June, 2024

Manual for the Review and Approval of Prescribed Organizations

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 Organizations

The prescribed organization ("PO") has the power and the duty to develop and maintain the electronic health record ("EHR") in accordance with Part V.1 of the ***Personal Health Information Protection Act, 2004*** ("PHIPA") and Ontario Regulation 329/04 ("the regulations").

The PO must perform the following functions set out under subsection 55.2 (2) of PHIPA:

1. Manage and integrate **personal health information** ("PHI") it receives from custodians.
2. Ensure the proper functioning of the EHR by servicing the electronic systems that support the EHR.
3. Ensure the accuracy and quality of the PHI that is accessible by means of the EHR by conducting data quality assurance activities on the PHI it receives from **health information custodians** ("custodians").
4. Conduct analyses of the PHI that are accessible by means of the EHR in order to provide alerts and reminders to custodians for their use in the provision of health care to individuals.

The PO is required to carry out prescribed powers, duties, or functions under Part V.1 of PHIPA and its related regulations. For the purpose of Part V.1 of PHIPA, "electronic health record" means the electronic systems that the PO develops and maintains to enable custodians to collect, use, and disclose PHI by means of the systems in accordance with Part V.1 and its related regulations.

When a custodian provides PHI to the PO to develop or maintain the EHR, the custodian is considered not to be disclosing the information to the PO and the PO is considered not to be collecting the information (see subsection 55.1(3) of PHIPA).

Subsection 55.9.1(1) of PHIPA states that where the prescribed requirements, if any, are met, the PO may provide PHI that is accessible by means of the EHR to a coroner in relation to an investigation conducted under the *Coroners Act*. In doing so, the PO must comply with section 55.3 of PHIPA and with the requirements of this *Manual for the Review and Approval of Prescribed Organizations* ("the Manual").

Requirements for a Prescribed Organization

The PO is required to have in place and comply with, practices and procedures to protect the privacy and confidentiality of the individuals whose PHI it receives to develop or maintain the EHR. The Information and Privacy Commissioner of Ontario ("IPC") must review and approve the practices and procedures of the PO initially and every three years thereafter to determine if its practices and procedures continue to meet the requirements. The requirement for the IPC's review of practices and procedures under paragraph 14 of section 55.3 of PHIPA is set out in subsection 55.12(1) of PHIPA.

Purpose of this Manual

The purposes of the Manual are to:

- Outline the process to be followed by the IPC in reviewing the practices and procedures implemented by the PO to protect the privacy and confidentiality of individuals whose PHI they receive to develop and maintain the EHR.
- Set out the requirements that are reasonably necessary to protect the PHI that the PO is permitted to receive.
- Assist the PO in complying with its obligations under PHIPA and its regulations.

Every three years, the PO must demonstrate compliance with the requirements in the Manual 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**."

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 PO to ensure continued compliance with the Manual as amended from time to time.

Other Manuals and Addenda

Under PHIPA, custodians may disclose PHI to a prescribed person ("PP") without consent for their compilation or maintenance of registries of PHI for purposes 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. Custodians may disclose PHI to a prescribed entity ("PE"), without consent, for the PE to analyse or compile 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. Like the PO, PPs and PEs under PHIPA, 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 Persons and Prescribed Entities*** that sets out the requirements for review and approval of PPs and PEs.

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*.

The PO, PPs, and PEs under PHIPA, as well as PEs under the CYFSA and the *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 The Prescribed Organization

The PO must have in place practices and procedures to protect the privacy and confidentiality of individuals whose PHI it receives to develop and maintain the EHR. At a minimum, these practices and procedures must:

- include the policies, procedures, practices, agreements, and other documentation set out in **appendix "A"**
- 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 PO
- amount and sensitivity of the PHI received to develop and maintain the EHR
- number and roles of the individuals with access to the PHI
- obligations and duties of the PO 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 PO, or to the **three-year review**, which is conducted every three years from the date of the initial approval by the IPC.

Initial Review of the Prescribed Organization

The PO seeking initial approval must submit to the IPC the applicable policies, procedures, and practices described in **appendix "A"** to the Manual that contain 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 PO and the requirements in **appendix "A"** or **appendix "B"** of the Manual, the PO 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 PO'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 PO has achieved, or will achieve, an equivalent standard to protect the privacy and confidentiality of the individuals whose PHI it receives; where a PO 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 the PO, the PO does not need to 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 PO, along with any Statements of Requested Exceptions and Statements of Inapplicability 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 PO. The purpose of the on-site meeting is to:

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

Approval Process

Following the on-site meeting:

- The PO 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 PO 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 PO 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 PO'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 PO 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 PO 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 PO 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 on whether to approve the practices and procedures of the PO, 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 PO. The IPC will track all recommendations to ensure that the PO 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).

The PO may not operate as a PO, 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 PO 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**, the IPC will not approve the practices and procedures of the PO. Generally, the IPC will endeavour to notify the PO 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 PO 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 PO's response and demonstrated assurances, the IPC may, in its sole discretion, approve the practices and procedures of the PO.

In the case where the policies, procedures, and practices of a PO are not approved on the date of requested or required approval, the IPC will inform the PO in writing of the reasons why approval was not granted, including the significant divergence(s) that must be addressed by the PO prior to obtaining approval. The PO 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 PO. To prevent undue delay in operating as a PO, this approval may be provided in the intervening time period between typical three-year review periods.

Three-Year Review of the Prescribed Organization

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, the PO seeking the continued approval of its policies, procedures, and practices must submit to the IPC 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 normal circumstances, the PO 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 using the template 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 PO 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 PO and the requirements in **appendix "A"** or **appendix "B"** of the Manual, the PO 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 PO'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 PO has achieved, or will achieve, an equivalent standard to protect the privacy and confidentiality of the individuals whose PHI it receives; where the PO 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 the PO, the PO does not need to 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 PO, along with any Statements of Requested Exceptions and Statements of Inapplicability 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 PO as set out above, the IPC will determine the scope of the policies, procedures, and practices of the PO 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 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 it considers relevant, including:

- whether there have been any changes to the PO'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 PO
- 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 PO
- results of privacy and information security audits conducted by the PO since the last review
- recent decisions, guidelines, fact sheets, etc. issued by the IPC or other relevant oversight offices
- privacy and information security trends emerging from complaints and privacy and information security breaches reported to the IPC
- privacy and information security trends identified through the IPC's environmental scanning function
- privacy and information security issues recently reported in the media more generally
- privacy and information security issues identified in a Statement of Requested Exceptions or a Statement of Inapplicability
- changes in requirements arising from new or amended laws or regulations
- evolving industry privacy and information security standards and best practices
- any other information the IPC and the PO 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 the PO 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 the PO 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 55.12(1) of PHIPA, depending on the level of privacy and information security risks revealed in the information and documentation provided by the PO.

Review of Selected Policies, Procedures, and Practices

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

The IPC will review the selected policies, procedures, and practices. The IPC will assess whether the PO's policies, procedures, and practices protect the privacy and confidentiality of individuals

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

Based on its assessment, the IPC will inform the PO 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 PO 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 PO 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 PO 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 PO 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 PO 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 PO 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 PO for a further three-year period.

The IPC's decision whether to approve the practices and procedures of a PO, 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 PO. The IPC will track all recommendations to ensure that the PO 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).

An organization may not continue to operate as a PO more than three years after the date of its prior approval, unless the IPC has advised the PO, 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 PO 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 above), the IPC will not approve the practices and procedures of the PO for a further three-year period. Generally, the IPC will endeavour to notify the PO 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 PO 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 PO's response and demonstrated assurances, the IPC may, in its sole discretion, approve the practices and procedures of the PO 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 the PO 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 PO in writing of the reasons why approval was not granted, including the significant divergence(s) that must be addressed by the PO prior to regaining approval. The PO 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 PO. To prevent undue delay in resumption of PO 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 PO, 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**.

The PO is also required to have a statement on its public-facing website 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 PO'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 PO claims is confidential, the PO 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 PO must:

- identify the specific information it believes should not be published
- provide a rationale for why this information is confidential and should not be published
- provide a draft copy of the indicators, Statement of Requested Exceptions or Statement of Inapplicability, redact the precise information it claims to be confidential, and suggest 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 each request and may request additional information from the PO 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 the PO is subject to other three-year reviews under PHIPA or different statutes, the reviews will be combined and conducted by a single review team at the IPC, if possible. The PO must also identify a single review team that will work on all three-year reviews together.

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 Organization*	18
	2. *Policy, Procedures, and Practices for Ongoing Review of Privacy Policies, Procedures, and Practices*	23
Transparency	3. *Policy on the Transparency of Privacy Policies, Procedures, and Practices*	25
Receiving Personal Health Information	4. *Policy, Procedures, and Practices for Receiving Personal Health Information*	27
	5. *List of Types of Personal Health Information Received*	30
	6. *Policy, Procedures, and Practices for Descriptions of Types of Personal Health Information Received*	30
	7. *Description of Types of Personal Health Information Received*	32
Consent Management in the Electronic Health Record	8. *Policy, Procedures, and Practices for Managing Consent in the Electronic Health Record*	32
	9. *Log of Notices of Consent Directives*	40
	10. *Log of Notices of Consent Overrides*	41
	11. *Log of Reports of Consent Overrides to the Information and Privacy Commissioner*	41
	12. *Log of Requests for Electronic Records from Health Information Custodians*	42
	13. *Log of Requests for Electronic Records from the Information and Privacy Commissioner*	42
	14. *Log of Audits of the Electronic Records of Consent Directives and Consent Overrides*	42
Viewing, Handling, or Otherwise Dealing with Personal Health Information	15. *Policy, Procedures, and Practices for Viewing, Handling, or Otherwise Dealing with Personal Health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization*	43

Categories	Required Policies, Procedures, and Practices	Page No. Appendix B
Viewing, Handling, or Otherwise Dealing with Personal Health Information (Cont'd)	16. Log of Employees and Other Persons Acting on Behalf of the Prescribed Organization Granted Permission to View, Handle, or Otherwise Deal with Personal Health Information	47
Provision of Personal Health Information Pursuant to Direction	17. Policy, Procedures, and Practices for the Provision of Personal Health Information Pursuant to a Direction Issued by a Member of a Ministry Data Integration Unit or by the Minister	48
	18. Log of Directions Issued by a Member of the Ministry Data Integration Unit or by the Minister	50
Requests for Access and Correction	19. Policies, Procedures, and Practices for Responding to Requests for Access and Correction of Records of Personal Health Information	50
	20. Log of Access and Correction Requests	55
Third-Party Service Provider Agreements	21. Policy, Procedures, and Practices for Executing Agreements with Third-Party Service Providers in Respect of Personal Health Information	57
	22. Template Agreement for Third-Party Service Providers	61
	23. Log of Agreements with Third-Party Service Providers	67
Privacy Impact Assessments	24. Policy, Procedures, and Practices for Privacy Impact Assessments	68
	25. Log of Privacy Impact Assessments	71
Privacy Audit Program	26. Policy, Procedures, and Practices in Respect of Privacy Audits	72
	27. Log of Privacy Audits	75
Privacy Breaches	28. Policy, Procedures, and Practices for Privacy Breach Management	75
	29. Log of Privacy Breaches	83
Privacy Complaints and Inquiries	30. Policy, Procedures, and Practices for Privacy Complaints	85
	31. Log of Privacy Complaints	90
	32. 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***	94
	2. ***Policy, Procedures, and Practices for Ongoing Review of Information Security Policies, Procedures and Practices***	96
Physical Security	3. ***Policy, Procedures, and Practices for Ensuring Physical Security of Personal Health Information***	98
	4. ***Policy, Procedures, and Practices with Respect to Access by Employees and Other Persons Acting on Behalf of the Prescribed Organization***	98
	5. ***Policy, Procedures, and Practices with Respect to Access By Visitors***	103
	6. ***Log of Eemployees or Other Persons Acting on behalf of the Prescribed Organization with Access to the Premises of the Prescribed Organization***	104
Secure Retention, Transfer, and Disposal	7. ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information***	104
	8. ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information on Mobile Devices and Remotely Accessing Personal Health Information***	106
	9. ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information***	111
	10. ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information***	113
Information Security	11. ***Policy, Procedures, and Practices Relating to Authentication and Passwords***	115
	12. ***Policy, Procedures, and Practices in Respect of Privacy Flags and Notices to Employees and Other Persons Acting On Behalf of the Prescribed Organization***	117
	13. ***Policy, Procedures, and Practices for Acceptable Use Agreements with Employees and Other Persons Acting On Behalf of the Prescribed Organization***	119

Categories	Required Policies, Procedures, and Practices	Page No. Appendix B
Information Security (Cont'd)	14. ***Template Acceptable Use Agreement with Employees and Other Persons Acting On Behalf of the Prescribed Organization***	121
	15. ***Log of Acceptable Use Agreements***	122
	16. ***Policy, Procedures, and Practices for End User Agreements***	123
	17. ***Template End User Agreements***	124
	18. ***Log of End User Agreements***	125
	19. ***Policy, Procedures, and Practices for Logging, Monitoring, and Auditing Privacy and information Security Events***	125
	20. ***Log of Requests for Electronic Records from Health Information Custodians***	136
	21. ***Log of Requests for Electronic Records from the Information and Privacy Commissioner***	137
	22. ***Policy, Procedures, and Practices for Vulnerability and Patch Management***	137
	23. ***Policy, Procedures, and Practices Related to Change Management***	143
	24. ***Policy, Procedures, and Practices for Back-Up and Recovery of Records of Personal Health Information***	147
	25. ***Policy, Procedures, and Practices on the Acceptable Use of Technology***	147
	26. ***Policy, Procedures, and Practices for Threat and Risk Assessments***	149
	27. ***Log of Threat and Risk Assessments***	151
Information Security Audit Program	28. ***Policy, Procedures, and Practices in Respect of Information Security Audits***	152
	29. ***Log of Information Security Audits***	155
Information Security Breaches	30. ***Policy, Procedures, and Practices for Information Security Breach Management***	156
	31. ***Log of Information Security Breaches***	164

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***	66
	2. ***Log of Completion of Initial and Ongoing Privacy Training***	170
Information Security Training and Awareness	3. ***Policy, Procedures, and Practices for Information Security Training and Awareness***	171
	4. ***Log of Completion of Initial and Ongoing Information Security Training***	175
Confidentiality Agreements	5. ***Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Employees and Other Persons Acting on Behalf of the Prescribed Organization***	175
	6. ***Template Confidentiality Agreement with Employees and Other Persons Acting on Behalf of the Prescribed Organization***	177
	7. ***Log of Executed Confidentiality Agreements with Employees and Other Persons Acting on Behalf of the Prescribed Organization***	179
Privacy and Information Security Leadership	8. ***Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program***	180
	9. ***Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Information Security Program***	181
Termination or Cessation	10. ***Policy, Procedures, and Practices upon Termination or Cessation of the Employment or Contractual Relationship***	182
Discipline and Corrective Action	11. ***Policy, Procedures, and Practices for Discipline and Corrective Action***	184

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***	185
	2. ***Information Security Governance and Accountability Framework***	187
	3. ***Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Information Security Program***	189
Risk Management	4. ***Corporate Risk Management Framework***	189
	5. ***Corporate Risk Register***	193
	6. ***Policy, Procedures, and Practices for Maintaining a Consolidated Log of Recommendations***	193
	7. ***Consolidated Log of Recommendations***	194
Business Continuity and Disaster Recovery	8. ***Business Continuity and Disaster Recovery Plan***	195

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 Organization

A PO must develop and implement an overarching privacy policy ("Privacy Policy") in relation to PHI it receives under Part V.1 of PHIPA ("the Privacy Policy"). At a minimum, the Privacy Policy must address the matters outlined below.

