assessments, other information security reviews and audits, and information security best practices in response to the evolving threat landscape.

The policy, procedures, and practices must require a reasonable combination of the following auditing and monitoring types:

- proactive (e.g., to identify potential privacy and information security breaches) and reactive (e.g., in response to a privacy complaint or the investigation of a real or potential privacy or information security breach), and
- targeted (e.g., activities of a specific agent or activities of all agents in relation to a specific individual) and random (e.g., activities of a randomly selected agent or activities of all agents in respect of a randomly selected individual).

The policy, procedures, and practices must set out a process for addressing the findings arising from the audit of the privacy and information security event logs, and identify the agent(s) responsible for:

- assigning other agent(s) to address the findings
- establishing timelines to address the findings
- monitoring and ensuring the treatment of findings within stated timelines, and
- addressing any mitigations to resolve residual risks remaining after implementation, as required.

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

- the nature of the documentation, if any, that must be completed, provided, and/or executed following an audit of the privacy and information security event log(s)
- agent(s) responsible for completing, providing, executing, and/or ensuring the execution of the documentation
- agent(s) to whom the documentation must be provided
- frequency with which this documentation must be provided
- timeframe within which the documentation must be provided
- required content of the documentation

- manner and format for communicating the findings of the audit of the privacy and information security event logs, including the level of required detail, and how the findings have been or are being addressed
- the agent(s) responsible for communicating the findings of the audit of the privacy and information security event logs
- timeframe within which the findings of the audit of the privacy and information security event logs must be communicated
- persons to whom the findings must be communicated, including the circumstances in which the findings must be communicated to the chief executive officer or the executive director (or equivalent position)
- process to be followed in tracking that the findings of the audit of the privacy and information security event logs have been addressed within the identified timelines, and
- agent(s) responsible for tracking that the findings have been addressed within the identified timelines.

Review of Logging, Monitoring, and Auditing Practices

The policy, procedures, and practices must require that the privacy and information security event logging, monitoring, and auditing practices be regularly reviewed and must include assessments to determine if the logging, monitoring, and auditing practices effectively meet the requirements of the policies, procedures, and practices. Specifically, the policy, procedures, and practices must identify the:

- agent(s) responsible for reviewing the privacy and information security event logging, monitoring, and auditing practices
- frequency with which and the circumstances in which privacy and information security event logging, monitoring, and auditing practices are required to be reviewed
- process to be followed in conducting the reviews,
- process to be followed when reviewing and updating the types of privacy and information security events that must be logged, and
- required content of each log of privacy and information security events.

Further, the policy, procedures and practices must require the PP or PE to establish a process for detecting situations where the information environment fails to log privacy and information security events as required or are otherwise rendered inaccessible to monitoring processes. Such reviews must be conducted in accordance with the ***Policy, Procedures, and Practices in Respect of Information Security Audits***.

Relationship with Privacy Breach Management and Information Security Breach Management

The policy, procedures, and practices must:

- require the agent(s) responsible for logging, monitoring, and auditing of the privacy and information security events to notify the PP or PE, at the first reasonable opportunity, of:
    - a privacy breach or suspected privacy breach in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, and/or
    - an information security breach or information security incident in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, and
- identify the relationship between this policy, procedures, and practices and the ***Policy, Procedures, and Practices for Privacy Breach Management*** and the ***Policy, Procedures, and Practices for Information Security Breach Management***.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

14. Policy, Procedures, and Practices for Vulnerability and Patch Management

A policy, procedures, and practices must be developed and implemented for vulnerability and patch management.

Asset Inventory

The policy, procedures, and practices must:

- require that an inventory be maintained of all networks, information systems, technologies, applications, software, servers, components, and configurations within the **information environment** of the PP or the PE
- define the frequency with which and the circumstances in which the inventory must be updated
- identify the agent(s) responsible for maintaining and updating the inventory

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

Vulnerability Assessments

The policy, procedures, and practices must require that the components within the information environment listed in the inventory be subject to regular assessments. The purpose of the assessments is for the PP or PE to complete a systematic review to identify the vulnerabilities or the security weaknesses within the information environment and identify, track, and apply mitigations to protect the PHI.

The policy, procedures, and practices must specify the:

- types of vulnerability assessment(s) the PP or PE would apply to the **information security components** within the **information environment**
- purpose of each assessment
- process for how the PP or PE would quantify the severity of any vulnerabilities
- need to develop recommendations and timelines to mitigate those vulnerabilities
- agent(s) responsible for ensuring scans are conducted for the presence of vulnerabilities to information security components within the information environment listed in the inventory
- documentation required to be completed, provided, and/or executed
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom this documentation must be provided, and
- required content of the documentation.

The policy, procedures, and practices must also:

- set out the frequency with which regular scanning must be conducted
- detail the circumstances that may trigger the need for immediate scanning
- specify the procedure that must be followed
- require scanning the information environment of the PP or the PE from both internal and external vantage points, and must include authenticated and unauthenticated scanning
- require tool(s) used for vulnerability scanning to be kept up-to-date with detection methods for the latest vulnerabilities, and
- identify the agent(s) responsible and process to be followed in keeping the tool(s) used for vulnerability scanning up-to-date.

Vulnerability Assessment and Recommendations

The policy, procedures, and practices must require that each vulnerability assessment performed include:

- a clear articulation of the test(s) to be conducted
- the identification of any weakness(es) in the information environment and its components
- risks associated with identified vulnerabilities
- an assessment of the severity of the vulnerability, and
- recommendation(s) to be developed and implemented to mitigate those risk(s) in accordance with the ***Policy, Procedures, and Practices in Respect of Information Security Audits***.

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

- criteria upon which the assessments and recommendations are to be made
- process by which the assessments and recommendations are to be made
- agent(s) responsible for:
    - assessing vulnerabilities, including residual vulnerabilities likely to remain after patches and other mitigation measures
    - developing recommendations
    - determining the timeframe for the implementation of recommendations such as patches or other mitigation methods, and
    - documentation that must be completed, provided, and/or executed.

At a minimum, the vulnerability risk assessment process must include:

- a requirement to document every instance in which there was a failure to conduct a vulnerability assessment in accordance with the policy, procedures, and practices, and for each instance, the:
    - time and date of the failure to conduct vulnerability scanning
    - type(s) of assessment(s) attempted
    - nature of the failure
    - reason for the failure, and
    - time and date at which scanning resumed
- a framework for ranking risk severity of identified vulnerabilities (e.g., informational, low, medium, high, critical); this framework must be used:
    - when a PP or PE is conducting an assessment of each identified vulnerability, and

    - to support decision-making with respect to the timeframe associated with the approval and implementation of recommendations such as patches or other mitigation methods

- a process for determining if identified vulnerabilities warrant an audit of privacy and information security event logs in order to search for evidence of exploitation; such an audit must be conducted in accordance with the ***Policy, Procedures, and Practices for Logging, Monitoring, and Auditing Privacy and Information Security Events*** and the ***Policy, Procedures, and Practices in Respect of Information Security Audits***, and
- a process for monitoring the implementation of recommendations which must address the:
    - circumstances in which one or more components and configurations within the information environment listed in the inventory must be re-scanned to verify the effectiveness of risk mitigation and any residual risks remaining
    - agent(s) responsible for ensuring the re-scanning is administered, including the documentation that must be completed, provided, and/or executed
    - agent(s) responsible for completing, providing, and/or executing this documentation
    - agent(s) to whom this documentation must be provided, and
    - required content of the documentation.

Patch Monitoring

The policy, procedures, and practices must require the PP or PE to monitor for the availability of patches and other mitigation methods. The policy, procedures, and practices must also identify the:

- agent(s) responsible for monitoring for the availability of patches and other mitigation methods (e.g., configuration changes) on behalf of the PP or PE
- frequency with which such monitoring must be conducted, and
- procedure that must be followed.

In monitoring for the availability of patches and other mitigation methods, the policy, procedures, and practices must have regard to the risks identified through vulnerability management scans and patches released periodically by the vendor.

Patch Analysis

The policy, procedures, and practices must:

- identify the agent(s) responsible for analyzing the patches and other mitigation methods
- identify the agent(s) responsible for making a determination as to whether the patches and other mitigation methods should be implemented
- set out the process that must be followed, and

- specify the criteria that must be considered by the agent(s) responsible for undertaking this analysis and making this determination.

Where Patch is Not to Be Implemented

In circumstances where a determination is made that the patches and other mitigation methods should not be implemented, the policy, procedures, and practices must require the responsible agent(s) to document the:

- description of the patches and other mitigation methods
- date that the patches and other mitigation methods became available
- severity level of the patch (e.g., informational, low, medium, high, critical)
- components within the information environment to which the patches and other mitigation methods relate, and
- rationale for determining that the patches and other mitigation methods should not be implemented.

Where Patch is to Be Implemented

In circumstances where a determination is made that the patches and other mitigation methods should be implemented, the policy, procedures, and practices must:

- identify the agent(s) responsible for establishing the:
    - timeframe for implementation of the patches and other mitigation methods, and
    - priority of the patches and other mitigation methods
- set out the criteria upon which these determinations are to be made
- specify the process by which these determinations are to be made, and
- detail the documentation that must be completed, provided, and/or executed.

Patch Implementation

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

- process for the implementation of patches and other mitigation methods, including the agent(s) responsible for their implementation
- circumstances in which patches and other mitigation methods must be tested prior to implementation, including the:
    - timeframe within which patches and other mitigation methods must be tested
    - procedure for testing, and
    - agent(s) responsible for testing, and
- documentation to be maintained in respect of:

- the implementation of patches and other mitigation methods
- the testing of patches and other mitigation methods
- patches and other mitigation methods that have been implemented, and
- agent(s) responsible for completing, providing, and/or executing, as well as maintaining this documentation.

At a minimum, such documentation must include:

- a description of the patches and other mitigation methods
- the date that the patches and other mitigation methods became available
- the severity level and priority of the patches and other mitigation methods (e.g., informational, low, medium, high, critical)
- the components within the information environment to which the patches and other mitigation methods relate
- the date that the patches and other mitigation methods were implemented
- the agent(s) responsible for implementing the patches and other mitigation methods
- if the patch or other mitigation method was not implemented in accordance with the required timeframe, the reason why the implementation did not occur within the required timeframe
- the date, if any, when the patches and other mitigation methods were tested prior to implementation
- the agent(s) responsible for testing, and
- whether or not the testing was successful.