Status under the *Personal Health Information Protection Act*

The Privacy Policy in respect of its status as a PO must be described as defined in PHIPA and reflect the duties and responsibilities that arise as a result of this status. In particular, the Privacy Policy must indicate that the PO has implemented policies, procedures, and practices to protect the privacy and confidentiality of individuals whose PHI it receives to develop and maintain the EHR pursuant to section 55.2 of PHIPA. It must also provide that these policies, procedures, and practices are subject to review by the IPC every three years.

This Manual applies only to the role of a PO as that term is defined in section 2 of PHIPA. If the PO engages in activities or roles that are otherwise regulated by PHIPA, it should have appropriate policies, procedures, and practices in place that address the requirements of those other activities and roles.

The Privacy Policy must also articulate a commitment by the PO to comply with the provisions of PHIPA and its regulations applicable to the PO.

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 PO.

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
    - the privacy and information security policies, procedures, and practices implemented.

- identify the position(s) that have been delegated day-to-day authority to manage the privacy program and the information security program, including:
    - to whom these positions report
    - their duties and responsibilities to manage the privacy program and the information security program
    - some of the key activities in respect of these programs

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

Authority to Receive Personal Health Information

The Privacy Policy must:

- state that the PO receives PHI to develop and maintain the EHR
- describe the types of PHI received for this purpose
- identify the persons or organizations from which PHI is typically received
- ensure that each purpose for which PHI is received as identified in the Privacy Policy, is permitted by PHIPA and its regulations
- articulate a commitment by the PO not to receive PHI if other information will serve the purpose and not to receive more PHI than is reasonably necessary to meet the purpose
- outline the policies, procedures, and practices implemented by the PO to ensure that both the amount and the type of PHI received is limited to that which is reasonably necessary for its purpose
- list the types of PHI and the repositories within which the PHI is maintained by the PO
- identify where an individual may obtain further information in relation to the above

Consent Management

The Privacy Policy must set out the:

- process to manage consent directives made by individuals to withhold or withdraw, in whole or part, their consent to the collection, use, and disclosure of their PHI that is accessible by means of the EHR for the purpose of providing or assisting in the provision of health care to the individual
- name and/or title, mailing address and contact information for the employee(s) or other person(s) acting on behalf of the PO to whom consent directives may be submitted
- manner and format in which these consent directives may be submitted
- levels of specificity at which PHI may be made subject to a consent directive, and the extent to which its collection, use, and disclosure may be restricted

- data elements that may be collected, used, or disclosed for the purpose of uniquely identifying an individual whose PHI is collected by means of the EHR notwithstanding a consent directive

Minimizing the Personal Health Information Received

The Privacy Policy must articulate a commitment to, and the reasonable steps taken by the PO to limit the PHI it receives to that which is reasonably necessary for the purpose of developing or maintaining the EHR. In this regard, the Privacy Policy must:

- outline the policies, procedures, and practices implemented by the PO to ensure that both the amount and the type of PHI received is limited to that which is reasonably necessary for its purpose
- list the types of PHI maintained by the PO
- identify where an individual may obtain further information in relation to the types and sources of the PHI received by the PO for the purpose of developing or maintaining the EHR

Viewing, Handling, or Otherwise Dealing with Personal Health Information

The Privacy Policy must identify the purposes for which employees or any other persons acting on behalf of the PO, may view, handle, or otherwise deal with PHI received to develop and maintain the EHR. In identifying these purposes, the Privacy Policy must:

- specify that the PO does not permit its employees or any other person acting on its behalf to view, handle, or otherwise deal with the PHI received to develop and maintain the EHR, unless the employee or person acting on its behalf agrees to comply with the restrictions that apply to the PO, identify the policies, procedures, and practices the PO has implemented to prohibit its employee(s) or any other person(s) acting on its behalf from:
    - viewing, handling, or otherwise dealing with PHI if other information, such as de-identified or aggregate information, will serve the purposes
    - using more PHI than is reasonably necessary to meet the purpose(s) identified
- state that the PO remains responsible for PHI viewed, handled, or otherwise dealt with by its employees and any other persons acting on its behalf
- identify the policies, procedures, and practices implemented to ensure that its employees and other persons acting on behalf of the PO only view, handle, or otherwise deal with PHI in accordance with PHIPA and its regulations and in compliance with the privacy and information security policies, procedures, and practices implemented

Providing Personal Health Information to Another Person

The Privacy Policy must state that the PO may not provide PHI to any person, except as permitted or required by PHIPA and its regulations.

The Privacy Policy must specify:

- that a member of a ministry data integration unit ("MDIU"), located within the Ministry of Health ("Ministry"), may issue a direction requiring the PO to provide it with the limited amount of PHI from the EHR the MDIU is permitted to collect pursuant to subsection 55.9(1) of PHIPA, and that the PO must comply with such a direction
- the limited purposes for which and circumstances in which the member of the MDIU is permitted to collect the PHI under subsection 55.9(1) of PHIPA
- that the Minister of Health ("Minister") may direct the disclosure of PHI that is accessible by means of the EHR, as if the Minister had custody and control of the information, in accordance with clause 39(1)(c), subsection 39(2), or section 44 or 45 of PHIPA and that the PO must comply with the direction

The Privacy Policy must also state that a direction of the member of the MDIU or the Minister may specify the form, manner, and timeframe in which the information that is the subject of the direction is to be provided to the MDIU or disclosed.

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

The Privacy Policy must address the secure retention of records of PHI received by the PO to develop and maintain the EHR 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
- the manner in which records of PHI 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 and confidentiality of individuals whose PHI the PO receives to develop and maintain the EHR
- specify the steps taken to ensure that PHI accessible by means of the EHR is not collected without authority
- ensure the PHI accessible by means of the EHR is protected against:
    - theft, loss, and unauthorized collection, use, or disclosure
    - 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 compliance of the PO with PHIPA and its regulations and the privacy policies, procedures, and practices implemented by the PO.

The Privacy Policy must also:

- include the name and/or title, mailing address, and contact information of the employee(s) and other person(s) acting on behalf of the PO 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 privacy-related complaints regarding the compliance of the PO or one or more custodian(s) who collect, use, or disclose PHI by means of the EHR, with PHIPA and its regulations to the IPC and provide the mailing address and contact information for the IPC
- identify where individuals may obtain further information in relation to the privacy policies, procedures, and practices of the PO or one or more custodian(s)

Access and Correction

The Privacy Policy must set out the policies, procedures, and practices by which the PO will respond to a request made by an individual under Part V of PHIPA to access or correct a record of the individual's PHI that is accessible by means of the EHR or the electronic records kept by the PO under paragraphs 4, 5, and 6 of section 55.3 of PHIPA. The information provided must:

- include the name and/or title, mailing address, and contact information for the employee(s) or other person(s) acting on behalf of the PO to whom requests for access or correction may be directed
- describe the manner and format in which these requests may be made
- state that individuals may direct complaints related to access and correction to the IPC
- set out the policies, procedures, and practices that have been approved by the Minister for responding to or facilitating a response to a request made by an individual to a custodian under Part V of PHIPA to access or correct a record of their PHI that is accessible by means of the EHR

Transparency of Practices

The Privacy Policy must state that the PO makes available to:

- the public and to each custodian that provided PHI to it for the purpose of developing or maintaining the EHR, a plain language description of the EHR, including a general description of the administrative, technical, and physical safeguards in place, and any directives, guidelines, and policies, procedures, and practices of the PO that apply to the PHI that is accessible by means of the EHR
- the name and contact information of individuals from whom further information may be obtained in relation to the privacy policies, procedures, and practices of the PO

- each custodian that provided PHI to the PO for the purpose of developing or maintaining the EHR, for each system that retrieves, processes, or integrates PHI that is accessible by means of the EHR, a written copy of the result of an assessment with respect to the threats, vulnerabilities, and risks to the security and integrity of the PHI that is accessible by means the EHR, and how each system may affect the privacy of the individuals to whom the information relates
- the public, for each system that retrieves, processes, or integrates PHI that is accessible by means of the EHR, a summary of the results of any assessments with respect to the threats, vulnerabilities and risks to the security and integrity of the PHI accessible by means of the EHR, and how each system may affect the privacy of the individuals to whom the information relates

Compliance, Audit, and Enforcement

The Privacy Policy must:

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

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

A policy, procedures, and practices must be developed and implemented for the ongoing review of the PO'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 scheduled three-year review by the IPC pursuant to section 55.12 of PHIPA, and whenever the Minister issues a directive to the PO with respect to the carrying out of its responsibilities and functions

- employee(s) and other person(s) acting on behalf of the PO responsible and the procedure for undertaking the review
- timeframe in which the review will be undertaken
- employee(s) and other person(s) acting on behalf of the PO responsible and the procedure for amending, and/or drafting new privacy policies, procedures, and practices
- employee(s) and other person(s) acting on behalf of the PO 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
- employee(s) and other person(s) acting on behalf of the PO responsible and the procedure for communicating the amended or newly developed privacy policies, procedures, and practices
- method and nature of the communication to employee(s) and other persons acting on behalf of the PO, 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 PO must have regard to:

- any directives made to the PO by the Minister pursuant to section 55.4 of PHIPA
- 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 PO
- 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 PO continue to be consistent with its actual practices
- whether there is consistency between and among the privacy and information security policies, procedures, and practices implemented

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require employees and other persons acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) and other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an employee or other person acting on behalf of the PO breaches or believes there may have been breach of this policy, procedures, or practices

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

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, including custodians that provide PHI to the PO to develop and maintain the EHR, relating to the privacy policies, procedures, and practices implemented by the PO ("transparency policy") and that identifies the means by which such information is made available.

At a minimum, the transparency policy must require the PO to make the following information available to the public and each custodian that provides PHI to the PO to develop and maintain the EHR:

- its **Privacy Policy**
- documentation related to the review by the IPC of the policies, procedures, and practices implemented by the PO pursuant to PHIPA and its regulations
- brochures, frequently asked questions, and/or other plain language tools related to the privacy policies, procedures, and practices implemented by the PO
- a list of the repositories that are accessible by means of the EHR and a description of the nature and type(s) of PHI in each
- a plain language description of the EHR, including a general description of the administrative, technical, and physical safeguards in place to protect:
    - PHI accessible by means of the EHR against theft, loss, and unauthorized collection, use, or disclosure and to protect records of PHI against unauthorized copying, modification, or disposal
    - the integrity, security, and confidentiality of the PHI that is accessible by means of the EHR
- any directives, guidelines, and policies that apply to the PHI that is accessible by means of the EHR, to the extent that these do not reveal a trade secret or confidential scientific, technical, commercial, or labour relations information

- a description of the privacy policies, procedures, and practices implemented in respect of PHI, including the:
    - types of PHI received and the persons or organizations from which this PHI is typically received
    - purposes for which employee(s) or other person(s) acting on behalf of the PO may view, handle, or otherwise deal with PHI
    - requirement for the PO to comply with a directive issued by the Minister to the PO to provide PHI to the Minister or to disclose PHI to a person, in accordance with clause 39(1)(c), subsection 39(2) or section 44 or 45 of PHIPA
- the name and/or title, mailing address, and contact information of the employee(s) and other person(s) acting on behalf of the PO to whom inquiries, concerns, or complaints may be directed regarding:
    - requests to make directives to withhold or withdraw, in whole or part, consent to the collection, use, and disclosure of their PHI by means of the EHR by a custodian for the purpose of providing or assisting in the provision of health care to the individual
    - inquiries, concerns, or complaints regarding the PO's compliance with PHIPA and its regulation, and the privacy policies, procedures, and practices implemented pursuant thereto
    - requests for access to or correction of an individual's records of PHI that are accessible by means of the EHR developed or maintained by the PO

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. In particular, such content must:

- describe the status of the PO 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 received and the persons or organizations from which this PHI is typically received
    - purposes for which PHI is received
    - purposes for which employee(s) or other person(s) acting on behalf of the PO may view, handle, or otherwise deal with PHI
    - PHI viewed, handled, or otherwise dealt with, and if identifiable information is not routinely viewed, handled, or otherwise dealt with, the nature of the information that is used

  - 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 integrity, security, and 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
- provide the name and/or title, mailing address, and contact information of the employee(s) and other person(s) acting on behalf of the PO to whom inquiries, concerns, or complaints may be directed regarding the PO's compliance with the privacy policies, procedures, and practices

Statement on Public Website

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

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

Receiving Personal Health Information

4. Policy, Procedures, and Practices for Receiving Personal Health Information

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

- the purpose for which PHI will be received by the PO

- the nature of the PHI that will be received
- from whom the PHI will typically be received
- the secure manner in which PHI will be received

The policy, procedures, and practices must articulate a commitment by the PO to:

- take reasonable steps to limit the PHI it receives to that which is reasonably necessary to develop and maintain the EHR
- receive the PHI that classes of custodians or specific custodians are required to provide to the PO in accordance with PHIPA and its regulations

Review and Approval Process for Receiving Personal Health Information

The policy, procedures, and practices must identify the:

- employee(s) and other person(s) acting on behalf of the PO responsible for reviewing and determining the PHI the PO should receive to develop and maintain the EHR, other than the PHI, if any, that classes of custodians or specific custodians must provide to the PO, pursuant to the regulations
- process that must be followed
- requirements, conditions, restrictions, and other criteria that must be satisfied
- steps that must be taken to ensure that the PHI is not received without authority

At a minimum, the above criteria must require the responsible employee(s) and other person(s) acting on behalf of the PO responsible for determining whether to approve the receipt of PHI to ensure that:

- the receipt of PHI is permitted by PHIPA and its regulations and that any and all conditions or restrictions set out in PHIPA and its regulations or by the Minister have been satisfied
- 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 develop and maintain the EHR

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

- the manner of documenting the decision approving or denying the receipt of PHI and the required content of the documentation
- the reasons for the decision are documented
- the method and format in which the decision will be communicated
- to whom the decision will be communicated

Conditions or Restrictions on the Approval to Receive Personal Health Information

The policy, procedures, and practices must identify the conditions or restrictions that are required to be satisfied prior to the receipt of PHI to develop and maintain the EHR, 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 employee(s) and other person(s) acting on behalf of the PO and other persons or organizations responsible for completing, providing, or executing the documentation and/or agreements
- the conditions or restrictions that must be completed, provided, or executed, having regard to requirements of PHIPA and its regulations, any directions issued by the Minister, and identified in the policy, procedures, and practices
- the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring that any conditions or restrictions that must be satisfied prior to the receipt of PHI to develop and maintain the EHR 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 received by the PO to develop and maintain the EHR be retained in a secure manner in compliance with the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information***
- that records of PHI provided to the PO to develop and maintain the EHR, be transferred in a secure manner in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information***
- the identification of the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring that the records of PHI that have been received to develop and maintain the EHR 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 PO's receipt of the PHI

If the records of PHI are required to be securely returned to the person or organization from which they were received, 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 employees and other persons acting on behalf of the PO to comply with the policy, procedures, and practices

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

5. List of Types of Personal Health Information Received

The PO must develop and retain an up-to-date list of each of the repositories that are accessible by means of the EHR, and a brief description of the types of PHI the PO receives to develop or maintain the EHR that are contained in each repository.

6. Policy, Procedures, and Practices for Descriptions of Types of Personal Health Information Received

A policy, procedures, and practices must be developed and implemented with respect to the creation, review, amendment, and approval of descriptions of types of PHI received by the PO to develop or maintain the EHR.

The policy, procedures, and practices must require the descriptions to set out:

- an up-to-date list of each type of PHI received (e.g., demographic, laboratory, drugs)
- a description of each type of PHI (e.g., requisitions, orders, results)
- the source(s) of the PHI (e.g., Minister, laboratories, hospitals)
- the repository in which the PHI is contained
- explain whether or not the PHI is received pursuant to the regulations

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

- employee(s) and other person(s) acting on behalf of the PO responsible and the process that must be followed in completing the descriptions of the types of PHI received to develop or maintain the EHR
- employee(s) or other person(s) acting on behalf of the PO responsible for approving the description of types of PHI received
- the employee(s) or other person(s) acting on behalf of the PO and other persons or organizations that must be consulted in the process
- employee(s) or other person(s) acting on behalf of the PO responsible for approving the description of the types of PHI received

- role of the employee(s) or other person(s) acting on behalf of the PO that have been delegated day-to-day authority to manage the privacy program in respect of the description of the types of PHI received
- person(s) and organization(s) that will be provided the description of the types of PHI received must also be identified, including, at a minimum, the custodian(s) or other person(s) or organization(s) from whom the PHI is received
- frequency with which and the circumstances in which the description of the types of PHI received must be reviewed
- employee(s) and other person(s) acting on behalf of the PO responsible and the process that must be followed in reviewing the description of the types of PHI received, if necessary
- employee(s) and other person(s) acting on behalf of the PO or other person(s) or organization(s) that must be consulted in reviewing, and if necessary, amending the description of the types of PHI received
- employee(s) and other person(s) acting on behalf of the PO responsible for approving the amended description of the type and nature of PHI received
- person(s) and organization(s) that will be provided the amended description of the types of PHI received upon approval, including custodians or other persons or organizations from whom the PHI is received

The policy, procedures, and practices must be reviewed on an ongoing basis to ensure their continued accuracy, that the PHI received for purposes of developing or maintaining the EHR continues to be necessary for the identified purpose(s).

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

7. Description of Types of Personal Health Information Received

For each type of PHI received to develop or maintain the EHR, the PO must describe:

- each type of PHI received (e.g., demographic, laboratory, drugs)
- the nature of the PHI (e.g., requisitions, orders, results)
- the source(s) of the PHI (e.g., Minister, laboratories, hospitals)
- the repository in which the PHI is contained
- whether or not the PHI is received pursuant to the regulations

Consent Management in the Electronic Health Record

8. Policy, Procedures, and Practices for Managing Consent in the Electronic Health Record

A policy, procedures, and practices must be developed and implemented to address the process to be followed in receiving, documenting, implementing, testing, auditing, and monitoring individuals' requests to withhold or withdraw, in whole or part, the individual's consent to the collection, use, and disclosure of their PHI by means of the EHR by a custodian for the purpose of providing or assisting in the provision of health care to the individual (consent directives). Where the individual has made such a consent directive, the policy, procedures, and practices must also address the process to be followed in receiving, documenting, and implementing an individual's request to modify or withdraw such consent directives.

The policy, procedures, and practices must:

- require the PO to implement, withdraw, or modify a consent directive prescribed in the regulations when or as requested to do so by an individual
- set out the level of specificity at which PHI may be made subject to a consent directive, including whose collection, use, and disclosure of the information may be restricted and, at a minimum, this must include the level of specificity prescribed in the regulations
- specify the data elements that may be collected, used, or disclosed by a custodian for the purpose of uniquely identifying an individual in order to collect PHI by means of the her, notwithstanding any consent directive of the individual, and this must be consistent with the data elements that may not be made subject to a consent directive prescribed in the regulations

The policy, procedures, and practices must also identify the information that must be communicated to the public relating to consent directives. This information must include:

- the specificity at which PHI may be made subject to a consent directive, including whose collection, use, and disclosure of the information may be restricted
- any data elements that may not be made subject to a consent directive
- the name and/or title, mailing address, and contact information of the employee(s) or other person(s) acting on behalf of the PO to whom such requests may be submitted

- the manner and format in which individuals may submit requests to make, modify, or withdraw consent directives

Receiving Requests for Consent Directives

The policy, procedures, and practices must establish the process to be followed in receiving requests to make, modify, or withdraw consent directives in accordance with section 55.6 of PHIPA. This must include:

- the nature of the information to be requested from the individual submitting the request, and any documentation that must be completed, provided, and/or executed by the individual making the request
- the employee(s) or other person(s) acting on behalf of the PO responsible for receiving the request, and any documentation that must be completed, provided, and/or executed, including the required content of the documentation
- the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, or ensuring the execution of the documentation
- the required content of the documentation
- the employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided
- the timeframe within which the documentation must be completed and provided

The policy, procedures, and practices must require the PO to offer assistance to the individual in reformulating a consent directive, if the directive does not contain sufficient detail to enable the PO to implement the directive with reasonable efforts. In this regard, the policy, procedures, and practices must identify the employee(s) or other person(s) acting on behalf of the PO responsible for assisting individuals, including the manner in which such assistance will be offered, and the timeframe within which such assistance will be offered.

Implementing and Testing Consent Directives

The policy, procedures, and practices must establish the process to be followed in implementing an individual's request to make, modify, or withhold a consent directive. At minimum, the policy, procedures, and practices must identify the:

- employee(s) or other person(s) acting on behalf of the PO responsible for implementing the request
- manner in which the consent directive must be implemented
- documentation that must be completed, provided, and/or executed, including the required content of the documentation
- employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, or ensuring the execution of the documentation
- employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided

- timeframe within which the request must be implemented, and the documentation that must be provided
- requirement for consent directives to be implemented in accordance with the requirements prescribed in the regulations, if any

The policy, procedures, and practices must also require the PO to take reasonable steps to ensure that requests to make, modify, or withdraw a consent directive have been properly implemented. At a minimum, the process to be followed in testing whether requests have been properly implemented should specify the:

- employee(s) or other person(s) acting on behalf of the PO responsible for testing to ensure that the request has been properly implemented
- manner in which the testing must be done
- documentation that must be completed, provided, and/or executed, including the required content of the documentation
- employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, or ensuring the execution of the documentation
- employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided
- timeframe within which the testing must be completed and documentation to be provided

The policy, procedures, and practices must establish a process to be followed for notifying an individual that a consent directive has been implemented. In this regard, the policy must identify the:

- employee(s) or other person(s) acting on behalf of the PO responsible for notifying individuals
- manner in which the notice must be provided and the required content of the notice
- documentation that must be completed, provided, and/or executed by the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, or ensuring the execution of the documentation, and the required content of the documentation
- employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided
- timeframe within which the notice must be provided and documentation to be provided

Keeping an Electronic Record of and Auditing and Monitoring Consent Directives

The policy, procedures, and practices must require the PO to keep an electronic record of all instances where a consent directive is made, modified or withdrawn, as required by paragraph 5 of section 55.3 of PHIPA. The electronic record must identify the:

- individual who made, withdrew, or modified the consent directive
- instructions the individual provided regarding the consent directive

- custodian, agent, or other person to whom the directive was made, withdrawn, or modified
- date and time that the consent directive was made, withdrawn, or modified

The policy, procedures and practices must require the PO to continuously audit and monitor the electronic record of all instances where a consent directive is made, withdrawn, or modified, to ensure that the consent directive continues to apply, as requested. This includes establishing the process for continuously auditing and monitoring the electronic record to ensure that the consent directive continues to apply. At a minimum, the policy, procedures, and practices must identify the:

- employee(s) or other person(s) acting on behalf of the PO responsible for continuously auditing and monitoring to ensure that consent directives continue to apply
- manner in which this continuous auditing and monitoring must be done
- documentation that must be completed, provided, and/or executed, and the required content of the documentation
- employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, or ensuring the execution of the documentation
- employee(s) or other person(s) acting on behalf of the PO to whom the documentation must be provided
- timeframe within which the documentation must be provided

Providing Notice of Consent Directives

If a custodian seeks to collect PHI that is subject to a consent directive, the policy, procedures, and practices must require the PO to notify the custodian that an individual has made a directive without providing any PHI that is subject to the directive, in accordance with subsection 55.6(7) of PHIPA. The policy, procedures, and practices must establish a process to be followed in notifying a custodian that an individual has made a consent directive and must identify the:

- employee(s) or other person(s) acting on behalf of the PO responsible for ensuring that a custodian has been notified of a consent directive
- manner in which the notice must be provided, and the required content of the notice
- documentation that must be completed, provided, or executed, including the required content of the documentation
- employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, or ensuring the execution of the required documentation
- employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided
- timeframe within which the documentation must be provided

Overrides of Consent Directives

The policy, procedures, and practices must require the PO to permit a custodian to override a consent directive in the circumstances set out in section 55.7 of PHIPA. In particular, the policy, procedures, and practices must require the PO to permit a custodian to override a consent directive only where the custodian that is seeking to collect the information:

- obtains the express consent of the individual to whom the information relates, or
- believes, on reasonable grounds, that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the individual to whom it relates, and it is not reasonably possible for the custodian that is seeking to collect the PHI to obtain the individual's consent in a timely manner, or
- believes, on reasonable grounds, that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom it relates or a group of persons

The policy, procedures, and practices must set out the process to be followed in overriding a consent directive, including by identifying the:

- employee(s) or other person(s) acting on behalf of the PO responsible for ensuring the custodians are able to override a consent directive and the manner in which a consent directive may be overridden
- documentation that must be completed, provided, and/or executed by the employee(s) or other person(s) acting on behalf of the PO responsible for ensuring that consent directives can be overridden, and/or by the custodian that overrides the consent directive, including the required content of the documentation
- employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, or ensuring the execution of the documentation
- employee(s) or other person(s) acting on behalf of the PO or other persons to whom this documentation must be provided
- timeframe within which the documentation must be provided

At a minimum, the policy, procedures, and practices must require the PO to notify the custodian in the event the custodian overrides a consent directive.

Keeping an Electronic Record of and Auditing and Monitoring Consent Overrides

The policy, procedures, and practices must require the PO to keep an electronic record of all instances where a consent directive is overridden by a custodian, as required by paragraph 6 of section 55.3 of PHIPA. The electronic record must identify:

- the custodian that disclosed the PHI
- the custodian that collected the PHI
- any agent of the custodian who collected the information

- the individual to whom the information relates
- the type of information that was disclosed and collected
- the date and time of the disclosure and collection
- the purpose of the disclosure (i.e., to provide health care or facilitate the provision of health care to the individual with the consent of the individual, to prevent harm to the individual to whom the information relates, or to prevent harm to another person or group of persons)

The policies, procedures, and practices must require the PO as required by paragraph 7 of section 55.3 of PHIPA, to audit and monitor the electronic record of all instances where a consent directive is overridden by a custodian, including by identifying the:

- employee(s) or other person(s) acting on behalf of the PO responsible for auditing and monitoring the consent override and the manner in which this auditing and monitoring must be completed
- documentation that must be completed, provided, and/or executed, and the required content of the documentation
- employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, or ensuring the execution of the documentation, and to whom this documentation must be provided
- timeframe within which the documentation must be provided

Providing Notice of Consent Overrides

The policy, procedures, and practices must set out the process that must be followed in notifying custodians about consent overrides, as required by subsection 55.7 (6) of PHIPA. At a minimum, where PHI that has been made subject to a consent directive has been collected by a custodian pursuant to a consent override, the policy, procedures, and practices must:

- require the PO to immediately provide written notice, in accordance with the requirements prescribed in the regulations, to the custodian that collected the information
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for identifying consent overrides and for notifying custodians about consent overrides
- specify the form, manner, and timeframe within which the notice must be provided, in accordance with the requirements in the regulations
- set out the information that must be contained in the notice which, at a minimum, must include:
    - the name of the individual to whom the information relates
    - the name of any agent of the custodian who collected the information, if available
    - a general description of the type of PHI that was collected

- the reason(s) for the consent override as described in PHIPA (i.e., to provide health care or facilitate the provision of health care to the individual with the consent of the individual, to prevent harm to the individual to whom the information relates, or to prevent harm to another person or group of persons)
- the date and time of the collection

Reporting Consent Overrides to the Information and Privacy Commissioner

The policy, procedures, and practices must require the PO to submit to the IPC a report of every instance where PHI that is accessible by means of the EHR that is the subject of a consent directive is disclosed pursuant to a consent override since the time of the last report, as required by paragraph 16 of section 55.3 of PHIPA. With respect to the report of consent overrides the PO must submit to the IPC, the policy, procedures, and practices must:

- require that the report be submitted at least annually
- specify the form and manner of the report which must be in accordance with that specified by the IPC
- identify the information that must be contained in the report which, at a minimum, must not include any PHI
- set out the employee(s) or other person(s) acting on behalf of the PO:
  - responsible for preparing the report
  - to whom the report must be provided
  - responsible for approving the report
  - responsible for providing the report to the IPC
- specify the timeframe within which the report must be provided to the IPC

Responding to Requests for Electronic Records of Consent Directives and Consent Overrides

The policy, procedures, and practices must set out the process that must be followed in responding to requests from custodians pursuant to paragraph 9 of section 55.3 of PHIPA for the electronic records of consent directives and consent overrides that the PO is required to keep pursuant to paragraphs 5 and 6 of section 55.3 of PHIPA. At a minimum, the policy, procedures, and practices must:

- indicate that the PO must provide, upon the request of a custodian that requires the records to audit and monitor its compliance with PHIPA, the electronic records that the PO is required to keep under PHIPA
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for receiving requests for electronic records from custodians
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for preparing and providing the electronic records requested by custodians

- specify any documentation, and its required content, that must be completed, provided, and/or executed by the employee(s) or other person(s) acting on behalf of the PO and/or the custodian requesting the electronic records
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, and ensuring the execution of documentation
- identify the employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided
- specify the form, manner, and timeframe within which the electronic records requested by custodians must be provided

The policy, procedures, and practices must also set out the process that must be followed in responding to requests from the IPC pursuant to paragraph 8 of section 55.3 of PHIPA for electronic records that the PO is required to keep pursuant to paragraphs 5 and 6 of section 55.3 of PHIPA. At a minimum, the policy, procedures, and practices must:

- indicate that the PO must provide, upon the request of the IPC, the electronic records that the PO is required to keep under PHIPA to the IPC for the purposes of Part VI of PHIPA
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for:
    - receiving requests for electronic records from the IPC
    - preparing the electronic records requested by the IPC
    - providing the requested information to the IPC
- specify the documentation, and its required content, that must be completed, provided, and/or executed by the employee(s) or other person(s) acting on behalf of the PO, and/or the IPC
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, and ensuring the execution of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO to whom the documentation must be provided
- specify the form, manner, and timeframe within which the electronic records requested by the IPC must be provided

Logging

The policy, procedures, and practices must further require that logs be maintained of the following:

- all instances where a notice of a consent directive is provided to a custodian pursuant to subsection 55.6 (7) of PHIPA
- all instances where a notice of a consent override is provided to a custodian pursuant to subsection 55.7 (6) of PHIPA

- all instances where a report of consent overrides is provided to the IPC pursuant to paragraph 16 of section 55.3 of PHIPA
- all requests from the IPC, made pursuant to paragraph 8 of section 55.3 of PHIPA, for the electronic records the PO is required to maintain pursuant to paragraphs 5 and 6 of section 55.3 of PHIPA
- all requests from custodians, made pursuant to paragraph 9 of section 55.3 of PHIPA, for the electronic records the PO is required to maintain pursuant to paragraphs 5 and 6 of section 55.3 of PHIPA
- the audits, required by paragraph 7 of section 55.3 of PHIPA, of the electronic records that the PO is required to keep under paragraphs 5 and 6 of section 55.3 of PHIPA

The policy, procedures, and practices must also identify the employee(s) or other person(s) acting on behalf of the PO responsible for:

- maintaining each log
- auditing and monitoring the log to ensure that notices of consent overrides are provided to individuals and reports of consent overrides are provided to the IPC

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

9. Log of Notices of Consent Directives

The PO must maintain a log of notices of consent directives that have been provided to a custodian pursuant to subsection 55.6(7) of PHIPA. At a minimum, the log must set out the:

- employee(s) or other person(s) acting on behalf of the PO who sent the notice
- custodian to whom the notice was sent
- date the notice was sent

- individual to whom the PHI relates
- type of PHI subject to the consent directive