Compliance, Audit, and Enforcement

The PP or PE must:

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

15. Policy, Procedures, and Practices Related to Change Management

A policy, procedures, and practices must be developed and implemented for receiving, reviewing, and determining whether to approve or deny a request for a change to the **information environment** of the PP or PE.

Review and Approval Process

The policy, procedures, and practices must identify the:

- agent(s) responsible for receiving, reviewing, and determining whether to approve or deny a request for a change to the **information environment**
- criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request for a change to the information environment
- process that must be followed and the requirements that must be satisfied in the decision-making process
- method and format in which the decision will be communicated, and to whom
- documentation required to be completed, provided, and/or executed, which at a minimum must describe:
    - the change requested
    - why the change is necessary, and
    - the impact of executing or not executing the change to the operational environment
- manner of documenting the decision approving or denying the request for a change to the information environment
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom this documentation must be provided, and
- required content of the documentation of the decision approving or denying the request for change to the information environment, which at a minimum, must describe:
    - the change to the information environment that was requested
    - date that the change was requested
    - name of the agent requesting the change
    - reasons for the decision to approve or not approve the change
    - the impact of executing or not executing the change, and
    - the name of the agent(s) responsible for making the decision.

Change Testing and Implementation

In cases where the change to the **information environment** is approved, the policy, procedures, and practices must also set out the:

- agent(s) responsible for determining the timeframe for implementation of the change and the priority assigned to the change requested
- criteria upon which these determinations are to be made
- process by which these determinations are to be made
- documentation that must be completed, provided, and/or executed in this regard
- process for implementation of the approved change(s) to the information environment
- agent(s) responsible for implementation
- documentation that must be completed, provided, and/or executed by the agent(s) responsible for implementation
- circumstances in which changes to the information environment must be tested (including information security testing)
- timeframe within which changes must be tested
- procedure for testing
- agent(s) responsible for testing, and
- documentation that must be completed, provided, and/or executed by the agent(s) responsible for testing.

The policy, procedures, and practices must also require documentation to be maintained of changes that have been implemented and identify the agent(s) responsible for maintaining this documentation. At a minimum, the documentation must include:

- a description of the change requested
- the name of the agent requesting the change
- the date that the change was requested
- the priority assigned to the change
- the date that the change was implemented
- the agent(s) responsible for implementing the change
- the date, if any, when the change was tested
- the agent(s) responsible for testing, and
- whether or not the testing was successful.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the PP or PE at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if

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

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

16. Policy, Procedures, and Practices for Back-Up and Recovery of Records of Personal Health Information

A policy, procedures, and practices must be developed and implemented for the back-up and recovery of records of PHI. The policy, procedures, and practices must identify the:

- nature and types of back-up storage devices maintained by the PP or PE
- frequency with which records of PHI are backed-up
- agent(s) responsible for the back-up and recovery of records of PHI
- process that must be followed and the requirements that must be satisfied
- documentation that must be completed, provided, and/or executed
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom this documentation must be provided, and
- required content of the documentation.

Testing Procedures for Back-Up, Recovery, and Retention of Records

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

- testing the procedure for back-up and recovery of records of PHI
- agent(s) responsible for testing
- frequency with which the procedure is tested
- process that must be followed in conducting such testing
- documentation that must be completed, provided, and/or executed by the agent(s) responsible for testing
- agent(s) responsible for ensuring that back-up storage devices containing records of PHI are retained in a secure manner
- location where they are required to be retained, and
- length of time that they are required to be retained.

The policy, procedures, and practices must require the backed-up records of PHI to be retained in compliance with the ***Policy, Procedures, and Practices for Secure Retention of Records of PHI*** and identify the agent(s) responsible for ensuring that they are retained in a secure manner.

Availability of Backed-Up Records

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

- need for the availability of backed-up records of PHI, and
- circumstances in which the backed-up records are required to be made available.

Third-Party Service Providers

If a TPSP is contracted to retain backed-up records of PHI, or where a TPSP backs-up records of PHI it has been contracted to retain, the policy, procedures, and practices must incorporate the requirements set out in the:

- ***Policy, Procedures, and Practices for Executing Agreements with Third- Party Service Providers in Respect of Personal Health Information,*** and
- ***Template Agreement for Third- Party Service Providers***.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

17. Policy, Procedures, and Practices on the Acceptable Use of Technology

A policy, procedures, and practices must be developed and implemented outlining the acceptable use of **information security components** within the **information environment** regardless of whether they are owned, leased, or operated by the PP or PE.

The policy, procedures, and practices of the PP or PE must set out the uses that are:

- permitted
- prohibited without exception, and
- permitted only with prior approval.

Where Use is Permitted Only with Prior Approval

For those uses that are permitted only with prior approval, the policy, procedures, and practices must identify the:

- agent(s) responsible for receiving, reviewing, and determining whether to approve or deny the request
- process that must be followed and the requirements that must be satisfied in receiving, reviewing, and determining whether to approve or deny requests
- documentation that must be completed, provided, and/or executed
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom this documentation must be provided, and
- required content of the documentation.

The policy and procedures must further set out the:

- criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request
- conditions or restrictions that apply to agents whose requests have been approved
- manner of documenting the decision approving or denying the request and the reasons for the decision, and
- method by which and the format in which the decision will be communicated, and to whom the decision will be communicated.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

Information Security Audit Program

18. Policy, Procedures, and Practices in Respect of Information Security Audits

A policy, procedures, and practices must be developed and implemented that sets out the types of information security audits that are required to be conducted.

Types of Information Security Audits

At a minimum, the audits required to be conducted must include:

- audits to assess compliance with the information security policies, procedures, and practices implemented by the PP or PE
- threat and risk assessments
- security reviews, tests, or assessments
- vulnerability assessments
- penetration testing or ethical hacks
- audits of information security breach procedures (e.g., tabletop exercise, red teaming, etc.);
- information security control effectiveness assessments (e.g., monitoring procedures, event logging practices, reviews of privacy and information security logging, monitoring, and auditing practices), and
- audits of privacy and information security event logs.

Information Security Audits

With respect to each information security audit that is required to be conducted, the policy, procedures, and practices must set out the:

- purposes of the information security audit
- nature and scope of the information security audit
- agent(s) responsible for conducting the information security audit, and
- frequency with which and the circumstances in which each information security audit is required to be conducted and must:
    - require an information security audit schedule to be developed, and
    - identify the agent(s) responsible for developing and ensuring the implementation of the information security audit schedule.

At a minimum, audits of agents granted access to the premises of the PP or PE and to locations within the premises where records of PHI are retained, under the ***Policy, Procedures, and Practices for Ensuring Physical Security of Personal Health Information***, must be conducted on an annual basis.

For each type of information security audit that is required to be conducted, the policy, procedures, and practices must also specify:

- the process to be followed in conducting the audit
- 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.

Exceptions

The policy, procedures, and practices may allow for certain **information security components** within the **information environment** to be exempted from penetration testing or ethical hacks in exceptional circumstances, where the penetration testing or ethical hacks could reasonably be expected to compromise the confidentiality, integrity, or availability of the information security components within the information environment.

The policy, procedures, and practices must not permit exceptions from penetration testing or ethical hacks for certain information security components unless the PP or PE can maintain a testing environment that is identical to the information environment. In the case of any information security components that are excepted from penetration testing or ethical hacks in the information environment, these excepted components must be subject to penetration testing or ethical hacks in the testing environment. The identified risks and recommendations resulting from the penetration testing or ethical hacks in the testing environment must be treated as though they were found within the information environment.

Required Documentation

The policy, procedures, and practices must further set out the:

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

Risk Treatment

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

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

Required Documentation

The policy, procedures, and practices of the PP or PE must also set out the:

- nature of the documentation that must be completed, provided, and/or executed at the conclusion of the information security audit
- agent(s) responsible for completing, providing, and/or executing the documentation
- required content of the documentation, and
- agent(s) to whom the documentation must be provided.

Risk Reporting

The policy, procedures, and practices of the PP or PE must also address the manner, circumstances, and format in which the findings and recommendations of information security audits, including the status of addressing the recommendations, are communicated. This must include identifying:

- the agent(s) responsible for communicating the findings of the information security audit
- the mechanism and format for communicating the findings of the information security audit, including the required level of detail for communicating the findings
- the timeframe within which the findings of the information security audit must be communicated, and
- to whom the findings of the information security audit will be communicated, including whether the findings must be communicated to the chief executive officer or the executive director (or equivalent position).

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

19. Log of Information Security Audits

A PP or PE must maintain a log of information security audits that have been completed. The log must set out the:

- nature and type of the information security audit conducted, i.e., a manual process, an automated process or some combination thereof
- type of information security audit(s) conducted
- date that the information security audit was completed
- agent(s) responsible for completing the information security audit
- findings arising from the information security audit, mitigations, and other relevant recommendations
- agent(s) responsible for addressing each mitigation and other relevant recommendation
- date that each mitigation and relevant recommendation was or is expected to be addressed, and
- manner in which each recommendation was or is expected to be addressed.

In addition to the above content, where a log entry relates to a vulnerability assessment, the log of information security audits must also set out:

- the assessment of the severity for each identified vulnerability (e.g., informational, low, medium, high, critical)
- a description of the vulnerability
- the number of **information security components** within the **information environment** with or affected by the identified vulnerability, and
- the following details for each component with the identified vulnerability:
    - date that each recommendation was or is expected to be addressed
    - agent(s) responsible for addressing each recommendation, and
    - manner in which each recommendation was or is expected to be addressed.

Information Security Breaches

20. Policy, Procedures, and Practices for Information Security Breach Management

A policy, procedures, and practices must be developed and implemented to address the identification, reporting, containment, notification, investigation, and remediation of **information security breaches** and must provide a definition of the term "information security breach."

At a minimum, an information security breach must be defined to include an occurrence that:

- actually or imminently jeopardizes the confidentiality, integrity, or availability of information or the information environment

- constitutes a contravention or imminent threat of contravention of PHIPA or its regulations, or
- constitutes a contravention or imminent threat of contravention of the terms of any written agreements, other legal obligations, or information security policies, procedures, and practices implemented by the PP or PE, related to the requirements of the Manual.

The policy, procedures, and practices of a PP or PE may refer to some types of information security breaches using the term "information security incident" instead of "**information security breach**," so long as the requirements contained in the policy, procedures, and practices related to information security incidents otherwise comply with the requirements of the Manual applicable to information security breaches. For the purposes of this Manual, suspected information security breaches are considered information security incidents until confirmed as information security breaches.

Identification of Information Security Breaches

The policy, procedures, and practices must set out the manner in which **information security breaches** or information security incidents will be identified by the PP or PE. At a minimum, the policy, procedures, and practices must indicate:

- that information security breaches or information security incidents will be identified through notifications, including by agents and electronic service providers of the PP or PE, as well as information security audits, privacy complaints, and inquiries, and
- the auditing and monitoring required to be performed by the PP or PE in accordance with the:
    - ***Policy, Procedures, and Practices for Logging, Monitoring, and Auditing Privacy and Information Security Events,*** and
    - **Policy, Procedures, and Practices in Respect of Information Security Audits**.

The policy, procedures, and practices must require that agents notify the PP or PE of all information security breaches or information security incidents at the first reasonable opportunity.

In this regard, the policy, procedures, and practices must:

- identify the agent(s) who must be notified of the information security breach or information security incident and provide their contact information
- stipulate whether the notification must be provided orally and/or in writing and the nature of the information that must be included within the notification
- set out the documentation that must be completed, provided, and/or executed with respect to notification
- identify the agent(s) responsible for completing, providing, and/or executing the documentation
- identify the agent(s) to whom this documentation must be provided, and
- specify the required content of the documentation.

Determination of Whether an Information Security Breach Occurred

Upon notification of an information security breach, the policy, procedures, and practices must set out a process for determining:

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

Prioritization Framework

The policy, procedures, and practices should include a prioritization framework based on risk that supports the systematic allocation of resources for addressing information security breaches or information security incidents. Such a framework should include specific criteria for determining the prioritization level for a particular information security breach or information security incident at a given point in time, allowing for **information security breaches** or information security incidents to be escalated or de-escalated in response to an evolving situation.

The prioritization framework criteria should include the consideration of factors, such as the:

- potential impact of the information security breach
- recoverability from the information security breach, and
- the extent at which PHI may be affected.

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

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

Breach Notification to Senior Management

The policy, procedures, and practices must further address when and in what circumstances senior management, including the chief executive officer or the executive director (or equivalent position), will be notified. This must include:

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

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

Relationship to Policy, Procedures, and Practices for Privacy Breach Management

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

Containment

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

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

In undertaking containment, the policy, procedures, and practices must ensure that:

- reasonable steps are taken in the circumstances to protect PHI from further theft, loss, or unauthorized collection, use, or disclosure, and
- additional information security breaches cannot occur through the same means.

The policy, procedures, and practices must identify the:

- agent(s) responsible and the process to be followed in:
    - reviewing the containment measures implemented
    - determining whether the information security breach has been effectively contained or whether further containment measures are necessary
- documentation that must be completed, provided, and/or executed by the agent(s) responsible for reviewing the containment measures
- required content of the documentation, and
- agent(s) to whom this documentation must be provided.

Breach Notification to Custodians or Other Organizations

The policy, procedures, and practices must require the PP or PE to notify the custodian(s) or other organization(s) that disclosed the PHI to the PP or PE at the first reasonable opportunity whenever PHI is or is believed to be stolen, lost or collected, used or disclosed without authority and whenever required pursuant to the agreement with the custodian or other organization.

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

- agent(s) responsible for notifying the custodian(s) or other organization(s)

- format of the notification, and
- nature of the information that will be provided upon notification.

At a minimum, the policy, procedures, and practices must require the custodian(s) or other organization(s) to be advised of:

  - the extent of the **information security breach**
  - the nature of the PHI at issue, if any
  - the measures implemented to contain the information security breach, and
  - further actions that will be undertaken with respect to the information security breach, including investigation and remediation.

Breach Notification to the IPC

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

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

The PP or PE must notify the IPC, at the first reasonable opportunity, of information security breaches in the circumstances set out in subsections 6.3(1) and 18.3(1) of PHIPA's regulations, as if the PP or PE were a custodian.

Breach Notification to Affected Individuals

However, as a secondary collector of PHI, a PP or PE should not directly notify the individual to whom the PHI relates of an **information security breach**. Where applicable, the required notification to individuals must be provided by the relevant custodian(s), unless an alternative decision regarding breach notification to affected individuals is approved by the IPC.

Investigation and Recommendations

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

- agent(s) responsible for investigating the **information security breach**
- nature and scope of the investigation (e.g., document reviews, interviews, forensic analysis, site visits, inspections)
- process that must be followed in investigating the information security breach
  - documentation that must be completed, provided, and/or executed in undertaking the investigation
  - agent(s) responsible for completing, providing, and/or executing the documentation

- agent(s) to whom this documentation must be provided, and
- required content of the documentation.

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

- assigning other agent(s) to address the mitigations and any other relevant recommendations
- establishing timelines to address the mitigations and any other recommendations
- monitoring and ensuring that the mitigations and any other relevant recommendations are addressed within the stated timelines, and
- evaluating the residual risks remaining after implementation.

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

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

Communication of Findings of Investigation and Recommendations

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

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

Tracking Information Security Breaches

The policy, procedures, and practices must require that a log be maintained of **information security breaches** and must:

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

21. Log of Information Security Breaches

A PP or PE must maintain a log of **information security breaches** and information security incidents. At a minimum, the log must set out:

- the date of the information security breach or information security incident;
- the date that the information security breach was identified or suspected
- the nature of the PHI, if any, that was the subject matter of the information security breach and the nature and extent of the information security breach
- a description of the information security breach or information security incident and who identified the information security breach or information security incident
- the cause of the information security breach or information security incident
- whether an unauthorized person who is not an agent or **electronic service provider** caused the information security breach or information security incident and the name or a description of the unauthorized person, if applicable
- the date that the chief executive officer or executive director (or equivalent position) and senior management were notified of the information security breach or information security incident, if the applicable
- the date that the information security breach was contained and the nature of the containment measures
- the name of the agent(s) responsible for containing the information security breach or information security incident
- the date that the investigation was commenced
- the date that the investigation was completed

- the agent(s) responsible for conducting the investigation
- the findings, mitigations, and any other relevant recommendations arising from the investigation
- the agent(s) responsible for addressing each recommendation
- the manner in which each recommendation was or is expected to be addressed
- the date that each recommendation was or is expected to be addressed
- the date that the chief executive officer or executive director (or equivalent position) and senior management were notified of the findings, mitigations, and other relevant recommendations arising from the investigation, if applicable
- the date that the custodian or other organization that disclosed the PHI to the PP or PE was notified, if applicable
- the date that notification was provided to the IPC, if applicable, and
- the date that notification was provided to individuals, if applicable.

Part 3 – Human Resources Policies, Procedures, and Practices

Privacy Training and Awareness

1. Policy, Procedures, and Practices for Privacy Training and Awareness

A policy, procedures, and practices must be developed and implemented requiring agents of the PP or PE to attend initial privacy training as well as ongoing privacy training.

Timing and Method of Initial and Ongoing Privacy Training

The policy, procedures, and practices must set out the timeframe within which agents must complete the initial privacy training as well as address the frequency of ongoing privacy training. At a minimum, the policy, procedures, and practices must:

- require an agent to complete the initial privacy training prior to being given access to PHI
- require an agent to complete ongoing privacy training provided by the PP or PE on an annual basis thereafter, and
- address the method(s) by which the initial and ongoing privacy training will be provided.

Process for Preparing the Content and Delivering Privacy Training

The policy, procedures, and practices must:

- identify the agent(s) responsible for preparing the content and ensuring the delivery of the initial and ongoing privacy training
- require the content of the initial and ongoing privacy training to be reviewed on an annual basis, and updated as needed
- specify the frequency with which the training will be reviewed
- identify the agents(s) responsible for reviewing and updating the training
- set out the process that must be followed in notifying the agent(s) responsible for ensuring the delivery of the initial privacy training when an agent has commenced or will commence an employment, contractual, or other relationship with the PP or PE
- identify the agent(s) responsible for providing notification
- set out the format of the notification and the timeframe within which such notification must be provided.

Initial Privacy Training

The policy, procedures, and practices must also require the content of the initial privacy training to be formalized and standardized, and be based on evolving industry privacy standards and best practices. At a minimum, the policy, procedures, and practices must require that the initial privacy training include:

- a description of the status of the PP or PE under PHIPA and the duties and responsibilities that arise as a result of this status
- a description of the nature of the PHI collected and from whom this information is typically collected
- an explanation of the purposes for which PHI is collected and used and how this collection and use is permitted by PHIPA and its regulations
- limitations placed on access to and use of PHI by agents
- a description of the manner in which the agent's activities in the information environment will be logged, monitored, and audited, including in relation to PHI
- limitations, conditions, or restrictions placed on the PHI, including prohibitions on collecting, using, or disclosing PHI if other information, such as de-identified and/or aggregate information, will serve the purpose identified and on collecting, using, or disclosing more PHI than is reasonably necessary
- a description of the procedure that must be followed in the event that an agent is requested to disclose PHI
- an overview of the privacy policies, procedures, and practices that have been implemented by the PP or PE and the obligations arising from these policies, procedures, and practices
- the consequences of breach of PHIPA or its regulations or breach of the privacy policies, procedures, and practices implemented
- an explanation of the privacy program, including the key activities of the program and the agent(s) who have been delegated day-to-day authority to manage the privacy program
- the administrative, technical, and physical safeguards implemented by the PP or PE to protect PHI against theft, loss, and unauthorized collection, use, or disclosure and to protect records of PHI against unauthorized copying, modification, or disposal
- the duties and responsibilities of agents in implementing the administrative, technical, and physical safeguards put in place by the PP or PE
- the purposes for which de-identified or aggregated information derived from PHI collected by the PP or PE may be used or disclosed
- a prohibition on using de-identified or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is:
    - done in accordance with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***, and
    - permitted by PHIPA or another law, and a notice that compliance with this prohibition will be audited and monitored
- the nature and purpose of Privacy Notices and Confidentiality Agreements, and the key provisions of these notices and agreements

- an explanation of the ***Policy, Procedures, and Practices for Privacy Breach Management*** and the related duties and responsibilities imposed on agents in identifying, reporting, containing, and participating in the investigation and remediation of privacy breaches, including the duty to notify the PP or the PE, at the first reasonable opportunity, of a privacy breach or a suspected privacy breach, and
- an explanation of the mandatory nature of privacy training, including the:
    - prohibition on all agents to handle PHI without having completed initial privacy training, and
    - mandatory nature of ongoing privacy training on an annual basis thereafter.