For overrides of consent made, the log must set out the:

- custodian that disclosed the PHI as a result of the override
- name of any agent who collected the PHI on a custodian's behalf
- date and time of the collection,
- purpose of the collection (i.e., to provide health care or facilitate the provision of health care to the individual with the consent of the individual, to prevent harm to the individual to whom the information relates, or to prevent harm to a person other than the individual to whom the information relates or to a group of persons)

10. Log of Notices of Consent Overrides

The PO must maintain a log of notices of consent overrides that have been sent to custodians pursuant to subsection 55.7(6) of PHIPA. At a minimum, the log must set out the:

- employee(s) or other person(s) acting on behalf of the PO who sent the notice
- custodian to whom the notice was sent
- date the notice was sent
- custodian that disclosed the PHI as a result of the override
- name of any agent who collected the PHI on a custodian's behalf
- individual to whom the PHI relates
- type of PHI that was collected and the date and time of the collection
- purpose of the collection (i.e., to provide health care or facilitate the provision of health care to the individual with the consent of the individual, to prevent harm to the individual to whom the information relates, or to prevent harm to a person other than the individual to whom the information relates or to a group of persons)

11. Log of Reports of Consent Overrides to the Information and Privacy Commissioner

The PO must maintain a log of annual reports provided to the IPC pursuant to paragraph 16 of subsection 55.3 of PHIPA respecting every instance where PHI that is accessible by means of the EHR was disclosed, notwithstanding a consent directive, since the time of the last report. At a minimum, for each annual report, the log must set out the:

- employee(s) or other person(s) acting on behalf of the PO who sent the report to the IPC
- IPC employee(s) to whom the report was sent
- date the report was sent
- date by which the next annual report must be sent to the IPC

12. Log of Requests for Electronic Records from Health Information Custodians

The PO must maintain a log of the electronic records that are provided to custodians, pursuant to paragraph 9 of section 55.3 of PHIPA. At a minimum, for each request for electronic records received from a custodian, the log must set out the:

- employee(s) or other person(s) acting on behalf of the PO who received the request for electronic records
- date the request for electronic records was received by the PO
- custodian who made the request for electronic records
- type(s) of electronic records that were requested by the custodian
- employee(s) or other person(s) acting on behalf of the PO who responded to the request
- type(s) of electronic records that were provided to the custodian
- agent of the custodian to whom the electronic records were provided
- form, manner, and date the electronic records were provided to the custodian

13. Log of Requests for Electronic Records from the Information and Privacy Commissioner

The PO must maintain a log of the electronic records that are provided to the IPC pursuant to paragraph 8 of section 55.3 of PHIPA. At a minimum, for each request for electronic records received from the IPC, the log must set out the:

- employee(s) or other person(s) acting on behalf of the PO who received the request for electronic records
- date the request was received
- IPC employee(s) who submitted the request
- type(s) of electronic records that were requested by the IPC
- employee(s) or other person(s) acting on behalf of the PO who responded to the request
- type(s) of electronic records that were provided to the IPC
- IPC employee(s) to whom the electronic records were provided
- form, manner, and date when the electronic records were provided to the IPC

14. Log of Audits of the Electronic Records of Consent Directives and Consent Overrides

The PO must maintain a log of all audits conducted on the electronic records the PO is required to maintain of consent directives and consent overrides pursuant to paragraphs 5 and 6 of section 55.3 of PHIPA. At a minimum, for each audit conducted, the log must set out the:

- nature and scope of the audit
- employee(s) or other person(s) acting on behalf of the PO who conducted the audit
- date the audit was conducted

- results of the audit
- follow-up action that is required to be taken as a result of the audit
- employee(s) or other person(s) acting on behalf of the PO responsible for taking the follow-up action
- date the follow-up action was completed
- employee(s) or other person(s) acting on behalf of the PO or other third parties to whom the results of the audit must be communicated
- employee(s) or other person(s) acting on behalf of the PO responsible for communicating the results of the audit

Viewing, Handling, or Otherwise Dealing with Personal Health Information

15. Policy, Procedures, and Practices for Viewing, Handling, or Otherwise Dealing with Personal Health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization

A policy, procedures, and practices must be developed and implemented based on the "need to know" principle, to limit the purposes for which and the circumstances in which PHI received for the purpose of developing or maintaining the EHR may be viewed, handled, or otherwise dealt with by employees and other persons acting on behalf of the PO, and the secure manner in which the PHI must be viewed, handled, or otherwise dealt with. This is to ensure that employees and other persons acting on behalf of the PO view, handle, or otherwise deal with the least identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual, or other responsibilities.

Levels of Access

The policy, procedures, and practices must:

- identify the limited and narrowly defined purposes for which and circumstances in which employees and other persons acting on behalf of the PO are permitted to view, handle, or otherwise deal with PHI and the levels of access to PHI that may be granted
- ensure that the duties of employees and other persons acting on behalf of the PO permitted to view, handle, or otherwise deal with PHI are segregated in order to avoid a concentration of privileges that would enable a single employee or other person acting on behalf of the PO to compromise PHI

For all other purposes and in all other circumstances, the policy, procedures, and practices must require employee(s) or other person(s) acting on behalf of the PO to access and use de-identified and/or aggregate information, as permitted by PHIPA or another Act.

The policy, procedures, and practices must explicitly prohibit employees or other persons acting on behalf of the PO from:

- viewing, handling, or otherwise dealing with PHI if other information, such as de-identified and/or aggregate information, will serve the identified purpose

- viewing, handling, or otherwise dealing with more PHI than is reasonably necessary to meet the identified purpose
- using 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 Act. This must include prohibiting any attempt to decrypt information that is encrypted or identifying an individual based on unencrypted information and/or prior knowledge

Review and Approval Process

The policy, procedures, and practices must identify the employee(s) and other person(s) acting on behalf of the PO responsible and the process to be followed in receiving, reviewing, and determining whether to approve or deny a request by an employee or other person acting on behalf of the PO to view, handle, or otherwise deal with PHI received to develop or maintain the EHR, along with the various level(s) of access that may be granted by the PO.

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 employee or other person acting on behalf of the PO to view, handle, or otherwise deal with PHI
- criteria that must be considered by the employee(s) and other person(s) acting on behalf of the PO responsible for determining whether to approve or deny a request to view, handle, or otherwise deal with PHI and the criteria for determining the appropriate level of access to grant
- manner of documenting the decision approving or denying the request to view, handle, or otherwise deal with 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, including the required content of the documentation
- employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation, and to whom the documentation must be provided

At a minimum, the employee(s) and other person(s) acting on behalf of the PO responsible for determining whether to approve or deny a request for access to and use of PHI must be satisfied that:

- the employee(s) or other person(s) acting on behalf of the PO is required to view, handle, or otherwise deal with PHI received to develop or maintain the EHR on an ongoing basis or for a specified period for their employment, contractual, or other responsibilities
- the identified purpose for the viewing, handling, or otherwise dealing with PHI is required or permitted by PHIPA and its regulations

- the identified purpose for the viewing, handling, or otherwise dealing with PHI cannot reasonably be accomplished without PHI
- de-identified and/or aggregate information will not serve the identified purpose
- no more PHI will be viewed, handled, or otherwise dealt with 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 employee or other person acting on behalf of the PO granted approval to view, handle, or otherwise deal with PHI received to develop or maintain the EHR, 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 employee or other person acting on behalf of the PO is only required to view, handle, or otherwise deal with PHI for a specified period, the policy, procedures, and practices must set out the process to be followed in ensuring that the viewing, handling, or otherwise dealing with PHI is permitted only for that specified time period.

All approvals granted to view, handle, or otherwise deal with PHI should be subject to an automatic expiry, following which an employee or other person acting on behalf of the PO must again be required to request approval to view, handle, or otherwise deal with 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 employee(s) or other person(s) acting on behalf of the PO should seek re-approval annually.

The policy, procedures, and practices must also prohibit employee(s) or other person(s) acting on behalf of the PO from:

- viewing, handling, or otherwise dealing with PHI except as necessary for their employment, contractual, or other responsibilities
- viewing, handling, or otherwise dealing with PHI if other information will serve the identified purpose
- viewing, handling or otherwise dealing with more PHI than is reasonably necessary to meet the identified purpose

The PO must also ensure that all employees or other persons acting on behalf of the PO only view, handle, or otherwise deal with PHI as 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, employee(s) or other person(s) acting on behalf of the PO granted approval to view, handle, or otherwise deal with PHI received to develop or maintain the EHR are permitted to provide or disclose the information. This includes, but is not limited to, disclosures of PHI as directed by the Minister.

Notification and Termination of a Permission to View, Handle, or Otherwise Deal with Personal Health Information

The policy, procedures, and practices must require employee(s) or other person(s) acting on behalf of the PO who are granted approval to view, handle, or otherwise deal with PHI, or their supervisor, to notify the PO when the employee(s) or other person(s) are no longer employed, contracted, or otherwise retained by the PO, or no longer need to view, handle, or otherwise deal with PHI. In this regard, the policy, procedures, and practices must:

- set out the procedure to be followed in providing the notification
- identify the employee(s) and other person(s) acting on behalf of the PO 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, including the required content of the documentation
- identify the employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing the documentation
    - to whom the documentation must be provided
    - responsible for terminating the viewing, handling, or otherwise dealing with PHI
- set out the procedure to be followed in terminating the viewing, handling, or otherwise dealing with PHI
- specify the method by which the viewing, handling, or otherwise dealing with PHI will be terminated and the timeframe within which the viewing, handling, or otherwise dealing with the PHI must be terminated

The PO 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 employee(s) or other person(s) acting on behalf of the PO who are granted approval to view, handle, or otherwise deal with 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 Approval to View, Handle, or Otherwise Deal with Personal Health Information

The policy, procedures, and practices must:

- require the PO to maintain information with regard to the employee(s) and other person(s) acting on behalf of the PO who are granted approval to view, handle, or otherwise deal with PHI in such a manner that the PO can promptly generate a log from the information
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for maintaining the information
- address where documentation related to the receipt, review, approval, denial, or termination of the permission to view, handle, or otherwise deal with PHI is to be retained, and the employee(s) and other person(s) acting on behalf of the PO responsible for retaining this documentation

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

16. Log of Employees and Other Persons Acting on Behalf of the Prescribed Organization Granted Permission to View, Handle, or Otherwise Deal with Personal Health Information

A PO must maintain information with regard to the employee(s)s and other person(s) acting on behalf of the PO who are granted approval to view, handle, or otherwise deal with PHI. The information must be maintained in such a manner that the PO 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 employee(s)s and other person(s) acting on behalf of the PO permitted to view, handle, or otherwise deal with PHI
- types of PHI to which the employee(s)s and other person(s) acting on behalf of the PO are permitted to view, handle, or otherwise deal with PHI
- level or type of viewing, handling, or otherwise dealing with PHI granted

- date the permission was granted
- termination date or the date of the next audit of the viewing, handling, or otherwise dealing with PHI

Provision of Personal Health Information Pursuant to Direction

17. Policy, Procedures, and Practices for the Provision of Personal Health Information Pursuant to a Direction Issued by a Member of a Ministry Data Integration Unit or by the Minister

A policy, procedures, and practices must be developed and implemented for the provision or disclosure of PHI that is accessible by means of the EHR developed or maintained by the PO to a member of a ministry data integration unit ("MDIU") or another person pursuant to a direction issued under subsections 55.9(3) or 55.10(1) of PHIPA.

The policy, procedures, and practices must stipulate that the Minister or a member of a MDIU may issue a direction requiring the PO to provide or disclose PHI accessible by means of the EHR developed or maintained by the PO to the member of a MDIU for the purposes of subsection 55.9(1) of PHIPA or to another person for the purposes of subsection 55.10(1) of PHIPA.

The policy, procedures, and practices must stipulate that:

- the direction issued by the Minister or the member of the MDIU under subsection 55.9(3) or 55.10(1) of PHIPA may specify the form, manner, and timeframe in which the PHI accessible by means of the EHR developed or maintained by the PO that is the subject of the direction must be provided to the member of the MDIU or another person
- pursuant to subsections 55.9(3) and 55.10(3) of PHIPA, the PO is required to comply with a direction issued under subsection 55.9(3) or 55.10(1) of PHIPA

Receiving the Direction

The policy, procedures, and practices must:

- identify the employee(s) or other person(s) acting on behalf of the PO responsible for receiving a direction issued by the member of the MDIU or by the Minister under subsections 55.9(3) or 55.10(1) of PHIPA for the provision or disclosure of PHI that is accessible by means of the EHR developed or maintained by the PO
- set out the documentation that must be completed, provided, and/or executed, including the required content of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO:
    - responsible for completing, providing, executing, and ensuring the execution of the documentation
    - to whom this documentation must be provided

Implementing the Direction

The policy, procedures, and practices must:

- identify the employee(s) or other person(s) acting on behalf of the PO responsible for implementing a direction issued by the member of the MDIU or by the Minister for the provision or disclosure of PHI that is accessible by means of the EHR developed or maintained by the PO under subsections 55.9(3) or 55.10(1) of PHIPA
- require the employee(s) or other person(s) acting on behalf of the PO responsible for implementing the direction to ensure that the PHI that is accessible by means of the EHR that is the subject of a direction is provided in the form, manner, and timeframe specified in the direction
- specify the documentation that must be completed, provided, and/or executed, including the required content of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, ensuring the execution of the documentation, and to whom this documentation must be provided

Secure Transfer

The policy, procedures, and practices must require PHI that is accessible by means of the EHR developed or maintained by the PO that is subject to a direction by the member of the MDIU or by the Minister under subsections 55.9(3) or 55.10(1) of PHIPA, to be transferred in a secure manner in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal Health Information***.

Logging

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

- includes all directions issued by the member of the MDIU or by the Minister
- identifies the employee(s) or other person(s) acting on behalf of the PO responsible for maintaining such a log
- sets out where documentation related to the log of directions will be retained
- identifies the employee(s) or other person(s) acting on behalf of the PO responsible for retaining this documentation

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require the employee(s)s and other person(s) acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) and other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if they believe there may have been a breach of this policy, procedures, or practices

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

18. Log of Directions Issued by a Member of the Ministry Data Integration Unit or by the Minister

The PO must maintain a log of directions issued by a member of the MDIU or by the Minister under subsections 55.9(3) or 55.10(1) of PHIPA, with respect to PHI the PO receives to develop and maintain the EHR. At a minimum, the log must include:

- the date(s) the direction was issued
- the date(s) the direction was received
- whether the direction was issued under subsection 55.9(3) or 55.10(1) of PHIPA
- for a direction issued under subsection 55.10 (1) of PHIPA, specification of whether the information that is the subject of the direction was requested in accordance with clause 39(1)(c), subsection 39(2), section 44, or section 45 of PHIPA
- a description of the PHI that is the subject of the direction
- the form, manner, and timeframe in which the PHI that is the subject of the direction must be provided
- the name of the person or organization to whom the PHI must be provided
- the name(s) of the employee(s) or other person(s) acting on behalf of the PO:
    - who received the direction
    - responsible for completing the required documentation, if any, relating to the direction, and
    - responsible for implementing the direction and ensuring the PHI that is the subject of a direction is provided in the form, manner, and within the timeframe specified in the direction, and
- the date the PHI that is the subject of a direction was provided.

Requests for Access and Correction

19. Policies, Procedures, and Practices for Responding to Requests for Access and Correction of Records of Personal Health Information

Pursuant to subsection 51(5) of PHIPA, the PO must develop and implement a policy, procedures, and practices that that sets out the practices and procedures that enable the PO to respond to a request made by an individual under Part V of PHIPA to access or correct:

- a record of the individual's PHI that is accessible by means of the EHR, or
- the electronic records kept by the PO under paragraphs 4, 5, and 6 of section 55.3 of PHIPA

The policies, procedures, and practices must enable the PO to respond to an individual's request in accordance with Part V of PHIPA as though the PO were a custodian and as though the PO has custody or control of the records.