Ongoing Privacy Training

The policy, procedures, and practices must also require the content of the ongoing privacy training to be formalized and standardized, and be based on evolving industry privacy standards and best practices. At a minimum, the policy, procedures, and practices must require that ongoing privacy training:

- include role-based training in order to ensure that agents understand how to apply the privacy policies, procedures, and practices in their day-to-day employment, contractual, or other responsibilities as these may have evolved since their last training
- address any new privacy policies, procedures, and practices and significant amendments to existing privacy policies, procedures, and practices, and
- incorporate any relevant changes since the last training, including:
    - recommendations with respect to privacy training made in privacy impact assessments, privacy audits, and the investigation of privacy breaches and privacy complaints
    - orders, decisions, guidelines, fact sheets, and best practices issued by the IPC under PHIPA and its regulations, and
    - amendments to PHIPA and its regulations relevant to the PP or PE.

Tracking, Auditing, and Monitoring Privacy Training

The policy, procedures, and practices must require a log to be maintained to track the attendance and completion of the initial and ongoing privacy training and identify the following:

- agent(s) responsible for maintaining such a log
- process to be followed in tracking completion of the initial and ongoing privacy training
- documentation that must be completed, provided, and/or executed to verify completion
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent to whom this documentation must be provided
- required content of the documentation

- where documentation related to completion of the initial and ongoing privacy training will be retained, and
- agent(s) responsible for retaining this documentation.

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

- agent(s) responsible for identifying agent(s) who do not complete the initial or ongoing privacy training
- process for ensuring that completion of initial or ongoing privacy training takes place within the identified timeframe, and
- consequences for agents failing to complete the required privacy training within the identified timeframe, which must include the PP or PE's refusal or withdrawal of an agent's permission to access PHI.

Other Mechanisms to Foster a Privacy Culture

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

- other mechanisms implemented by the PP or PE to foster a culture of privacy and to raise awareness of the privacy program and the privacy policies, procedures, and practices implemented
- frequency with which the PP or PE communicates with its agents in relation to privacy
- method and nature of the communication, and
- agent(s) responsible for the communication.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

Relationship to Policy, Procedures, and Practices for Information Security Training and Awareness

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

2. Log of Completion of Initial and Ongoing Privacy Training

A PP or PE must maintain a log of the completion of the initial and ongoing privacy training by agents. At a minimum, the log must set out the:

- name of each agent
- date that the agent commenced his or her employment, contractual, or other relationship with the PP or PE
- date that the agent completed the initial privacy training, and
- each date that the agent completed ongoing privacy training.

Information Security Training and Awareness

3. Policy, Procedures, and Practices for Information Security Training and Awareness

A policy, procedures, and practices must be developed and implemented requiring agents of the PP or PE to complete initial information security training as well as ongoing information security training.

Timing and Method of Initial and Ongoing Information Security Training

The policy, procedures, and practices must set out the timeframe within which agents must complete the initial information security training as well as address the frequency of ongoing information security training. At a minimum, the policy, procedures, and practices must:

- require agent(s) to complete the initial information security training prior to being given access to PHI
- require agent(s) to complete ongoing information security training provided by the PP or PE on an annual basis thereafter, and
- specify the method(s) by which the initial and ongoing information security training will be provided.

Process for Preparing and Delivering Information Security Training

The policy, procedures, and practices must:

- identify the agent(s) responsible for preparing the content and ensuring the delivery of the initial and ongoing information security training
- require the content of the initial and ongoing information security training to be reviewed and updated on a regular basis

- set out the frequency with which the training will be reviewed
- identify the agents(s) responsible for reviewing and updating the training
- require the initial training to be reviewed on an annual basis, and updated as needed
- set out a process that must be followed in notifying the agent(s) responsible for ensuring the delivery of the initial information security training when an agent has commenced or will commence an employment, contractual, or other relationship with the PP or PE
- identify the agent(s) responsible for providing such notification
- specify the timeframe within which notification must be provided, and
- set out the format of the notification.

Initial Information Security Training

The policy, procedures, and practices must also require the content of the initial information security training to be formalized and standardized, and be based on evolving industry information security standards and best practices. At a minimum, the policy, procedures, and practices must require that the initial information security training include:

- an overview of the information security policies, procedures, and practices that have been implemented by the PP or PE and the obligations arising from these policies, procedures, and practices
- the consequences of breach of PHIPA or its regulations or breach of the information security policies, procedures, and practices implemented
- an explanation of the information security program, including the key activities of the program and the agent(s) who have been delegated day-to-day authority to manage the information security program
- the administrative, technical, and physical safeguards implemented by the PP or PE to protect PHI against theft, loss, and unauthorized collection, use, or disclosure and to protect records of PHI against unauthorized copying, modification, or disposal
- the duties and responsibilities of agents in implementing the administrative, technical, and physical safeguards put in place by the PP or PE
- an explanation of the ***Policy, Procedures, and Practices for Information Security Breach Management*** and the related duties and responsibilities imposed on agents in identifying, reporting, containing, and participating in the investigation and remediation of information security breaches, including the duty to provide notification to the PP or the PE at the first reasonable opportunity of an information security breach or information security incident, and
- an explanation of the mandatory nature of information security training, including the prohibition on all agents to handle PHI without having completed initial information security training, and the mandatory nature of ongoing information security training on an annual basis thereafter.

Ongoing Information Security Training

The policy, procedures, and practices must also require the content of the ongoing information security training to be formalized and standardized, and be based on evolving industry information security standards and best practices. At a minimum, the policy, procedures, and practices must require that ongoing information security training:

- include role-based training in order to ensure that agents understand how to apply the information security policies, procedures, and practices in their day-to-day employment, contractual, or other responsibilities, as these may have evolved since their last training
- address any new information security policies, procedures, and practices and significant amendments to existing information security policies, procedures, and practices, and
- incorporate any relevant changes since their last training, including:
    - recommendations made with respect to:
        - information security training made in privacy impact assessments
        - the investigation of information security breaches
        - the conduct of information security audits including threat and risk assessments, security reviews or assessments, vulnerability assessments, penetration testing or ethical hacks, and
        - the audits of privacy and information security events
    - orders, decisions, guidelines, fact sheets, and best practices issued by the IPC under PHIPA and its regulations, and
    - amendments to PHIPA and its regulations relevant to the PP or PE.

Tracking, Auditing, and Monitoring Information Security Training

The policy, procedures, and practices must require that a log be maintained to track attendance and completion of the initial and ongoing information security training and identify the following:

- agent(s) responsible for maintaining such a log
- process to be followed in tracking completion of the initial and ongoing information security training
- documentation that must be completed, provided, and/or executed to verify completion
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom this documentation must be provided, and required content of the documentation
- where documentation related to the completion of the initial and ongoing information security training will be retained, and
- agent(s) responsible for retaining this documentation.

The policy, procedures, and practices must also:

- identify the agent(s) responsible for identifying agent(s) who do not complete the initial or ongoing information security training
- set out a process for ensuring that completion of initial and ongoing information security training take place within an identified timeframe, and
- set out the consequences for agents failing to complete the required information security training within the identified timeframe, which must include the PP or PE's refusal or withdrawal of agent's permission to access PHI.

Other Mechanisms to Raise Information Security Awareness

The policy, procedures, and practices must also address:

- other mechanisms implemented by the PP or PE to raise awareness of the information security program and the information security policies, procedures, and practices implemented
- the frequency with which the PP or PE communicates with its agents in relation to information security
- the method and nature of the communication, and
- the agent(s) responsible for the communication.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

Relationship to Policy, Procedures, and Practices for Privacy Training and Awareness

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

4. Log of Completion of Initial and Ongoing Information Security Training

A PP or PE must maintain a log of the completion of the initial and ongoing information security training by agents. At a minimum, the log must set out the:

- name of the agent
- date that the agent commenced his or her employment, contractual or other relationship with the PP or PE
- dates that the agent completed the initial information security training, and
- each date the agent completed ongoing information security training.

Confidentiality Agreements

5. Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Agents

A policy, procedures, and practices must be developed and implemented requiring agents to execute a Confidentiality Agreement that contains the requirements set out in the ***Template Confidentiality Agreement with Agents***.

Timing of Confidentiality Agreements

The policy, procedures, and practices must set out the timeframe within which agents must execute the **Confidentiality Agreement**. At a minimum, the policy, procedures, and practices must:

- require agents to execute a Confidentiality Agreement prior to being given access to PHI, including PHI that has been de-identified and/or aggregated, and on an annual basis thereafter, and
- identify the timeframe each year within which agents are required to execute the Confidentiality Agreement on an ongoing basis.

Process for Executing Confidentiality Agreements

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

- agent(s) responsible for ensuring that each agent executes a **Confidentiality Agreement** in compliance with the policy, procedures, and practices of the PP or PE
- process for notifying the responsible agent(s) each time an agent has commenced or will commence an employment, contractual, or other relationship with the PP or PE
- agent(s) responsible for providing such notification
- timeframe within which such notification must be provided, and
- format of the notification.

Tracking Execution of Confidentiality Agreements

The policy, procedures, and practices must:

- require that a log of executed **Confidentiality Agreements** be maintained
- identify the agent(s) responsible for maintaining the log and for tracking and ensuring that the Confidentiality Agreements have been executed, and
- outline the process that must be followed by the responsible agent(s) in tracking and ensuring the execution of Confidentiality Agreements, including the process that must be followed:
    - where an agent's executed Confidentiality Agreement is not received within a defined period of time following the commencement of the employment, contractual, or other relationship, or
    - within a defined period of time following the date that the Confidentiality Agreement is required to be executed on an annual basis.

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

- the documentation that must be completed, provided, and/or executed to verify that Confidentiality Agreements have been executed
- the agent(s) responsible for completing, providing, executing, and ensuring the execution of the documentation;
- the agent(s) to whom this documentation must be provided
- the required content of the documentation
- where documentation related to the Confidentiality Agreements will be retained, and
- the agent(s) responsible for retaining this documentation.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

6. Template Confidentiality Agreement with Agents

A **Confidentiality Agreement** must be executed by each agent of the PP or PE in accordance with the ***Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Agents*** that, at a minimum, addresses the matters set out below.

General Provisions

The **Confidentiality Agreement** must:

- describe the status of the PP or PE under PHIPA and the duties and responsibilities arising from this status
- state that individuals executing the agreement are agents of the PP or PE in respect of PHI and must outline the responsibilities associated with this status
- provide definitions of the terms "personal health information," "de-identified information," and "aggregate information," where the definitions provided for:
    - "personal health information" must be consistent with PHIPA and its regulations, and
    - "de-identified information" and "aggregate information" must be consistent with those definitions provided in the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation***.

Required Compliance

The **Confidentiality Agreement** must require agents to:

- comply with the:
    - provisions of PHIPA and its regulations relating to the role of the PPs or PEs, as the case may be, and
    - terms of the Confidentiality Agreement as may be amended from time to time, and
- acknowledge that they have read, understood, and agree to comply with:
    - the privacy and information security policies, procedures, and practices implemented by the PP or PE, and
    - any privacy and information security policies, procedures, and practices as may be implemented or amended from time to time following the execution of the Confidentiality Agreement.

Obligations with Respect to Collection, Use, and Disclosure of Personal Health Information

The **Confidentiality Agreement** must:

- identify the purposes for which agents are permitted to collect, use, and disclose PHI on behalf of the PP or PE and any limitations, conditions, or restrictions imposed thereon; in identifying the purposes for which agents are permitted to collect, use, or disclose

PHI, the PP or PE must ensure that each collection, use, or disclosure identified in the Confidentiality Agreement is permitted by:

  - PHIPA and its regulations, and
  - the policies, procedures, and practices put in place pursuant thereto

- prohibit agents from collecting, using, or disclosing PHI except as permitted in the Confidentiality Agreement or as required by law, and
- prohibit agents from collecting, using, or disclosing PHI if other information will serve the purpose and from collecting, using, or disclosing more PHI than is reasonably necessary to meet the purpose.

Obligations with Respect to De-Identified and Aggregate Information

The **Confidentiality Agreement** must:

- identify the purposes for which agents are permitted to use and disclose PHI which has been **de-identified or aggregated**, as the case may be, and
- prohibit agents from using the de-identified or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is done in accordance with the ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation*** and is permitted by PHIPA or another law; this must include prohibiting:
  - any attempt to decrypt information that is encrypted, or
  - identification of an individual based on unencrypted information and/or prior knowledge.

Termination of the Contractual, Employment, or Other Relationship

The **Confidentiality Agreement** must:

- require agents to securely return all property of the PP or PE, including records of PHI and all identification cards, access cards, and/or keys, on or before the date of termination of the employment, contractual, or other relationship in accordance with the ***Policy, Procedures, and Practices upon Termination or Cessation of the Employment or Contractual Relationship***, and
- stipulate the:
  - timeframe within which the property of the PP or PE must be securely returned
  - secure manner in which the property must be returned, and
  - agent to whom the property must be securely returned.

Breach Notification to PP or PE

At a minimum, the Confidentiality Agreement must require agents to notify the PP or PE at the first reasonable opportunity and in accordance with the ***Policy, Procedures, and Practices for***

Privacy Breach Management and/or the ***Policy, Procedures, and Practices for Information Security Breach Management***, if the agent breaches or believes that there may have been a breach of the Confidentiality Agreement or if the agent breaches or believes that there may have been a breach of the privacy or information security policies, procedures, and practices implemented by the PP or PE.

Consequences of Breach and Monitoring Compliance

The **Confidentiality Agreement** must:

- outline the consequences of breach of the agreement and must address the manner in which compliance with the Confidentiality Agreement will be enforced, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance with the Confidentiality Agreement will be audited, and
- address the manner in which compliance will be audited.

7. Log of Executed Confidentiality Agreements with Agents

A PP or PE must maintain a log of **Confidentiality Agreements** that have been executed by agents at the commencement of their employment, contractual, or other relationship with the PP or PE and on an annual basis. At a minimum, the log must include the:

- name of the agent
- date of commencement of the employment, contractual, or other relationship with the PP or PE, and
- dates that the Confidentiality Agreement(s) were executed.

Privacy and Information Security Leadership

8. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program

A job description for the position(s) that have been delegated day-to-day authority to manage the privacy program on behalf of the PP or PE must be developed. The job description must:

- set out the reporting relationship of this position(s) to the chief executive officer or the executive director (or equivalent position), as the case may be, and
- identify the responsibilities and obligations of the position(s) in respect of the privacy program; at a minimum, these responsibilities and obligations must include:
    - developing, implementing, reviewing, and amending privacy policies, procedures, and practices
    - ensuring compliance with the privacy policies, procedures, and practices implemented

- ensuring transparency of the privacy policies, procedures, and practices implemented
- facilitating compliance with PHIPA and its regulations
- ensuring agents are aware of PHIPA and its regulations and their duties thereunder
- ensuring agents are aware of the privacy policies, procedures, and practices implemented by the PP or PE and are appropriately informed of their duties and obligations thereunder
- directing, delivering, or ensuring the delivery of the initial and ongoing privacy training and fostering a culture of privacy
- conducting, reviewing, and approving privacy impact assessments in accordance with the ***Policy, Procedures, and Practices for Privacy Impact Assessments***
- receiving, documenting, tracking, investigating, remediating, and responding to privacy complaints pursuant to the ***Policy, Procedures, and Practices for Privacy Complaints***
- receiving and responding to privacy inquiries pursuant to the ***Policy, Procedures, and Practices for Privacy Inquiries***
- receiving, documenting, tracking, investigating, and remediating privacy breaches or suspected privacy breaches pursuant to the ***Policy, Procedures, and Practices for Privacy Breach Management***, and
- conducting privacy audits pursuant to the ***Policy, Procedures, and Practices in Respect of Privacy Audits***.

9. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Information Security Program

A job description for the position(s) that have been delegated day-to-day authority to manage the information security program on behalf of the PP or PE must be developed. The job description must:

- set out the reporting relationship of this position(s) to the chief executive officer or the executive director (or equivalent position), as the case may be, and
- identify the responsibilities and obligations of the position(s) in respect of the information security program; at a minimum, these responsibilities and obligations must include:
  - developing, implementing, reviewing, and amending information security policies, procedures, and practices
  - ensuring compliance with the information security policies, procedures, and practices implemented

- ensuring agents are aware of the information security policies, procedures, and practices implemented by the PP or PE and are appropriately informed of their duties and obligations thereunder
- directing, delivering, or ensuring the delivery of the initial and ongoing information security training and fostering a culture of information security awareness
- logging, monitoring, and auditing of privacy and information security events pursuant to the ***Policy, Procedures, and Practices for Logging, Monitoring, and Auditing Privacy and Information Security Events***
- receiving, documenting, tracking, investigating, and remediating information security breaches or information security incidents pursuant to the ***Policy, Procedures, and Practices for Information Security Breach Management***, and
- conducting information security audits pursuant to the ***Policy, Procedures, and Practices in Respect of Information Security Audits***.

Termination or Cessation

10. Policy, Procedures, and Practices upon Termination or Cessation of the Employment or Contractual Relationship

The policy, procedures, and practices must:

- require agents, as well as their supervisors, to notify the PP or PE of the termination or cessation of the employment, contractual, or other relationship, and
- identify the:
  - agent(s) to whom notification must be provided
  - nature and format of the notification
  - timeframe within which notification must be provided, and
  - process that must be followed in providing notification.

Secure Return of All Property

The policy, procedures, and practices must also require agents to securely return all property of the PP or PE on or before the date of termination or cessation of the employment, contractual, or other relationship. In this regard, a definition of property must be provided in the policy, procedures, and practices and this definition must, at a minimum, include records of PHI, computing equipment, mobile devices, identification cards, access cards, and/or keys.

The policy, procedures, and practices must identify the:

- agent(s) to whom the property must be securely returned
- secure method by which the property must be returned

- timeframe within which the property must be securely returned
- documentation that must be completed, provided, and/or executed
- agent(s) responsible for completing, providing, and/or executing the documentation
- required content of the documentation
- procedure to be followed in the event that the property of the PP or PE is not securely returned upon termination or cessation of the employment, contractual, or other relationship, and
- agent(s) responsible for implementing the procedure and the timeframe following termination or cessation within which the procedure must be implemented.

Terminating Access to Premises and Information Environment

The policy, procedures, and practices must also:

- require that access to the premises of the PP or PE, to locations within the premises where records of PHI are retained, and to components within the information environment, be immediately terminated upon the termination or cessation of the employment, contractual, or other relationship, and
- identify the:
    - agent(s) responsible for terminating access
    - procedure to be followed in terminating access
    - timeframe within which access must be terminated
    - documentation that must be completed, provided, and/or executed, and
    - agent(s) responsible for completing, providing, and/or executing the documentation.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

Discipline and Corrective Action

11. Policy, Procedures, and Practices for Discipline and Corrective Action

The PP or PE must develop and implement a policy, procedures, and practices for discipline and corrective action for breaches of agents' obligations and responsibilities in respect of protecting the privacy of individuals whose PHI the PP or PE receives and maintaining the confidentiality of that information.

The policy, procedures, and practices must address:

- the investigation of disciplinary matters, including the person(s) responsible for conducting the investigation
- the procedure that must be followed in undertaking the investigation
- any 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 required content of the documentation, and
- the agent(s) to whom the results of the investigation must be reported.

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

- types of discipline that may be imposed by the PP or PE on its agent(s)
- factors that must be considered in determining the appropriate discipline and corrective action to be taken
- agent(s) responsible for determining the appropriate discipline and corrective action
- procedure to be followed in making this determination
- agent(s) who must be consulted in making this determination, and
- documentation that must be completed, provided, and/or executed.

The policy, procedures, and practices should also address the retention of documentation related to the discipline and corrective action taken, including:

- where this documentation will be retained, and
- the agent(s) responsible for retaining the documentation.

Part 4 – Organizational Policies, Procedures, and Practices

Governance and Accountability

1. Privacy Governance and Accountability Framework

A privacy governance and accountability framework must be established for ensuring compliance with:

- PHIPA and its regulations, and
- the privacy policies, procedures, and practices implemented by the PP or PE.