NOTE: At the time of publication of this Manual, subsection 51(5) of PHIPA had not yet been proclaimed. The requirements set out below that pertain to the prescribed organization's obligations pursuant to subsection 51(5) of PHIPA must not apply until such time as that subsection is proclaimed.

The PO must also develop and implement a policy, procedures, and practices that set out the practices and procedures that have been approved by the Minister for responding to or facilitating a response to an individual's request to a custodian under Part V of PHIPA to access or correct a record of their PHI that is accessible by means of the EHR.

Receiving and Reviewing Requests

The policy, procedures, and practices should:

- set out the process to be followed when receiving and reviewing requests to access or correct records of PHI that are accessible by means of the EHR
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for the process to be followed when receiving, reviewing, completing, providing, executing, and ensuring the execution of requests to access or correct the records of PHI
- set out the documentation that must be completed, provided, and/or executed, and the required content of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, ensuring the execution of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided

Responding to Requests

Access Requests

The policy, procedures, and practices must set out practices and procedures by which the PO will respond to an individual's access request in accordance with the provisions of Part V of PHIPA. In particular, the policy, procedures, and practices must address the PO's obligations with respect to each of the following, as applicable:

- making a determination as to whether:
    - Part V of PHIPA applies
    - the individual has a right of access to the requested record

- taking reasonable steps to be satisfied as to the identity of the requester
- consulting with a member of the College of Physicians and Surgeons of Ontario or a member of the College of Psychologists of Ontario regarding whether granting access could reasonably be expected to result in a risk of serious bodily harm to the treatment or recovery of the individual or risk of serious bodily harm to the individual or another person
- providing assistance to a requester to reformulate a request that does not contain sufficient detail to enable the PO to identify and locate the record
- providing a response to the requester, including, as applicable:
    - making the record available to the requester for examination or providing a copy of the record to the individual
    - giving the requester an explanation of any term, code or abbreviation used in the record
    - giving written notice that:
        - the PO has concluded that a record does not exist, cannot be found, or is not a record to which Part V of PHIPA applies
        - the PO is entitled to refuse the request, in whole or in part, and, where required by PHIPA, the reason for the refusal
        - the requester may make a complaint to the IPC
- providing a response within the timeframe required by PHIPA, including, as applicable:
    - making a decision to extend the time limit and providing notice of such decision to the requester
    - responding to a request by the requester for expedited access
- determining whether to charge the requester a fee, the quantum of any such fee, providing an estimate of the fee to the requester, and determining whether to waive any such fee

The policy, procedures, and practices must also set out the process to be followed with respect to each of the above obligations, including, as applicable:

- the employee(s) or other person(s) acting on behalf of the PO responsible for making a decision or implementing an action
- the process to be followed with respect to making a decision or implementing an action
- the requirements that must be satisfied and the criteria that must be considered with respect to any decision or action
- any documentation that must be completed, provided, and/or executed, and the required content of this documentation
- the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, ensuring the execution of the documentation

- the employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided

Correction Requests

The policy, procedures, and practices must set out practices and procedures by which the PO will respond to an individual's correction request in accordance with the provisions of Part V of PHIPA. In particular, the policy, procedures, and practices must address the PO's obligations with respect to each of the following, as applicable:

- making a determination as to whether the PO is required to correct the record
- correcting the record
- providing a response to the requester, including, as applicable giving written notice:
    - that the PO made the requested correction
    - that the PO refused to make the requested correction, and the reasons for the refusal
    - regarding the requester's rights with respect to a statement of disagreement, or
    - that the requester may make a complaint to the IPC
- applying a statement of disagreement
- giving written notice to any required person regarding the correction or statement of disagreement
- providing a response within the timeframe required by PHIPA, including, as applicable, a decision made to extend the time limit, and providing the requester with the decision

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

- the process to be followed with respect to each of the above obligations
- the employee(s) or other person(s) acting on behalf of the PO responsible for making a decision or implementing an action
- the process to be followed with respect to making a decision or implementing an action
- the requirements that must be satisfied and the criteria that must be considered with respect to any decision or action
- any documentation that must be completed, provided, and/or executed, and the required content of the documentation
- the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, and ensuring the execution of the documentation
- the employee(s) or other person(s) acting on behalf of the PO to whom the documentation must be provided

Facilitating a Response to Requests Received by a Custodian

The PO must have in place and comply with policies, procedures, and practices that have been approved by the Minister for responding or facilitating a response to a request made by an individual under Part V in respect of the individual's record of PHI that is accessible by means of the EHR. In this regard, the policy, procedures, and practices must:

- identify the employee(s) or other person(s) acting on behalf of the PO responsible for responding to or facilitating a response
- set out the process to be followed in responding to or facilitating a response
- specify any documentation that must be completed, provided, and/or executed, and set out the required content of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, and ensuring the execution of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided
- specify the format, manner, and timeframe within which a response must be facilitated

Where the PO must respond or facilitate a response to a request made by an individual to a custodian, the policy, procedures, and practices must:

- identify the employee(s) or other person(s) acting on behalf of the PO responsible for notifying the individual that the PO will be responding or facilitating a response to the request
- specify the process for notifying the individual
- specify the format, manner, and timeframe within which the individual must be notified
- set out any documentation that must be completed, provided, and/or executed, and the required content of this documentation
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, and ensuring the execution of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided

Notice to the Public

The policy, procedures, and practices must set out the information that must be provided to the public with respect to the individual's right to access and request correction of their records of PHI that are accessible by means of the EHR. At minimum, the information must include the:

- name and/or title, mailing address, and contact information for the employee(s) or other person(s) acting on behalf of the PO to whom requests for access or correction may be made
- manner and format in which these requests may be made

Tracking Requests

The policy, procedures, and practices must require that a log be maintained of all requests to access and correct records of PHI that are accessible by means of the EHR developed and maintained by the PO. The policy, procedures, and practices must identify:

- the employee(s) or other person(s) acting on behalf of the PO responsible for maintaining such a log
- where documentation relating to requests for access and correction will be retained
- the employee(s) or other person(s) acting on behalf of the PO responsible for retaining the documentation

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

20. Log of Access and Correction Requests

The PO must maintain a log of all requests for access and correction of records of PHI accessible by means of the EHR developed or maintained by the PO. At a minimum, the log must include each of the following, as applicable.

Where the PO responds in accordance with Part V of PHIPA to a request received from an individual, the log must include, at a minimum, the following:

- the date the request was received
- the name and contact information for the individual to whom the information relates
- the type of request (i.e., access or correction)
- a description of the request, including a description of the PHI that is the subject of the request

- the employee(s) or other person(s) acting on behalf of the PO who received and reviewed the request
- the names of any member of the College of Physicians and Surgeons of Ontario or member of the College of Psychologists of Ontario who were consulted regarding whether granting access could reasonably be expected to result in a risk of serious bodily harm to the treatment or recovery of the individual or risk of serious bodily harm to the individual or another person
- if the PO extended the time limit for responding, the reason for the extension, and the length of the extension
- if a request was made for expedited access, whether the request was granted
- the employee(s) or other person(s) acting on behalf of the PO responsible for deciding whether to grant the request
- the decision that was made (granted, granted in part, or refused)
- the reason for the refusal, where applicable
- the employee(s) or other person(s) acting on behalf of the PO responsible for communicating the decision to the individual
- the date the decision was communicated to the individual
- where a decision was made to grant the request, the employee(s) or other person(s) responsible for implementing the decision
- the date the decision was implemented
- the amount of fees charged to respond to the request, if any
- where a statement of disagreement is attached, the employee(s) or other person(s) acting on behalf of the PO responsible for receiving and attaching the statement of disagreement
- the date the statement of disagreement was attached
- the employee(s) or other person(s) acting on behalf of the PO responsible for notifying others about a correction or a statement of disagreement
- the date others were notified about a correction or a statement of disagreement

Where the PO responds to or facilitates a response to a request received by a custodian, the log must include all of the above, to the extent that they are known to the PO and, in addition, must include the following:

- the name and contact information for the custodian to whom the request was made
- a description of each decision that was made or action that was taken by the PO in responding to or facilitating the response.

Third-Party Service Provider Agreements

21. 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 PO prior to permitting TPSPs to view, handle, or otherwise deal with PHI received by the PO to develop or maintain the EHR
- require the written agreements to contain the relevant language from the ***Template Agreement for Third-Party Service Providers***
- identify the employee(s) and other person(s) acting on behalf of the PO 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 Provision and the Viewing, Handling, and Otherwise Dealing with Personal Health Information

The policy, procedures, and practices must state that only TPSPs contracted or otherwise engaged to provide services in or for the PO may be provided and are permitted to view, handle, or otherwise deal with the PHI received to develop or maintain the EHR.

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

- prohibit a TPSP from viewing, handling, or otherwise dealing with PHI if other information, namely de-identified and/or aggregate information, will serve the purpose, or from viewing, handling, or otherwise dealing with more PHI than is reasonably necessary to meet the purpose
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for making this determination
- ensure that TPSPs agree to comply with the restrictions and conditions that are necessary to enable the PO to comply with all of the requirements in section 55.3 of PHIPA
- prohibit TPSPs from viewing, handling, or otherwise dealing with PHI that the PO received from custodians to develop or maintain the EHR, unless the TPSP is permitted to do so in the TPSP Agreement and agrees to comply with the restrictions that apply to the PO
- maintain a detailed inventory of the records of PHI that are transferred to a TPSP, whose primary service is to retain or dispose of records of PHI outside the premises of the PO
- outline the process to be followed by the PO in auditing the TPSP's compliance with the agreement and must set out the manner and circumstances in which compliance will be audited and the notice, if any, that will be provided to the TPSP of the audit
- outline the consequences of a breaching 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 PO, 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, if any, records of PHI received by the PO to develop or maintain the EHR 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
    - employee(s) and other person(s) acting on behalf of the PO responsible for ensuring the secure transfer and retrieval of the records
    - require the records to be transferred in a secure manner in compliance with the ***Policy, Procedures, and Practices for Secure Transfer of Records of Personal 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 employee(s) and other person(s) acting on behalf of the PO 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 PO
- the identification of the employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for implementing the procedure and processes related to certificates of destruction
- 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 with the TPSP, including the:
    - employee(s) and other person(s) acting on behalf of the PO responsible for implementing this process
    - timeframe following the termination of the agreement within which this process must be implemented
    - employee(s) and other person(s) acting on behalf of the PO responsible for ensuring that any records of PHI that are transferred to a TPSP are either securely returned to the PO 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 the PO received from custodians to develop or maintain the EHR, the policy, procedures, and practices must further:

- require that a written agreement be executed with the TPSP containing the relevant language from the ***Template Agreement for Third-Party Service Providers***
- identify the employee(s) and other person(s) acting on behalf of the PO 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 the PO received from custodians to develop or maintain the EHR, or where a TPSP backs-up records of PHI the PO has contracted with the TPSP to retain, regardless of whether the TPSP uses remote-based (cloud) systems or on-premise systems.

Prohibition on Disclosure of Personal Health Information by the Third-Party Service Provider

The policy, procedures and practices must:

- require the PO to prohibit TPSPs contracted or otherwise engaged to provide services in or for the PO from disclosing PHI it receives to develop or maintain the EHR
- set out the processes and safeguards implemented to prevent a disclosure by TPSPs contracted or otherwise engaged to provide services in or for the PO
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for implementing the processes and safeguards

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 view, handle, or otherwise deal with PHI. The policy, procedures, and practices must further:

- identify the employee(s) and other person(s) acting on behalf of the PO responsible for maintaining such a log and for tracking the TPSP Agreements
- outline the process to be followed in tracking all TPSPs who are contracted or otherwise engaged to provide services in or for the PO who are permitted to view, handle, or otherwise deal with 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:
    - employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, executing, and ensuring the execution of the documentation
    - employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided
    - required content of the documentation
- outline the process to be followed and the employee(s) and other person(s) acting on behalf of the PO responsible for identifying TPSPs contracted or otherwise engaged to provide services in or for the PO who have not executed the agreement, and for ensuring that these TPSPs do so within a set timeframe
- indicate where documentation related to the execution of TPSP Agreements will be retained
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for retaining this documentation

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

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

22. Template Agreement for Third-Party Service Providers

A written **TPSP Agreement** must be entered into with TPSPs that will be permitted to view, handle, or otherwise deal with PHI provided to the PO to develop or maintain the EHR. 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 PO 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 PO under PHIPA and the duties and responsibilities arising from this status
- describe the authority under PHIPA and its regulation pursuant to which the PO is permitted to view, handle, or otherwise deal with PHI to develop or maintain the EHR and the duties and responsibilities imposed on the PO in this regard
- state whether or not the TPSP is an employee or other person acting on behalf of the PO in providing services pursuant to the agreement

All TPSPs that are permitted to view, handle, or otherwise deal with PHI in the course of providing services to the PO must be considered employees, or other persons acting on behalf of the PO, with the possible exception of **electronic service providers**. Agreements with electronic service providers must explicitly state whether or not the TPSP is also an employee or other person acting on behalf of the PO in providing services pursuant to the agreement.

If the TPSP is an employee or other person acting on behalf of the PO, the TPSP Agreement must require the TPSP to comply with the provisions of PHIPA and its regulations relating to the PO, including all requirements set out in section 55.3 of PHIPA, and to comply with the privacy and information security policies, procedures, and practices implemented by the PO in providing services pursuant to the agreement.

The TPSP Agreement must 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 view, handle, or otherwise deal with 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 persons acting on behalf of the TPSP.

Obligations with Respect to Viewing, Handling, or Otherwise Dealing with Personal Health Information

The **TPSP Agreement** must identify the limited and narrowly defined purposes for which the TPSP is permitted to view, handle, or otherwise deal with PHI received by the PO to develop or maintain the EHR and any limitations, conditions, or restrictions imposed thereon, including where a TPSP is not an employee or other person acting on behalf of the PO (i.e., a TPSP who acts solely as an **electronic service provider**).

In the case of a TPSP that is not an employee or other person acting on behalf of the PO, the TPSP Agreement must prohibit TPSPs from using PHI, except:

- as permitted in the TPSP Agreement
- for the purposes for which the PO is permitted to view, handle, or otherwise deal with PHI under PHIPA and its regulations
- as necessary in the course of providing services pursuant to the agreement or as required by law

In the case of a TPSP that is also an employee or other person acting on behalf of the PO, the TPSP Agreement must further:

- prohibit the TPSP from viewing, handling, or otherwise dealing with PHI if other information, such as de-identified and/or aggregate information, will serve the purposes identified in the agreement
- prohibit the viewing, handling, or otherwise dealing with more PHI than is reasonably necessary to meet the purposes identified in the agreement
- identify the one or more instance(s) where viewing, handling, or otherwise dealing with PHI is/are consistent with the viewing, handling, or otherwise dealing with PHI permitted by PHIPA and its regulations or another law

Prohibition on Disclosure

The TPSP Agreement must prohibit the TPSP contracted or otherwise engaged to provide services in or for the PO from disclosing PHI the PO receives from custodians.

Secure Transfer

The **TPSP Agreement** must identify the purposes for which and the circumstances in which, if any, records of PHI received by the PO may be transferred to the TPSP contracted or otherwise engaged to provide services in or for the PO, and transferred from the TPSP back to the PO, if any.

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

In particular, the TPSP Agreement must:

- specify the secure manner in which the records will be transferred

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

In identifying the secure manner in which records of 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 PO.

In addition, where the retention or disposal of records of PHI outside the premises of the PO is the primary service provided by the TPSP, the TPSP Agreement must require the TPSP to provide documentation to the PO setting out the date, time, and mode of transfer of the records of PHI and confirming receipt of records by the TPSP. 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 or otherwise engaged to retain records of PHI received by the PO to develop or maintain the EHR, the **TPSP Agreement** must require the TPSP to retain the records of PHI 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 provided to the PO to develop or maintain the EHR, having regard to the ***Policy, Procedures, and Practices for Secure Retention of Records of Personal Health Information*** implemented by the PO.