The privacy governance and accountability framework must stipulate that the chief executive officer or the executive director (or equivalent position), as the case may be, is ultimately accountable for ensuring that the PP or PE and its agents comply with:

- PHIPA and its regulations, and
- the privacy policies, procedures, and practices implemented by the PP or PE.

The privacy governance and accountability framework must:

- identify the position(s) that have been delegated day-to-day authority to manage the privacy program
- describe the nature of the reporting relationship to the chief executive officer or the executive director (or equivalent position)
- set out the responsibilities and obligations of the position(s) that have been delegated day-to-day authority to manage the privacy program
- identify the other individuals, committees, and teams that have been delegated supporting roles to manage the privacy program
- describe the role(s) of the individuals, committees, and teams in respect of the privacy program
- specify the method and manner by which the privacy governance and accountability framework will be communicated to agents of the PP or PE, and
- identify the agent(s) responsible for this communication.

The privacy governance and accountability framework should be accompanied by a privacy governance organizational chart.

Board of Directors

The privacy governance and accountability framework must also:

- describe the role of the board of directors in respect of the privacy program, including any committee of the board of directors to which privacy oversight has been delegated

- address the frequency with which the board of directors is updated with respect to the privacy program which, at a minimum, should be annually, and preferably in the form of a written report
- identify the agent(s) responsible for providing such updates
- set out the method and manner by which the board of directors is required to be updated, and
- identify the type of matters with respect to which the board of directors is required to be updated.

The update provided to the board of directors must, at a minimum, address risks that may negatively affect the PP's or PE's ability to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information that has been ranked as being high risk on the corporate risk register. Such matters should include:

- major financial investments required to ensure a robust and sustainable privacy governance and accountability framework
- the development, implementation, and evaluation of major information technology transformation projects and high-risk information processing applications with privacy implications, such as artificial intelligence
- relevant initiatives undertaken by the privacy program including privacy training
- the development and implementation of new privacy-related policies, procedures, and practices, including those that are of major, corporate-wide significance and have implications for the Board, its members and the proper functioning of its committees
- the findings, mitigations, and any other relevant recommendations arising from privacy audits and privacy impact assessments, including the status of implementation of the mitigations and any other relevant recommendations
- privacy breaches, suspected privacy breaches, and privacy complaints that were investigated, as applicable, including the findings, mitigations, and any other relevant recommendations arising from these investigations and the status of implementation of the mitigations / recommendations
- major privacy related litigation matters, including privacy class-action lawsuits facing the PP or PE
- privacy related issues that have been identified through whistleblowers, and
- major changes to the privacy governance and accountability framework, including changes of personnel in high-level position(s) that have been delegated day-to-day authority to manage the privacy program and related reporting relationships.

The privacy governance and accountability framework must set out whether, and the circumstances in which, the above information is provided to the board of directors, including the level of detail in which the information is provided.

Relationship to Information Security Governance and Accountability Framework

This governance and accountability framework may either be a stand-alone document or may be combined with the ***Information Security Governance and Accountability Framework***.

2. Information Security Governance and Accountability Framework

An information security governance and accountability framework for ensuring compliance with PHIPA and its regulations and for ensuring compliance with the information security policies, procedures, and practices implemented by the PP or PE must be established.

The information security governance and accountability framework must stipulate that the chief executive officer or the executive director (or equivalent position), as the case may be, is ultimately accountable for ensuring the:

- security of PHI, and
- PP or PE and its agent(s) comply with the information security policies, procedures, and practices implemented.

The information security governance and accountability framework must also:

- identify the position(s) that have been delegated day-to-day authority to manage the information security program
- describe the nature of the reporting relationship to the chief executive officer or the executive director (or equivalent position)
- set out the responsibilities and obligations of the position(s) that have been delegated day-to-day authority to manage the information security program
- identify the other individuals, committees, and teams that have been delegated supporting roles in respect of the information security program
- set out the method and manner by which the information security governance and accountability framework will be communicated to agents of the PP or PE, and
- identify the agent(s) responsible for this communication.

The information security governance and accountability framework should be accompanied by an information security governance organizational chart.

Board of Directors

The information security governance and accountability framework must also address the:

- role of the board of directors in respect of the information security program, including any committee of the board of directors to which information security oversight has been delegated
- frequency with which the board of directors is updated with respect to the information security program which, at a minimum, should be annually and preferably in the form of a written report

- matters on which the board of directors must be updated
- method and manner by which the board of directors is updated, and
- agent(s) responsible for providing such updates.

The update provided to the board of directors must, at a minimum, address risks that may negatively affect the PP's or PE's ability to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information that have been ranked as being high risk on the corporate risk register. Such matters should include:

- regular updates on the level of cybersecurity risks facing the PP or PE, and the measures that have been put in place to mitigate them
- major financial and other investments required to ensure a robust and sustainable information security governance and accountability framework
- the development, implementation, and evaluation of major information technology transformation projects and high-risk information processing applications with information security implications, such as artificial intelligence
- relevant initiatives undertaken by the information security program including information security training
- the development and implementation of new information security-related policies, procedures, and practices, including those that are of major, corporate-wide significance and have implications for the Board, its members and the proper functioning of its committees
- the findings and associated recommendations arising from information security audits, such as threat and risk assessments, including the status of implementation of the mitigations and any other relevant recommendations
- information security breaches that were investigated, as applicable, including the findings, mitigations, and other relevant recommendations arising from these investigations and the status of implementation of the mitigations / recommendations
- major information security-related litigation matters, including information security class-action lawsuits facing the PP or PE
- information security related issues that have been identified through whistle-blowers, and
- major changes to the information security governance and accountability framework, including changes of personnel in high-level position(s) that have been delegated day-to-day authority to manage the information security program and related reporting relationships.

The information security governance and accountability framework must set out whether, and the circumstances in which, the above information is provided to the board of directors, including the level of detail in which the information is provided.

Relationship to Privacy Governance and Accountability Framework

This governance and accountability framework may either be a stand-alone document or may be combined with the ***Privacy Governance and Accountability Framework***.

3. Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Information Security Program

The PP or PE must establish terms of reference for each committee that has a role in respect of the privacy and/or the information security program. For each committee, the terms of reference must identify the:

- membership of the committee
- chair of the committee
- mandate and responsibilities of the committee in respect of the privacy and/or the information security program
- duration of the committee, and
- frequency with which the committee meets.

The terms of reference must also set out:

- to whom the committee reports
- the types of reports produced by the committee, if any
- the format of the reports
- to whom these reports are presented, and
- the frequency of these reports.

Risk Management

4. Corporate Risk Management Framework

A PP or PE must develop and implement a comprehensive and integrated corporate risk management framework to:

- identify, assess, rank, mitigate, and monitor risks, including risks that may negatively affect its ability to protect the privacy of individuals whose PHI is received, and
- maintain the confidentiality of that information.

Risk Identification, Assessment, and Ranking

The corporate risk management framework must address the:

- agent(s) responsible, and
- process that must be followed and criteria that must be considered in identifying privacy and information security-related risks, and ranking them in terms of their likelihood of occurrence and their potential impact, which must include a discussion of the:

- agents or other persons or organizations that must be consulted in identifying, assessing, and ranking the risks
- documentation that must be completed, provided, and/or executed
- agent(s) responsible for completing, providing, and/or executing the documentation
- required content of the documentation, including a description of the rationale underlying the assessment and ranking of risks, and
- agent(s) to whom this documentation must be provided.

Risk Mitigation

The corporate risk management framework must identify the:

- agent(s) responsible
- process that must be followed, and
- criteria that must be considered in identifying strategies to mitigate the privacy and information security-related risks that were identified, assessed, and ranked.

The framework must include a process for implementing the mitigation strategies and evaluating the residual risks likely to remain after the mitigation strategies have been implemented. The framework must further identify the:

- agents or other persons or organizations that must be consulted in identifying and implementing the mitigation strategies
- agent(s) responsible for:
  - assigning other agent(s) to address the mitigations and any other recommendations as required
  - establishing timelines to address the mitigations and any other recommendations
  - monitoring and ensuring the treatment of the mitigations and any other relevant recommendations within stated timelines, and
  - evaluating the residual risks remaining after implementation
- documentation that must be completed, provided, and/or executed
- agent(s) responsible for completing, providing, and/or executing the documentation
- required content of the documentation, including a description of the rationale underlying the strategies to mitigate risks and evaluating residual risks, and
- agent(s) to whom this documentation must be provided.

Approval

The corporate risk management framework must set a process for approving and endorsing the results of the risk management process, which includes the identification, assessment, and

ranking of risks, the identification, implementation, and monitoring of mitigation strategies, and the evaluation of residual risks.

The framework must also:

- identify the agent(s) responsible for determining whether to approve and endorse or not to approve and endorse the results of the risk management process
- address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve and endorse, or to not approve and endorse, the results of the risk management process, and
- set out the manner of documenting the:
    - decision to approve and endorse, or to not approve and endorse
    - results of the risk management process and the reasons for the decision, and
    - agent(s) responsible for completing this documentation.

Risk Communication and Reporting

The corporate risk management framework must:

- address the manner, circumstances, and format in which the results of the corporate risk management processes are communicated and reported, which involves identifying:
    - the agent(s) responsible for communicating and reporting the results of the corporate risk management process, the nature, format, and content of the communication, including the level of detail, and
    - to whom the results of the corporate risk management process will be communicated and reported to, including whether the results must be communicated to the chief executive officer or the executive director (or equivalent position), and
- outline the process that must be followed for the approval and endorsement of the results of the risk management process, including the agent(s) responsible for approval and endorsement.

Risk Register

Further, the corporate risk management framework must:

- require that the corporate risk register be maintained and reviewed on an ongoing basis, and at a minimum on an annual basis, in order to ensure that all relevant privacy and information security-related risks continue to be identified, assessed, ranked, and mitigated
- identify the frequency with which the corporate risk register must be reviewed
- specify the agent(s) responsible for the review, and

- identify the process that must be followed in reviewing and amending the corporate risk register.

Integration of Risk Management Framework

The corporate risk management framework of the PP or PE must:

- ensure that the risks identified in the corporate risk management framework are addressed in the policies, procedures, and practices of the PP or PE and in the projects undertaken by the PP or PE, and
- identify the agent(s) responsible for ensuring that the risks are addressed.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

5. Corporate Risk Register

A PP or PE must develop and maintain a corporate risk register that:

- identifies and integrates privacy and information security-related risks, among other enterprise-wide risks, that may negatively affect the ability of the PP or PE to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information, and
- for each privacy and information security-related risk identified, the corporate risk register must include:
    - an assessment of the risk
    - a ranking of the risk
    - the mitigation strategy that has been identified to reduce the risk, including the:

- date that the mitigation strategy was implemented or is required to be implemented
- agent(s) responsible for implementation of the mitigation strategy, and
- residual risk likely to remain despite implementation of the mitigation strategy.

6. Policy, Procedures, and Practices for Maintaining a Consolidated Log of Recommendations

A PP or PE must at a minimum, develop and implement a policy, procedures, and practices that:

- requires a consolidated and centralized log of all findings, mitigations, and other recommendations arising from privacy impact assessments, privacy audits, information security audits, and the investigation of privacy breaches, privacy complaints, and/or information security breaches
- requires the inclusion of recommendations, orders and decisions made by the IPC under PHIPA and its regulations, and
- sets out the:
    - frequency with which and the circumstances in which the consolidated and centralized log must be reviewed
    - agent(s) responsible for reviewing and amending the log, and
    - process that must be followed.

At a minimum, the log should be updated each time that:

- a privacy impact assessment, privacy audit, information security audit, investigation of a privacy breach, investigation of a privacy complaint, investigation of an information security breach, or review by the IPC is completed, and
- one or more recommendations, orders, or decisions, including those issued by the IPC under PHIPA and its regulations, have been addressed.

The consolidated and centralized log should be reviewed on an ongoing basis in order to ensure that the mitigations/recommendations, orders, and decisions, including those issued by the IPC under PHIPA and its regulations, are addressed in a timely manner.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require agents to comply with the policy, procedures, and practices
- require agents to notify the PP or PE at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management*** and/or the ***Policy, Procedures, and Practices for Information Security Breach Management***, as the case may be, if an agent breaches or believes there may have been breach of this policy, procedures, or practices

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

7. Consolidated Log of Recommendations

The consolidated log of recommendations of a PP or PE must, at a minimum, be developed and maintained to:

- include a consolidated and centralized log of all findings, mitigations, and other recommendations arising from privacy impact assessments, privacy audits, information security audits, the investigation of privacy breaches, the investigation of privacy complaints, and/or the investigation of information security breaches
- include recommendations, orders, and decisions made by the IPC
- set out the:
    - name and date of the document, investigation, audit, and/or
    - review from which the findings, mitigations, and other recommendations, orders, or decisions, including those issued by the IPC under PHIPA and its regulations, arose; for each finding, mitigation, and other recommendations, orders, or decisions, the log must set out the:
        - finding, recommendation, order, or decision made
        - manner in which the recommendation, order, or decision was addressed or is proposed to be addressed
        - date that the mitigation/recommendation, order, or decision was addressed or by which it is required to be addressed, and
        - agent(s) responsible for addressing the recommendation, order, or decision.

Business Continuity and Disaster Recovery

8. Business Continuity and Disaster Recovery Plan

A policy, procedures, and practices must be developed and implemented to protect and ensure the continued availability of the information environment of the PP or PE in the event of:

- short and long-term business interruptions, and
- threats to the operating capabilities of the PP or PE, including natural, human, environmental, and technical interruptions, and threats.

The business continuity and disaster recovery plan must also address the:

- notification of the interruption or threat
- documentation of the interruption or threat
- assessment of the severity of the interruption or threat
- activation of the business continuity and disaster recovery plan, and
- recovery of PHI.

Notification of Interruption or Threat

In relation to notification of the interruption or threat, the business continuity and disaster recovery plan must identify the:

- agent(s) as well as the other persons or organizations that must be notified of short and long-term business interruptions and threats to the operating capabilities of the PP or PE
- agent(s) responsible for providing such notification
- timeframe within which notification must be provided
- manner and format of notification
- nature of the information that must be provided upon notification
- process for developing and maintaining an updated contact list of all agents, service providers, stakeholders, and other persons or organizations that must be notified
- agent(s) responsible for creating and maintaining this contact list, and
- documentation that must be completed, provided, and/or executed.

Severity Assessment

In relation to the assessment of the severity level of the interruption or threat, the business continuity and disaster recovery plan must identify:

- the agent(s) responsible for the assessment
- the criteria pursuant to which this assessment is to be made
- the agents and other persons or organizations that must be consulted in assessing the severity level of the interruption or threat
- the documentation that must be completed, provided, and/or executed resulting from or arising out of this assessment, including the required content of the documentation
- the agent(s) to whom the documentation must be provided, and
- to whom the results of this assessment must be reported.

Initial Impact Assessment

In relation to the assessment of the interruption or threat, the business continuity and disaster recovery plan must set out:

- the agent(s) responsible for the business continuity and disaster recovery plan, and
- the process that must be followed in conducting an initial impact assessment of the interruption or threat, including its impact on the technical and physical infrastructure and business processes of the PP or PE.

In outlining the initial impact assessment process to be followed, the business continuity and disaster recovery plan must identify the:

- agent(s) and other person(s) or organization(s) that are required to be consulted in undertaking the assessment
- requirements that must be satisfied and the criteria that must be utilized in conducting the assessment
- documentation that must be completed, provided, and/or executed
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom the documentation must be provided, and
- agent(s) to whom the results of the initial impact assessment must be communicated.

Damage Assessment

The business continuity and disaster recovery plan must further identify the:

- agent(s) responsible for conducting and preparing a detailed damage assessment in order to evaluate the extent of the damage caused by the threat or interruption and the expected effort required to resume, recover, and restore components within the information environment
- manner in which the assessment is required to be conducted
- agent(s) and other persons or organizations that are required to be consulted in undertaking the assessment
- requirements that must be satisfied and the criteria that must be considered in undertaking the assessment
- documentation that must be completed, provided, and/or executed
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom the documentation must be provided, and
- agent(s) to whom the results of the assessment must be communicated.

Resumption and Recovery Following the Interruption or Threat

The business continuity and disaster recovery plan must also identify the:

- agent(s) responsible for resumption and recovery
- procedure that must be utilized in resumption and recovery for each critical application and business function

- prioritization of resumption and recovery activities
- criteria pursuant to which the prioritization of resumption and recovery activities is determined
- recovery time objectives for critical applications
- agents and other persons or organizations that are required to be consulted with respect to resumption and recovery activities
- documentation that must be completed, provided, and/or executed
- required content of the documentation
- agent(s) responsible for completing, providing, and/or executing the documentation
- agent(s) to whom the documentation must be provided, and
- agent(s) to whom the results of these activities must be communicated.

Documenting Business Interruptions and Threats

The policy, procedures, and practices must detail:

- how decisions made and actions taken during business interruptions and threats to the operating capabilities of the PP or PE will be documented and communicated
- the agent(s) responsible, and
- by whom and to whom the business interruptions and threats to the operating capabilities will be communicated.

Inventory of Critical Applications, Business Functions, Hardware, and Software

The business continuity and disaster recovery plan must require that an inventory be developed and maintained of all critical applications and business functions and of all hardware and software, software licences, recovery media, equipment, system network diagrams, hardware configurations, software configuration settings, configuration settings for database systems and configuration settings for methods to detect unauthorized connections and devices, routers, domain name servers, email servers, and the like. The business continuity and disaster recovery plan must further identify the:

- agent(s) responsible for developing and maintaining the inventory
- agent(s) and other person(s) and organization(s) that must be consulted in developing the inventory, and
- criteria upon which the determination of critical applications and business functions must be made.

Testing, Maintenance, and Assessment of Business Continuity and Disaster Recovery Plan

The business continuity and disaster recovery plan must also address the testing, maintenance, and assessment of the business continuity and disaster recovery plan. This includes identifying the:

- frequency of testing, which at a minimum must be done on an annual basis
- agent(s) responsible for ensuring that the business continuity and disaster recovery plan is tested, maintained, and assessed
- agent(s) responsible for amending the business continuity and disaster recovery plan as a result of the testing
- procedure to be followed in testing, maintaining, assessing, and amending the business continuity and disaster recovery plan, and
- agent(s) responsible for approving the business continuity and disaster recovery plan and any amendments thereto.

Communication of Business Continuity and Disaster Recovery Plan

The business continuity and disaster recovery plan must identify:

- the agent(s) responsible and the procedure to be followed in communicating the business continuity and disaster recovery plan to all agents, including:
    - any amendments thereto, and
    - the method and nature of the communication, and
- the agent(s) responsible for managing communications in relation to the threat or interruption, including the method and nature of the communication.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

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

Part 1 – Privacy Indicators

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

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

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

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

Categories	Privacy Indicators
Privacy Breaches (Cont'd)	- whether an unauthorized person who is not an agent or electronic service provider caused the privacy breach or suspected privacy breach and the name or a description of the unauthorized person, if applicable - the containment measures implemented - the date(s) that the containment measures were implemented - the date(s) that notification was provided to the custodians or any other organizations - the date that the investigation was commenced - the date that the investigation was completed - a brief description of each finding, mitigation, and any other recommendation made - the date that the chief executive officer or executive director (or equivalent position) and senior management was notified of the findings, mitigations, and other recommendations arising from the investigation, if applicable - the date each recommendation was addressed or is expected to be addressed - the manner in which each recommendation was addressed or is expected to be addressed - the date notification was provided to the IPC, if applicable, and - the date that notification was provided to individuals, if applicable.