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 PO.

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
- 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 PO
- 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 PO. 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-premises systems.

Secure Return or Disposal of Records of Personal Health Information

Where the **TPSP Agreement** provides that records of PHI received by the PO to develop or maintain the EHR may be transferred to the TPSP contracted or otherwise engaged to provide services in or for the PO, the TPSP Agreement must address whether records of PHI will be securely returned to the PO or will be disposed of in a secure manner. At a minimum, the TPSP Agreement must require that records of PHI the PO 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
- employee or other person acting on behalf of the PO 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 PO.

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**

- the ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information*** implemented by the PO

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
- person(s) responsible for ensuring the secure disposal of the records

Certificate of Destruction

The **TPSP Agreement** must identify the:

- employee or other person acting on behalf of the PO to whom the **certificate of destruction** must be provided
- timeframe following secure disposal within which the certificate of destruction must be provided by the TPSP
- 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
- bear the name and signature of the person who performed the secure disposal

Implementation of Safeguards

The **TPSP Agreement** must require the TPSP contracted or otherwise engaged to provide services in or for the PO to take steps that are reasonable in the circumstances to ensure that the records of PHI subject to the agreement are viewed, handled, or otherwise dealt with 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 PO.

Training of Employees or Other Persons Acting on Behalf of the Third-Party Service Provider

The **TPSP Agreement** must require the TPSP contracted or otherwise engaged to provide services in or for the PO to:

- provide training to its employee(s) or other person(s) acting on behalf of the PO on the importance of protecting the privacy of individuals whose PHI is viewed, handled, or otherwise dealt with in the course of providing services pursuant to the agreement
- inform its employee(s) or other person(s) acting on behalf of the PO of the consequences that may arise in the event of a breach of these obligations
- ensure that its employee(s) or other person(s) acting on behalf of the PO who will view, handle, or otherwise deal with records of PHI are aware of and agree to comply with the terms and conditions of the agreement prior to viewing, handling, or otherwise dealing with the PHI

The TPSP Agreement must also set out the method by which this will be ensured. This should include requiring employees and other persons acting on behalf of the TPSP to sign an acknowledgement, prior to being permitted to view, handle, or otherwise deal with 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 contracted or otherwise engaged to provide services in or for the PO to subcontract the services provided under the agreement, the TPSP must be required to:

- acknowledge and agree that it will provide the PO 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 PO
- provide the PO with a right to obtain a copy of the written subcontracting agreement, upon request

Breach Notification to the Prescribed Organization

At a minimum, the **TPSP Agreement** must require the TPSP contracted or otherwise engaged to provide services in or for the PO to notify the PO at the first reasonable opportunity if:

- there has been a breach or suspected breach of the TPSP Agreement
- PHI viewed, handled, or otherwise dealt with by the TPSP on behalf of the PO is stolen, lost, or collected, used, or disclosed without authority, or
- PHI viewed, handled, or otherwise dealt with by the TPSP on behalf of the PO is believed to have been stolen, lost, 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 PO in its investigation.

Consequences of Breach and Monitoring Compliance

The **TPSP Agreement** must provide the PO 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 PO to request and obtain a copy of any independent audit of the TPSP's privacy and information security policies, procedures, and practices.

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

23. Log of Agreements with Third-Party Service Providers

A PO must maintain a log of executed agreements with TPSPs that are permitted to view, handle, or otherwise deal with PHI. At a minimum, the log must include:

- the name of the TPSP
- the nature of the services requiring the TPSP to view, handle, or otherwise deal with PHI on behalf of the PO
- the date that the TPSP Agreement was executed
- the date that the permission for the TPSP to begin to view, handle, or otherwise deal with the PHI, if any, was first provided
- the nature of the PHI that the TPSP is permitted to view, handle, or otherwise deal with in the course of providing the services
- the date of termination of the agreement with the TPSP
- the date the TPSP's viewing, handling, or otherwise dealing with records of PHI was terminated
- whether the records of PHI were transferred to the TPSP, and if so the nature of the records that were securely transferred and the date(s) of the secure transfer(s)
- whether the records of PHI, if any, will be securely returned or will be securely disposed of upon the termination of the agreement
- the date(s):
    - the records of PHI were securely returned
    - a **certificate of destruction** was provided, or by which records must be returned or disposed of
    - a TPSP's permission to view, handle, or otherwise deal with PHI was terminated
    - by which the records of PHI were returned

Privacy Impact Assessments

24. 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 must, at a minimum, ensure that the PO conducts privacy impact assessments:

- on each existing and proposed type of PHI that is being provided and for each type of PHI that is proposed to be requested or required by regulation to be provided to the PO to develop or maintain the EHR
- on each existing or whenever a new or a change to an existing information system, technology or program involving PHI that retrieves, processes, or integrates PHI that is accessible by means of the EHR developed or maintained by the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for making this determination
- ensuring that privacy impact assessments are in fact conducted, completed, reviewed, and amended, as necessary, and the employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- identify the employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided
- set out the required content of the documentation, including the criteria that must be used in making the determination that a privacy impact assessment is not to be conducted

Timing of Conducting and Reviewing Privacy Impact Assessments

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

- proposed types of PHI to be requested or required to be provided to the PO to develop or maintain the EHR 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, before the PHI is requested or required to be provided to the PO
    - reviewed and amended, if necessary, during the detailed design and implementation stage
- existing types of PHI provided to the PO, the policy, procedures, and practices must require:
    - a timetable be developed to ensure privacy impact assessments are conducted and updated, as and when necessary
    - the identification of the employee(s) and other person(s) acting on behalf of the PO 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 consistent with the information practices of the PO
- 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 information system, technology, or program at issue
- the nature and type of PHI collected, used, disclosed, retrieved, processed, or integrated, or that is proposed to be collected, used, disclosed, retrieved, processed, or integrated
- the sources of the PHI
- the purposes for which the PHI is collected, used, disclosed, retrieved, processed, or integrated, or is proposed to be collected, used, disclosed, retrieved, processed, or integrated
- 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 and/or the viewing, handling, or otherwise dealing with the PHI, if any
- 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 retrieved, processed, or integrated by the existing or proposed system, or will be retained, transferred, or disposed of
- the functionality for logging access, collection, use, modification, and disclosure of the PHI and the functionality to audit logs for unauthorized collection, use, or disclosure
- the risks to the privacy of individuals whose PHI is or will be retrieved, processed, or integrated by the existing or proposed system and an assessment of the risks
- recommendations to address and eliminate or reduce the privacy risks identified
- the administrative, technical, and physical safeguards implemented or proposed to be implemented to protect the PHI

For types of PHI that are or will be provided to the PO, the privacy impact assessment must describe the:

- types of PHI that are or will be provided to the PO to develop or maintain the EHR
- sources of the PHI that are or will be provided to the PO to develop or maintain the EHR
- statutory authority for the provision of the PHI to the PO, if any
- retention period for the types of PHI provided to the PO
- secure manner in which the records of PHI that are being provided to the PO are or will be retained, transferred, and disposed of
- functionality for logging access, use, modification, and disclosure of the PHI and the functionality to audit logs for unauthorized collection, use, or disclosure
- risks to the privacy of individuals whose PHI is or will be accessible by means of the EHR developed or maintained by the PO
- recommendations to address and eliminate or reduce the privacy risks identified
- 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 employee(s) and other person(s) acting on behalf of the PO responsible for:

- assigning other employee(s) and other person(s) acting on behalf of the PO to address the findings, mitigations, and any other relevant recommendations
- establishing timelines to address the mitigations, and any other recommendations
- monitoring and ensuring the treatment of the mitigations, and any other relevant recommendations within stated timelines
- evaluating the residual risks remaining after implementation

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

- privacy impact assessments that have been completed
- privacy impact assessments that have been undertaken, but that have not been completed
- privacy impact assessments that have not been undertaken
- The identification of the employee(s) and other person(s) acting on behalf of the PO 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 employees or other persons acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) or other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an employee or other person acting on behalf of the PO breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Privacy Audits***

25. Log of Privacy Impact Assessments

A PO 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 in respect of all systems that retrieve, process, or integrate PHI accessible by means of the EHR developed or maintained by the PO and for each type of PHI received by the PO to develop or maintain the EHR. The log must describe the:

- type of PHI at issue or the information system, technology, or program that retrieves processes, or integrates PHI that is at issue
- date that the privacy impact assessment was completed or is expected to be completed
- employee(s) and other person(s) acting on behalf of the PO responsible for completing or ensuring the completion of the privacy impact assessment
- findings, mitigations, and any other recommendations arising from the privacy impact assessment
- employee(s) and other person(s) acting on behalf of the PO responsible for addressing each mitigation and any other recommendations
- date that each mitigation or recommendation was or is expected to be addressed
- manner in which each recommendation was or is expected to be addressed

The PO must also maintain a log of systems that retrieve, process, or integrate PHI that is accessible by means of the EHR developed or maintained by the PO and of new, or changes to, existing information systems, technologies, or programs involving PHI, or for types of PHI received by the PO for which privacy impact assessments have not been undertaken. For each such type of PHI, information system, technology, or program, the log must set out the:

- description for the systems that retrieve, process, or integrate PHI that is accessible by means of the EHR developed or maintained by the PO or the types of PHI received by the PO at issue
- reasons that a privacy impact assessment will not be undertaken
- employee(s) or other person(s) acting on behalf of the PO responsible for making this determination
- date the determination was made

Privacy Audit Program

26. 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 in respect of PHI received by the PO to develop or maintain the EHR. 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 PO
- of the employee(s) and other person(s) acting on behalf of the PO permitted to view, handle, or otherwise deal with PHI pursuant to ***Policy, Procedures, and Practices for Viewing,***

Handling, or Otherwise Dealing with Personal Health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization

- of the employee(s) and other person(s) acting on behalf of the PO permitted to view, handle, or otherwise deal with PHI that has been de-identified or aggregated

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 employee(s) and other person(s) acting on behalf of the PO responsible for conducting the privacy audit
- establish the frequency with which and the circumstances in which each privacy audit is required to be conducted
- require a privacy audit schedule to be developed
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for developing the privacy audit schedule

At a minimum, audits of employees or other persons acting on behalf of the PO granted approval to view, handle, or otherwise deal with PHI must be conducted on an annual basis in accordance with the ***Policy, Procedures, and Practices for Viewing, Handling, or Otherwise Dealing with Personal Health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization***.

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

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

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

- assigning other employee(s) and other person(s) acting on behalf of the PO to address the mitigations, and any other recommendations as required
- establishing timelines to address the mitigations, and any other relevant recommendations
- monitoring and ensuring the treatment of mitigations, and any other recommendations within the stated timelines
- evaluating the residual risks remaining after implementation

Required Documentation

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

- documentation that must be completed, provided, and/or executed
- employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided
- required content of the documentation

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

- employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- employee(s) and other person(s) acting on behalf of the PO to whom the documentation must be provided
- required content of the documentation

Privacy Audit Findings

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

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

The policy, procedures, and practices must further:

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

- address where documentation related to privacy audits will be retained
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for retaining this documentation

Compliance, Audit, and Enforcement

The policy, procedures, and practices must require the employees and other persons acting on behalf of the PO responsible for conducting privacy audits to notify the PO, 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***.

27. Log of Privacy Audits

A PO 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
- employee(s) and other person(s) acting on behalf of the PO responsible for completing the privacy audit
- findings, mitigations, and other relevant recommendations arising from the privacy audit
- employee(s) and other person(s) acting on behalf of the PO responsible for addressing each recommendation
- date that each recommendation was or is expected to be addressed
- manner in which each recommendation was or is expected to be addressed

Privacy Breaches

28. 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 in respect of PHI received by the PO to develop or maintain the EHR.

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 accessible by means of the EHR developed or maintained by the PO that is not in compliance with PHIPA or its regulations
- the viewing, handling, or otherwise dealing with PHI that is not in compliance with PHIPA or its regulations
- a contravention of the privacy policies, procedures, or practices implemented by the PO, related to the requirements of the Manual

- a contravention of written acknowledgments, **Confidentiality Agreements** and **TPSP Agreements**, related to the requirements of the Manual, including written acknowledgements acknowledging and agreeing not to use PHI, which has been de-identified and/or aggregated, to identify an individual
- circumstances where PHI accessible by means of the EHR developed or maintained by the PO is stolen, lost, 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 PO must have regard to the guidelines produced by the IPC entitled **Responding to a Health Privacy Breach: Guidelines for the Health Sector** and any directions issued by the Minister.

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 employees or other persons acting on behalf of the PO. At a minimum, the policy, procedures, and practices must indicate that privacy breaches or suspected privacy breaches will be identified through notifications, including by employees or other persons acting on behalf of the PO, custodians that collect, use, and disclose PHI that is accessible by means of the EHR, privacy audits, and privacy complaints and inquiries.

The policy, procedures, and practices must require that employee(s) or other person(s) acting on behalf of the PO notify the PO of a privacy breach or suspected privacy breach at the first reasonable opportunity. The policy, procedures, and practices must:

- identify the employee(s) and other person(s) acting on behalf of the PO who must be notified of the privacy breach or suspected privacy breach and must provide their contact information
- specify the timeframe within which notification must be provided
- stipulate whether the notification must be provided orally and/or in writing and the nature of the information that must be included within the notification
- address the documentation and its required contents that must be completed, provided, and/or executed with respect to notification, including the employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing the documentation
    - to whom this documentation must be provided.

Privacy Breaches Caused by One or More Health Information Custodian(s)

The policy, procedures, and practices must specify that where the PO identifies a privacy breach or suspected privacy breach that was caused by one or more custodian(s), the PO must:

- report the privacy breach or suspected privacy breach to the custodian(s), and
- document requirements for instances where the Minister requests or directs the PO to cooperate with the custodian(s) to develop and/or implement a policy and procedures to:
    - determine whether a privacy breach has in fact occurred
    - contain, investigate, and remediate a privacy breach that has been confirmed
    - notify individuals in circumstances where the privacy breach or suspected privacy breach was caused by one or more custodian(s)

The policy, procedures, and practices must also:

- specify that the PO must assist custodians to determine, contain, investigate, remediate, or notify affected individuals of a privacy breach, when requested or directed to do so by the Minister
- set out the role of the PO in assisting custodians in fulfilling their obligations to notify individuals under subsections 12(2) and 55.5(7) of PHIPA. In this regard, the PO must take into consideration any directions issued by the Minister

Privacy Breaches Caused by the Prescribed Organization or an Unauthorized Person

The policy, procedures and practices must require the PO to take the following steps in any instance in which a privacy breach or suspected privacy breach is caused by:

- one or more employee(s) or other person(s) acting on behalf of the PO
- a system that retrieves, processes, or integrates PHI that is accessible by means of the EHR, or
- an unauthorized person who is neither an employee or other person acting on behalf of the PO nor an agent of a custodian

Determination of Whether a Privacy Breach Occurred

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

- whether a privacy breach has in fact occurred, and if so, what, if any, PHI accessible by means of the EHR has been breached
- the extent of the privacy breach
- whether the breach is a privacy breach, or an information security breach, or both
- the identification of the employee(s) and other person(s) acting on behalf of the PO responsible for making this determination

Prioritization Framework

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

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

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

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

Breach Notification to Senior Management

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

- identifying the employee(s) and other person(s) acting on behalf of the PO responsible for notifying senior management
- the timeframe within which notification must be provided
- the manner in which this notification must be provided
- the nature of the information that must be provided to senior management upon notification, including the level of detail that must be provided

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

The policy, procedures, and practices must address the process to be followed in identifying, reporting, containing, notifying, investigating, and remediating an event that is both a **privacy breach** or a 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 employee(s) and other person(s) acting on behalf of the PO responsible for containment and the procedure that must be followed, including any documentation and the required content of the documentation that must be completed, provided, and/or executed by the employee(s) and other person(s) acting on behalf of the PO responsible for containing the breach.

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 being further viewed, handled, or otherwise dealt with without authority, and to protect records of PHI accessible by means of the EHR 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
- 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
- if necessary, an acknowledgement of any further action(s) 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
- employee(s) and other person(s) acting on behalf of the PO responsible for reviewing the containment measures
- documentation that must be completed, provided, and/or executed in reviewing the containment measures, included the required content of the documentation

- employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and executing the documentation
- employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided

Breach Notification to Custodians or Other Organizations

The policy, procedures, and practices must require the PO to notify, at the first reasonable opportunity, the custodian(s) that provided the PHI to the PO to develop or maintain the EHR, 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:

- employee(s) and other person(s) acting on behalf of the PO responsible for notifying the custodians or other organization
- format of the notification
- nature of the information that must be provided upon notification
- timeframe for 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
- further actions that will be undertaken with respect to the privacy breach, including investigation and remediation
- the role of the PO in assisting custodians in fulfilling their obligations to notify individuals under subsections 12(2) and 55.5(7) of PHIPA, including the PO's consideration of any directions issued by the Minister in this regard

Breach Notification to the Information and Privacy Commissioner

At a minimum, the policy, procedures, and practices must require the PO to notify the IPC, in writing, immediately after becoming aware that PHI that is accessible by means of the EHR has been:

- viewed, handled, or otherwise dealt with by the PO or a TPSP contracted or otherwise engaged by the PO other than in accordance with PHIPA or its regulations, or
- made available or released by the PO or a TPSP contracted or otherwise engaged by the PO, other than in accordance with PHIPA and its regulations

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:

- employee(s) and other person(s) acting on behalf of the PO responsible for providing such notification
- format of the notification
- nature of the information that must be provided upon notification
- timeframe for notification

Breach Notification to Affected Individuals

However, as a recipient of PHI, a PO 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).

The policy, procedures and practices must set out the role of the PO in assisting custodians in fulfilling their obligations to notify individuals under subsections 12 (2) and 55.5 (7) of PHIPA. In this regard, the PO must take into consideration any directions issued by the Minister.

Investigation of Breach

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

- employee(s) or other person(s) acting on behalf of the PO 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
    - employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
    - employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided
    - required content of the documentation

The policy, procedures, and practices must also identify the employee(s) and other person(s) acting on behalf of the PO responsible for:

- assigning other employee(s) and other person(s) acting on behalf of the PO to address the mitigations, and any other relevant recommendations as required

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

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

- employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- employee(s) and other person(s) acting on behalf of the PO to whom the documentation must be provided
- required content of the documentation

Communication of Findings of Investigation and Recommendations

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

- the employee(s) and other person(s) acting on behalf of the PO responsible for communicating the findings of the investigation
- the mechanism and format for communicating the findings of the investigation, including the level of detail for communicating the findings
- the timeframe within which the findings of the investigation must be communicated
- to whom the findings of the investigation must be communicated, including whether the findings must be communicated to the chief executive officer or the executive director (or equivalent position)

Tracking Privacy Breaches

The policy, procedures, and practices must:

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

29. Log of Privacy Breaches

A PO must maintain a log of **privacy breaches** and suspected privacy breaches in respect of PHI accessible by means of the EHR developed or maintained by the PO. At a minimum, the log must set out each of the following, to the extent that they are known to the PO:

- 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, without providing any PHI
- a description of the privacy breach or suspected privacy breach and the manner in which the privacy breach or suspected privacy breach was identified, and by whom
- the cause of the privacy breach or suspected privacy breach
- where the cause of the privacy breach or suspected privacy breach is one or more custodian(s), the name of each:
    - custodian
    - custodian whose agent(s) or electronic service provider(s) caused the privacy breach or suspected privacy breach, or
    - agent and electronic service provider of the custodian that caused the privacy breach or suspected privacy breach, if applicable
- where the cause of the privacy breach or suspected privacy breach is the PO, the:

    - system that retrieves, processes, or integrates PHI that is accessible by means of the EHR developed or maintained by the PO, or
    - name of each employee and other person acting on behalf of the PO that caused the privacy breach, if applicable
- where the cause of the privacy breach or suspected privacy breach is not an employee or other person acting on behalf of the PO, or an agent or electronic service provider of a custodian caused the privacy breach or suspected privacy breach and the name or a description of the unauthorized person, if applicable
- the name of each custodian that provided the PHI to the PO
- 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, the employee(s) and other person(s) acting on behalf of the PO responsible for containing the privacy breach or suspected privacy breach, and the nature of the containment measures
- the name of the employee(s) and other person(s) acting on behalf of the PO or the name of the agent(s) of the custodian(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 employee(s) and other person(s) acting on behalf of the PO responsible for conducting the investigation
- the findings, mitigations, and other relevant recommendations arising from the investigation
- the employee(s) and other person(s) acting on behalf of the PO 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(s) that notification was provided to affected custodian(s), if applicable
- the date(s) that notification was provided to the IPC, if applicable
- the date(s) that the findings of the investigation and the measures taken, if any, in response to the privacy breach or suspected privacy breach were provided to affected individuals, if applicable

Privacy Complaints and Inquiries

30. 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** in respect of PHI accessible by means of the EHR developed or maintained by the PO. A definition of the term "privacy complaint" must be provided that, at a minimum, includes concerns or complaints relating to compliance of a custodian or the PO with the privacy policies, procedures, and practices implemented by the PO or 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 employee(s) and other person(s) acting on behalf of the PO to whom concerns or complaints may be directed
- information related to the manner and format in which privacy concerns or complaints may be directed to the PO
- information advising individuals that they may make a complaint to the IPC regarding the PO's compliance with PHIPA and its regulations
- the mailing address and contact information for the IPC

Process for Receiving Complaints

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

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

Complaint Relates to One or More Health Information Custodians

The policy, procedures, and practices must, where the PO receives a privacy complaint related to one or more custodian(s), or to agent(s) or electronic service provider(s) of one or more custodian(s):

- specify that the PO must forward the privacy complaint to the custodian(s) and require the PO to respond in writing to the complainant:
    - acknowledging receipt of the privacy complaint

    - advising that the privacy complaint has been forwarded to one or more custodian(s)
    - providing contact information for the custodian(s) to whom the complaint was forwarded
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for sending the above noted written communication to the complainant(s)
- set out the timeframe within which the communication will be sent to the individuals

The policy, procedures, and practices must specify that, when requested to do so or directed to do so by the Minister, the PO must:

- assist custodians in developing a policy and procedures to determine whether to investigate a privacy complaint
- investigate and remediate the privacy complaint in circumstances where the privacy complaint relates to more than one custodian(s), or to one or more agent(s) or electronic service provider(s) of more than one custodian, if required
- assist custodians to determine whether to investigate a privacy complaint
- assist in investigating and remediating the privacy complaint in circumstances where the privacy complaint relates to one or more custodian(s), or to an agent(s) or electronic service provider(s) of one or more custodians, if applicable

Complaint Relates to the Prescribed Organization or an Unauthorized Person

The policy, procedures, and practices must require the PO to take the following steps in any instance in which a privacy complaint is received relating to:

- employee(s) or other person(s) acting on behalf of the PO
- a system that retrieves, processes, or integrates PHI that is accessible by means of the EHR, or
- an unauthorized third-party who is not an employee or other person acting on behalf of the PO or an agent of a custodian

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:

- employee(s) and other person(s) acting on behalf of the PO responsible for making this determination
- timeframe within which this determination must be made
- process that must be followed to make the determination
- criteria that must be used in making the determination, including any documentation that must be completed, provided, and/or executed

- required content of the documentation

Where Complaint Will Not Be Investigated

In the event that it is determined that an investigation will not be undertaken, the policy, procedures, and practices must require the PO to provide a letter 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 PO has contravened or is about to contravene PHIPA or its regulations
- the contact information for the IPC

Where Complaint Will Be Investigated

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

- an acknowledgment of receipt of the **privacy complaint**
- advising that an investigation of the privacy complaint will be undertaken
- an explanation of the privacy complaint investigation procedure
- an indication of whether the complainant will be contacted for further information concerning the privacy complaint
- the projected timeframe for completion of the investigation
- 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 employee(s) and other person(s) acting on behalf of the PO responsible for sending the above noted letters to complainants, and the timeframe within which the letters will be sent.

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

- employee(s) and other person(s) acting on behalf of the PO responsible for investigating the privacy complaint
- nature and scope of the investigation (i.e., document reviews, interviews, site visits, inspections)
- process that must be followed in investigating the privacy complaint

- documentation that must be completed, provided, and/or executed in undertaking the investigation, including the:
    - employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
    - employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided
    - required content of the documentation

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

- assigning other employee(s) and other person(s) acting on behalf of the PO to address the mitigations, and any other relevant recommendations
- establishing timelines to address the mitigations, and any other recommendations
- monitoring and ensuring the treatment of the mitigations, and any other relevant recommendations within the stated timelines
- evaluating the residual risks remaining after implementation

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

- employee(s) and other person(s) acting on behalf of the PO responsible for completing, preparing, and/or executing the documentation
- employee(s) and other person(s) acting on behalf of the PO to whom the documentation must be provided
- required content of the documentation

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

- identifying the employee(s) and other person(s) acting on behalf of the PO responsible for communicating the findings of the investigation
- the mechanism and format for communicating the findings of the investigation, including the level of detail for communicating the findings
- the timeframe within which the findings of the investigation must be communicated
- to whom the findings must be communicated, including whether the findings must be communicated to the chief executive officer or the executive director (or equivalent position)

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

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

The policy, procedures, and practices must also identify the employee(s) and other person(s) acting on behalf of the PO 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
- employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for maintaining the log and for tracking the findings
- assess whether the mitigations, and other relevant recommendations arising from the investigation of privacy complaints are addressed within the identified timelines
- specify where documentation related to the receipt, investigation, notification, and remediation of privacy complaints will be retained
- detail the employee(s) and other person(s) acting on behalf of the PO responsible for retaining the documentation

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require employees or other persons acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) or other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Privacy Breach Management***, if an employee or other person acting on behalf of the PO breaches or believes there may have been a breach of this policy, procedures, or practices

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

Relationship to Other Policies, Procedures, and Practices

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

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

31. Log of Privacy Complaints

A PO must maintain a log of **privacy complaints** in respect of PHI accessible by means of the EHR developed and maintained by the PO. At a minimum, the log must set out each of the following, to the extent that they are known to the PO:

- the date that the privacy complaint was received
- the nature of the privacy complaint
- the custodian(s) to whom the privacy complaint was forwarded and the date the privacy complaint was forwarded, if applicable
- the date the individual was advised that the privacy complaint was forwarded to one or more custodian(s), if applicable
- the determination as to whether the privacy complaint will be investigated by the PO and the date that the determination was made
- the employee(s) and other person(s) acting on behalf of the PO and/or the agent(s) of a custodian who made the determination as to whether the privacy complaint would be investigated
- where the determination was made that the privacy complaint will not be investigated, the date that the complainant was advised that the complaint will not be investigated and informed of their right to file their complaint with the IPC
- where the determination is made that the privacy complaint will be investigated:
    - the date that the complainant was advised that the complaint will be investigated
    - the employee(s) and other person(s) acting on behalf of the PO and/or the agent(s) of a custodian 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 employee(s) and other person(s) acting on behalf of the PO and/or the agent(s) of a custodian responsible for addressing each recommendation
- the date that each recommendation was or is expected to be addressed
- the manner in which each recommendation was or is expected to be addressed
- the date that the complainant was advised of the findings of the investigation, the measures taken, if any, in response to the privacy complaint, and of their right to file a complaint with the IPC

32. 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 in respect of PHI that is accessible by means of the EHR developed or maintained by the PO. A definition of the term “privacy inquiry” must be provided that, at a minimum, includes inquiries relating to compliance of a custodian or the PO with PHIPA and its regulations, or with the privacy policies, procedures, and practices implemented by custodians or the PO in relation to PHI that is accessible by means of the EHR developed or maintained by the PO.

The information that must be communicate to the public relating to the manner in which, to whom, and where individuals may direct privacy inquiries must also be identified. At a minimum, the information communicated to the public must include:

- the name and/or title, mailing address, and contact information of the employee(s) and other person(s) acting on behalf of the PO to whom privacy inquiries may be directed
- the manner in which privacy inquiries may be made
- information as to where individuals may obtain further information about the privacy policies, procedures, and practices implemented by custodians or the PO

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

- the employee(s) and other person(s) acting on behalf of the PO responsible for receiving and responding to privacy inquiries
- the role of the employee(s) and other person(s) acting on behalf of the PO who have been delegated day-to-day authority to manage the privacy program and the information security program must also be identified
- any documentation that must be completed, provided, and/or executed

- the required content and format of the documentation the PO would issue in response to a privacy inquiry

Inquiry Relates to One or More Health Information Custodians

The policy, procedures, and practices must:

- specify that where the PO receives a privacy inquiry related to one or more custodian(s), the PO must forward the privacy inquiry to the custodian(s) to whom the inquiry relates
- explain that where the PO forwards the privacy inquiry to one or more custodian(s), the PO must respond in writing to the individual making the privacy inquiry:
    - acknowledging receipt of the privacy inquiry
    - advising that the privacy inquiry has been forwarded to one or more custodian(s)
    - providing contact information for the custodian(s) to whom the inquiry was forwarded
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for sending written communication to individuals making privacy inquiries and the timeframe within which the communication will be sent to the individuals
- specify that, when requested to do so or directed to do so by the Minister, the PO must assist custodians by leading or assisting with the development and/or the implementation of policy, procedures, and practices to respond to inquiries in circumstances where the privacy inquiries relate to one or more custodian(s) that provide PHI to the PO to develop or maintain the EHR

Inquiry Relates to the Prescribed Organization or an Unauthorized Person

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

- employee(s) or other person(s) acting on behalf of the PO
- a system that retrieves, processes, or integrates PHI accessible by means of the EHR developed or maintained by the PO or
- an unauthorized third-party who is not an employee or other person acting on behalf of the PO or an agent of a custodian

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

- set out the employee(s) or other person(s) acting on behalf of the PO responsible for receiving and responding to privacy inquiries
- specify the documentation that must be completed, provided, and/or executed and the required content of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, and ensuring the execution of documentation
- identify the format and content of the response to the individual making the privacy inquiry

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

Relationship to Policy, Procedures, and Practices for Privacy Complaints

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

Part 2 - Information Security Policies, Procedures, and Practices

The PO must take steps that are reasonable in the circumstances to ensure that PHI the PO receives to develop or maintain the EHR 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 also 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 not permitted by PHIPA or another Act).

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 PO to develop or maintain the EHR under PHIPA and its regulations. The information security policy must require steps to be taken that are reasonable in the circumstances to ensure that the PHI accessible by means of the EHR is protected against theft, loss, and unauthorized collection, use, or disclosure and to ensure that the records of PHI accessible by means of the EHR are protected against unauthorized copying, modification, or disposal.