Categories	Privacy Indicators
Privacy Complaints and Inquiries	• The number of **privacy complaints** received since the prior review by the IPC. • Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the IPC, and with respect to each privacy complaint investigated: - the date that the privacy complaint was received - the nature of the privacy complaint - the date that the investigation was commenced - the date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation - the date that the investigation was completed - a brief description of each finding, mitigation, and any other recommendation made - the date the chief executive officer or executive director (or equivalent position) and senior management were notified of the findings, mitigations, and other recommendations arising from the investigation, if applicable - the date each recommendation was addressed or is expected to be addressed - the manner in which each recommendation was addressed or is expected to be addressed, 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 – Information Security Indicators

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

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

Categories	Information Security Indicators
Information Security Audit Program (Cont'd)	• The number and a list of information security audits completed since the prior review by the IPC, and for each audit: - a description of the nature and type of audit conducted - the date of completion of the audit - a brief description of each recommendation made - the date that each recommendation was addressed or is expected to be addressed, and - the manner in which each recommendation was addressed or is expected to be addressed.
Information Security Breaches	• The total number of notifications of **information security breaches** or information security incidents received by the PP or PE since the prior review by the IPC. This indicator may be further subdivided to distinguish between information security breaches that: - actually, or imminently jeopardize the confidentiality, integrity, or availability of information or the information environment - constitute a contravention or imminent threat of contravention of PHIPA or its regulations, or - constitute a contravention or imminent threat of contravention of the terms of any written agreements, other legal obligations, or information security policies, procedures, and practices implemented by the PP or PE, related to the requirements of the Manual. • With respect to each information security breach or information security incident: - the date of the information security breach or information security incident - the date that the information security breach or information security incident was identified or suspected - the nature of the PHI, if any, that was the subject matter of the information security breach and the nature and extent of the information security breach - a description of the information security breach or information security incident and who identified the information security breach or information security incident - the cause of the information security breach or information security incident - the date that chief executive officer or executive director (or equivalent position) and senior management were notified of the information security breach or information security incident, if applicable

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

Part 3 – Human Resources Indicators

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

Part 4 – Organizational Indicators

Categories	Organizational Indicators
Risk Management	• The dates that the corporate risk register was reviewed by the PP or PE 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: Sworn Affidavit

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

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

2. [INSERT NAME OF PRESCRIBED PERSON OR PRESCRIBED ENTITY] has in place policies, procedures, and practices to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information in accordance with its obligations under the *Personal Health Information Protection Act, 2004* and the regulations thereto, as may be amended from time to time.

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

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

   b. Statements of Inapplicability attached hereto as Exhibit B.

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

5. [INSERT NAME OF PRESCRIBED PERSON OR 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 health information it receives is protected against theft, loss, and unauthorized collection, use, or disclosure and to ensure that records containing personal health 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/Notary Public

Appendix E: Glossary

Term	Definition
Agent	Means a person that, with the authorization of the PP/PE, acts for or on behalf of the PP/PE in respect of PHI for the purposes of the PP/PE, and not the agent's own purposes, whether or not the agent has the authority to bind the PP/PE, whether or not the agent is employed by the PP/PE and whether or not the agent is being remunerated.
Certificate of destruction	A certificate that evidences the destruction of records of PHI that must, at a minimum: • identify the records of PHI securely disposed of • stipulate the date, time, location, and method of secure disposal employed, and • bear the name and signature of the person who performed the secure disposal. Certificates of destruction are referred to in the following policies, procedures, and practices: • ***Policy, Procedures, and Practices for the Use of Personal Health Information for Research*** • ***Log of Approved Uses of Personal Health Information for Research*** • ***Policy, Procedures, and Practices for Disclosure of Personal Health Information for Purposes Other Than Research*** • ***Policy, Procedures, and Practices for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements*** • ***Template Research Agreement*** • ***Log of Research Agreements*** • ***Template Data Sharing Agreement*** • ***Policy, Procedures, and Practices for Executing Agreements with Third-Party Service Providers in Respect of Personal Health Information*** • ***Log of Agreements with Third-Party Service Providers*** • ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information***

Term	Definition
Confidentiality Agreement	An agreement that is executed between a PP/PE and each of its agents in accordance with the ***Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Agents*** and the ***Template Confidentiality Agreement with Agents***. Confidentiality Agreements are referred to in the following policies, procedures, and practices: • ***Policy, Procedures, and Practices for Privacy Breach Management*** • ***Policy, Procedures, and Practices for Privacy Training and Awareness*** • ***Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Agents*** • ***Template Confidentiality Agreement with Agents*** • ***Log of Executed Confidentiality Agreements with Agents***
Data Sharing Agreement	An agreement that is executed between a PP/PE and another party in accordance with the ***Policy, Procedures, and Practices for the Execution of Data Sharing Agreements*** and the ***Template Data Sharing Agreement***. Data Sharing Agreements are referred to in the following policies, procedures, and practices: • ***Policy, Procedures, and Practices for Disclosure of Personal Health Information for Purposes Other Than Research*** • ***Policy, Procedures, and Practices for the Execution of Data Sharing Agreements*** • ***Template Data Sharing Agreement*** • ***Log of Data Sharing Agreements*** • ***Policy, Procedures, and Practices with Respect to De-Identification and Aggregation*** • ***Policy, Procedures, and Practices for Privacy Breach Management*** • ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information***
De-identified and/or aggregate information	In relation to the PHI of an individual, means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual, and “de-identification” has a corresponding meaning.

Term	Definition
Electronic service providers	An electronic service provider (ESP) is a person who supplies services that enable a custodian to collect, use, modify, disclose, retain, or dispose of personal health information electronically as set out in s.6 of the regulations to PHIPA. Electronic service providers are referred to in the following policies, procedures, and practices: • ***Template Agreement for Third-Party Service Providers*** • ***Policy, Procedures, and Practices for Privacy Breach Management*** • ***Log of Privacy Breaches*** • ***Policy, Procedures, and Practices for Information Security Breach Management*** • ***Log of Information Security Breaches***
FIPPA	*Freedom of Information and Protection of Privacy Act*.
Health information custodian/custodian	A "health information custodian" within the meaning of PHIPA and its regulations.
Identifying information	Includes information that identifies an individual or for which it is reasonably foreseeable that it could be used, either alone or with other information, to identify an individual.
Information environment	The networks, information systems, technologies, applications, software, servers, components, and configurations that enable the collection, use, and disclosure of PHI in the custody or control of a PP or PE, and work to keep the PHI secure.
Information security breach	An occurrence that, at a minimum: • actually, or imminently, jeopardizes the confidentiality, integrity, or availability of information or the information environment, or • constitutes a contravention or imminent threat of contravention of PHIPA or its regulations, the terms of any written agreements, other legal obligations, or information security policies, procedures, and practices implemented by the PP or PE.
Information security component	Any individual network, information system, technology, application, software, server, or configuration within the information environment.
IPC	The Information and Privacy Commissioner of Ontario.
Manual	The Manual for the Review and Approval of Prescribed Persons and Prescribed Entities (*this document*).
Must	Anytime the word "must" appears in the Manual, it indicates a requirement.

Term	Definition
Personal health information (PHI)	"Personal health information" within the meaning of PHIPA and its regulations.
PHI	Personal health information.
PHIPA	The *Personal Health Information Protection Act, 2004*.
PE/PEs	Prescribed entity / prescribed entities.
Personal information	Personal information within the meaning of FIPPA.
PP/PPs	Prescribed person / prescribed persons.
Prescribed entity	Entities prescribed for the purposes of subsection 45(1) of PHIPA and that are prescribed in subsection 18(1) of PHIPA's regulations.
Prescribed person	Persons prescribed for the purposes of clause 39(1)(c) of PHIPA and that are prescribed in subsection 13(1) of PHIPA's regulations.
Privacy breach	An occurrence that, at a minimum, includes: • the collection, use, and disclosure of PHI that is not in compliance with PHIPA and its regulations • a contravention of the privacy policies, procedures, or practices implemented by the PP or PE • a contravention of written acknowledgments, Data Sharing Agreements, Research Agreements, Confidentiality Agreements and TPSP Agreements, or • circumstances where PHI is stolen, lost, or collected, used, or disclosed without authority or where records of PHI are subject to unauthorized copying, modification, or disposal.
Privacy complaint	At a minimum, includes concerns or complaints relating to the privacy policies, procedures, and practices implemented by the PP or PE and related to the compliance of the PP or PE with PHIPA and its regulations.
Regulations	Regulation 329/04 to PHIPA as well as in any other regulations that may be enacted under PHIPA from time to time.

Term	Definition
Research Agreement	An agreement between PPs / PEs and researchers to whom PHI will be disclosed that is executed prior to the disclosure of PHI. Research Agreements are referred to in the following policies, procedures, and practices: • ***Policy, Procedures, and Practices for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements*** • ***Template Research Agreement*** • ***Log of Research Agreements*** • ***Policy, Procedures, and Practices for the Linkage of Records of Personal Health Information*** • ***Log of Approved Linkages of Records of Personal Health Information*** • ***Policy, Procedures, and Practices for Privacy Breach Management***

Term	Definition
Research plan	A research plan sets out in writing the intentions of a researcher in conducting planned research and, in accordance with PHIPA and its regulations, the research plan must, at a minimum, set out: • the affiliation of each person involved in the research • the nature and objectives of the research and the public or scientific benefit of the research that the researcher anticipates, and • all other prescribed matters related to the research. A research plan must be approved by a research ethics board and is subject to a number of additional requirements set out under PHIPA and its regulations. Research plans are referred to in the following policies, procedures, and practices: • ***Policy, Procedures, and Practices for the Use of Personal Health Information for Research*** • ***Log of Approved Uses of Personal Health Information for Research*** • ***Policy, Procedures, and Practices for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements*** • ***Log of Research Agreements*** • ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information***
Should	• Anytime the word “should” appears in the Manual, it indicates a recommendation.
Statement of Requested Exceptions	• A PP or PE must submit a written Statement of Requested Exceptions to the IPC if compliance with the requirements in **appendix A** or **appendix B** of the Manual has not been achieved, is not expected to be achieved or will no longer be achieved. The Statement of Requested Exceptions must be attached as an exhibit to the sworn affidavit, and include a rationale for each requirement not achieved or not expected to be achieved as of the date of the submission.

Term	Definition
Statement of Inapplicability	A PP or PE must submit a written Statement of Inapplicability where one or more of the requirements in appendix A or appendix B is inapplicable to a PP or PE. Statements of Inapplicability must be attached as an exhibit to the sworn affidavit, and must identify each requirement of the Manual that is inapplicable and provide the IPC with a rationale for the identified inapplicability.
Third-party service provider (TPSP)	A third-party service provider (TPSP) contracted or otherwise engaged to provide services to or for the PP or PE.
TPSP Agreement	An agreement executed between the PP or PE and a TPSP in accordance with the ***Policy, Procedures, and Practices for Executing Agreements with Third-Party Service Providers in Respect of Personal Health Information*** and the ***Template Agreement for All Third-Party Service Providers***. TPSP Agreements are referred to in in the following policies, procedures, and practices: • ***Policy, Procedures, and Practices for Executing Agreements with Third-Party Service Providers in Respect of Personal Health Information*** • ***Template Agreement for Third-Party Service Providers*** • ***Policy, Procedures, and Practices for Privacy Breach Management***

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

January 2024