Threat and Risk Assessment

The information security policy must also:

- require the PO to undertake comprehensive and organization-wide threat and risk assessments of all **information security components** used to develop or maintain the EHR, including for each system that retrieves, processes, or integrates PHI that is accessible by means of the EHR, as well as appropriate project specific threat and risk assessments involving such PHI
- 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
- address the duties and responsibilities of employee(s) or other person(s) acting on behalf of the PO 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 received to develop or maintain the EHR are retained, viewed, handled, or otherwise dealt with by the PO
- 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 the 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 the protection against network intrusions, phishing attacks, and malicious code
- 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 PO, 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
- 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 the PHI accessible by means of the EHR developed or maintained by the PO. 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 the employee(s) or other person(s) acting on behalf of the PO to comply with the policy, procedures, and practices and with all other information security policies procedures, and practices
- require employee(s) or other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if the employee or other person acting on behalf of the PO breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of 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 implemented by the PO pursuant to PHIPA and its regulations. 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 pursuant to section 55.12 of PHIPA
    - whenever the Minister issues a directive to the PO with respect to the carrying out of its responsibilities and functions
- employee(s) or other person(s) acting on behalf of the PO responsible, and the procedure, for:
    - undertaking the review, including the timeframe in which the review will be undertaken
    - amending, and/or drafting new information security policies, procedures, and practices, if deemed necessary as a result of the review
    - 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
    - communicating the amended or newly developed information security policies, procedures, and practices
- method and nature of the communication to employee(s) or other person(s) acting on behalf of the PO, the public, each custodian that provided PHI to the PO to develop or maintain the EHR, 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 PO must have regard to:

- any directives issued by the Minister with respect to the carrying out of its responsibilities and functions
- 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 PO
- 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 PO continue to be consistent with its actual practices

- 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 employees or other persons acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) or other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if an employee or other person acting on behalf of the PO breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of 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 PO to protect PHI accessible by means of the EHR against theft, loss, and unauthorized collection, use, or disclosure and to protect records of PHI accessible by means of the EHR 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 PO are required to adhere to the same physical safeguards. The policy, procedures, and practices should ensure that the premises of the PO 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 Employees and Other Persons Acting on Behalf of the Prescribed Organization

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 employee(s) or other person(s) acting on behalf of the PO 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 employee(s) or other person(s) acting on behalf of the PO responsible and procedure for the ongoing review of employee(s) or other person(s) acting on behalf of the PO granted access to locations within the premises where records of PHI are retained
- identify the employee(s) or other person(s) acting on behalf of the PO 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
- 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 employee(s) or other person(s) acting on behalf of the PO to whom the documentation must be provided

The policy, procedures, and practices must address the criteria that must be considered by the employee(s) or other person(s) acting on behalf of the PO 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 employee(s) or other person(s) acting on behalf of the PO who routinely require such access for their employment, contractual, or other responsibilities.

At a minimum, the criteria considered by the employee(s) or other person(s) acting on behalf of the PO must ensure that access is only provided to employee(s) or other person(s) acting on behalf of the PO:

- who are employed, contracted, or otherwise engaged to provide services in or for the PO
- who are required to view, handle, or otherwise deal with PHI received by the PO to develop and maintain the EHR
- whose use of the PHI is permitted by PHIPA and its regulations and by the ***Policy, Procedures, and Practices for Viewing, Handling, or Otherwise Dealing with Personal Health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization***

In the event that an employee or other person acting on behalf of the PO 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:

- employee(s) or other person(s) acting on behalf of the PO 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
- process to be followed and documentation that must be completed, provided, and/or executed, including the:
    - employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, and/or receiving the documentation
    - required content of the documentation

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

The policy, procedures, and practices must require employees or other persons acting on behalf of the PO to notify the PO 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:

- employee(s) and other person(s) acting on behalf of the PO to whom the notification must be provided
- nature and format of the notification
- documentation that must be completed, provided, and/or executed
- employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided
- 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 employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for their issuance

- set out any documentation that must be completed, provided, and/or executed, including the required content of the documentation
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- identify the employee(s) and other person(s) acting on behalf of the PO to whom the documentation must be provided
- identify the employee(s) or other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for implementing the process to be followed in the event of non-return
- the timeframe within which this process must be implemented

Termination of the Employment, Contractual or Other Relationship

The policy, procedures, and practices must require employee(s) and other person(s) acting on behalf of the PO, as well as their supervisors, to:

- notify the PO of the termination or cessation of their employment, contractual, or other relationship with the PO
- return their identification cards, access cards, and/or keys to the PO on or before the date of termination or cessation 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***
- 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 employee(s) or other person(s) acting on behalf of the PO granted approval to access location(s) where records of PHI are retained, or their supervisor, to notify the PO when the employee(s) or other person(s) acting on behalf of the PO no longer require such access. In this regard, the policy, procedures, and practices must:

- set out the procedure to be followed in providing the notification
- identify the employee(s) or other person(s) acting on behalf of the PO 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, including the required content of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing this documentation
- identify the employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for terminating access to the PHI
- set out the procedure to be followed in terminating access
- specify the method by which access will be terminated and the timeframe within which access to the PHI must be terminated

Audits of Employees or Other Persons Acting on behalf of the Prescribed Organization with Access to the Premises

Audits must be conducted of employee(s) and other person(s) acting on behalf of the PO with access to the premises of the PO 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 employee(s) and other person(s) acting on behalf of the PO 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 in or for the PO
- be routinely required to use PHI received by the PO for the purpose of developing and maintaining the EHR
- require the same level of access to the PHI

In this regard, the policy, procedures, and practices must identify the employee(s) or other person(s) acting on behalf of the PO 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. At a minimum, these audits must be conducted annually.

Tracking and Retention of Documentation Related to Access to the Premises

The policy, procedures, and practices must:

- require that a log be maintained of employee(s) or other person(s) acting on behalf of the PO granted approval to access the premises of the PO and to locations within the premises where records of PHI are retained, and identify the employee(s) or other person(s) acting on behalf of the PO responsible for maintaining such a log
- 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

- identify the employee(s) or other person(s) acting on behalf of the PO responsible for maintaining this documentation

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

The policy, procedures, and practices must address the employee(s) or other person(s) acting on behalf of the PO responsible and the process to be followed in identifying, screening, and supervising visitors to the premises of the PO. At a minimum, the policy, procedures, and practices must set out the:

- identification that is required to be worn by visitors
- documentation that must be completed, provided, and/or executed by employee(s) or other person(s) acting on behalf of the PO responsible for identifying, screening and supervising visitors
- 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
- the name of the employee(s) or other person(s) acting on behalf of the PO with whom the visitors are meeting

The duties of employee(s) or other person(s) acting on behalf of the PO 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 PO
- the identification is returned prior to departure
- 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 their date and time of departure
- employee(s) or other person(s) acting on behalf of the PO responsible for implementing and maintaining the identified process
- location where documentation related to the identification, screening, and supervision of visitors will be retained
- employee(s) or other person(s) acting on behalf of the PO responsible for retaining this documentation

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

6. Log of Employees or Other Persons Acting on behalf of the Prescribed Organization with Access to the Premises of the Prescribed Organization

A log must be maintained of employee(s) or other person(s) acting on behalf of the PO granted approval to access the premises of the PO and the level of access granted. At a minimum, the log must include the name of the employee(s) or other person(s) acting on behalf of the PO granted approval to access the premises, and for each employee or other person acting on behalf of the PO, 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 employee or other person acting on behalf of the PO
- identification numbers on the identification cards, access cards, and/or keys, if any
- date of the next audit of access
- date that the identification cards, access cards, and/or keys were returned to the PO, 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 accessible by means of the EHR developed or maintained by the PO, 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 of PHI be retained for only as long as necessary to develop or maintain the EHR.

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 employee(s) and other person(s) acting on behalf of the PO 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 employee(s) or other person(s) acting on behalf of the PO to take steps that are reasonable in the circumstances to ensure that records of PHI accessible by means of the EHR are protected against theft, loss, unauthorized use or disclosure, and against unauthorized copying, modification, or disposal
- outline the reasonable steps that must be taken by the employee(s) or other person(s) acting on behalf of the PO

Third-Party Service Providers

If a TPSP is contracted or otherwise engaged to retain records of PHI on behalf of the PO, 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 employee(s) or other person(s) acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) or other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if an employee or other person acting on behalf of the PO breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices

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

8. Policy, Procedures, and Practices for Secure Retention of 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 PO permits PHI received to develop or maintain the EHR, to be 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 PO does not permit PHI to be retained, transferred, and/or disposed of on a mobile device, the policy and procedures must:

- explicitly prohibit such retention, transfer, and/or disposal
- indicate whether or not PHI may be accessed remotely through a secure connection or virtual private network
- explicitly prohibit such remote access if the PO 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***
- evolving privacy and information security standards and best practices

Where Personal Health Information is Permitted to be Retained, Transferred, and/or Disposed of on a Mobile Device

If the PO permits PHI received to develop or maintain the EHR, to be 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 PO.

Approval Process

The policy, procedures, and practices must state whether approval is required prior to 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 employee(s) and other person(s) acting on behalf of the PO responsible for receiving, reviewing, and determining whether to approve or deny a request for the retention, transfer, and/or disposal of PHI on a mobile device
- set out the documentation that must be completed, provided, and/or executed, including the required content of the documentation
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO to whom this documentation must be provided and the required content of the documentation
- set out the manner of documenting decisions approving or denying the requests
- 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 employee(s) and other person(s) acting on behalf of the PO responsible for determining whether to approve or deny a request for the retention, transfer, and/or disposal of PHI on a mobile device.

At a minimum, prior to any approval of a request to retain, transfer, and/or dispose of PHI on a mobile device, the policy, procedures, and practices must require the employee(s) and other person(s) acting on behalf of the PO 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 retained, transferred, and/or disposed of on the mobile device than is reasonably necessary to meet the identified purpose
- the viewing, handling or otherwise dealing with the PHI has been approved pursuant to the ***Policy, Procedures, and Practices for Viewing, Handling, or Otherwise Dealing with Personal health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization***

Conditions or Restrictions on the Retention, Transfer, and/or Disposal of Personal Health Information 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 Passwords***
- require a mandatory standardized password-protected device lock-out be enabled after a defined period of inactivity
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for encrypting mobile devices and for ensuring that the mandatory standardized password-protected device lock-out is enabled
- describe the technical administration of mobile devices that 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 PO

Where a mobile device is not under the PO's administrative control, the PO 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 retain, transfer, or dispose of PHI.

The policy, procedures, and practices must further identify the conditions or restrictions with which employee(s) and other person(s) acting on behalf of the PO granted approval to retain, transfer, and/or dispose of PHI on a mobile device must comply. At a minimum, employee(s) and other person(s) acting on behalf of the PO must:

- be prohibited from 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 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
- 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 employee(s) and other person(s) acting on behalf of the PO to protect the PHI 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 employee(s) and other person(s) acting on behalf of the PO 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***
- 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***

Where Personal Health Information is not Permitted to be Retained on a Mobile Device

If the PO does not permit PHI to be retained on a mobile device, the policy, procedures, and practices must expressly prohibit the retention of PHI on a mobile device and must indicate whether or not PHI received to develop or maintain the EHR may be accessed remotely through a secure connection or virtual private network.

Accessing PHI Through a Secure Connection or Virtual Private Network

If the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible and the process to be followed in 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 employee(s) and other person(s) acting on behalf of the PO 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, including the required content of the documentation
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO to whom the documentation must be provided
- set out the manner of documenting the decision approving or denying the request
- 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 employee(s) and other person(s) acting on behalf of the PO 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
- the viewing, handling, or otherwise dealing with the PHI has been approved pursuant to the ***Policy, Procedures, and Practices for Viewing, Handling, or Otherwise Dealing with Personal health information by Employees and Other Persons Acting on Behalf of the Prescribed Organization***

Conditions or Restrictions on the Remote Access to Personal Health Information

The policy, procedures, and practices must identify the conditions or restrictions with which employee(s) and other person(s) acting on behalf of the PO granted approval to access PHI remotely must comply, including in mobile and remote environments. At a minimum, the policy, procedures, and practices must:

- prohibit employee(s) and other person(s) acting on behalf of the PO from remotely accessing PHI if other information, such as de-identified and/or aggregate information, will serve the purpose
- prohibit employee(s) and other person(s) acting on behalf of the PO from remotely accessing more PHI than is reasonably necessary for the identified purpose
- set out the administrative, technical, and physical safeguards a PO must implement to reduce risks to a level consistent with the risks associated with non-remote access, before its employee(s) or other person(s) acting on behalf of the PO are permitted to access PHI remotely

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of 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 received to develop or maintain the EHR, 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 PO
- require employee(s) and other person(s) acting on behalf of the PO to use the approved method(s) of transferring records of PHI
- 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 employee(s) and other person(s) acting on behalf of the PO 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:
    - employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
    - required content of the documentation
- whether and in what circumstances the employee or other person acting on behalf of the PO 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
- whether and in what circumstances confirmation of receipt of the records of PHI is required from the recipient, and if so the:

- the manner of obtaining and recording acknowledgement of receipt of the records of PHI
- the employee(s) and other person(s) acting on behalf of the PO responsible for obtaining and recording acknowledgement of receipt of the records of PHI

In addressing whether and in what circumstances an employee(s) and other person(s) acting on behalf of the PO is required to document the transfer and confirm receipt, regard must be had to other privacy and information security policies, procedures, and practices of the PO, 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***
- ***Policy, Procedures, and Practices for Executing Agreements with Third-Party Service Providers 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 the employees or other persons acting on behalf of the PO 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 PO 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**
- any directives made by the Minister to the PO with respect to the carrying out of its responsibilities and functions under 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*** and ***Fact Sheet 18: The Secure Transfer of Personal Health Information***
- evolving privacy and information security standards and best practices

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require employee(s) or other person(s) acting on behalf of the PO to comply with the policy, procedures, and practices

- require employee(s) or other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if an employee(s) or other person(s) acting on behalf of the PO breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices In Respect of 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 received to develop or maintain the EHR in both paper and electronic format in order to ensure that reconstruction of these records is not reasonably foreseeable in the circumstances.

Where a determination is made to dispose of records of PHI, the policy, procedures, and practices must:

- 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**
- 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**
- any directives made by the Minister to the PO with respect to the carrying out of its responsibilities and functions under 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***
- 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
- the identification of the employee(s) and other person(s) acting on behalf of the PO 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 employee(s) or other person(s) acting on behalf of the PO, who is not a TPSP, the policy, procedures, and practices must:

- identify the designated employee(s) or other person(s) acting on behalf of the PO responsible for securely disposing of the records of PHI
- outline the timeframe within which, the circumstances in which, and the conditions pursuant to which the records of PHI must be securely disposed of
- set out the responsibilities of the designated employee(s) or other person(s) acting on behalf of the PO in securely disposing of the records

The policy, procedures, and practices must also outline the process to be followed and the employee(s) or other person(s) acting on behalf of the PO responsible for:

- tracking the dates that records of PHI are transferred for secure disposal, and ensuring the certificates of destruction are received from the designated employee(s) or other person(s) acting on behalf of the PO
- implementing the process for instances where a certificate of destruction is not received within the timeframe set out in the policy, procedures, and practices

In the event that records of PHI or certain categories of records of PHI will be securely disposed of by an employee(s) or other person(s) acting on behalf of the PO 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:

- employee(s) or other person(s) acting on behalf of the PO to whom the certificate of destruction must be provided
- timeframe following secure disposal within which the certificate of destruction must be provided
- required content of the certificate of destruction

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

- identify the records of PHI securely disposed of
- indicate the date, time, and method of secure disposal employed
- bear the name and signature of the employee(s) or other person(s) acting on behalf of the PO who performed the secure disposal

The policy, procedures, and practices must also address where **certificates of destruction** will be retained, and the employee(s) and other person(s) acting on behalf of the PO responsible for retaining the certificates of destruction.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require employee(s) or other person(s) acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) or other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if an employee or other person acting on behalf of the PO breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of 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 systems, technologies, equipment, resources,

applications, and programs used to develop or maintain the EHR regardless of whether they are owned, leased, or operated by the PO.

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
- whether and how passwords are managed by software applications, such as password managers

The PO must require additional levels of identity assurance in proportion to the sensitivity of the **information security components** within the **information environment** that an employee or other person acting on behalf of the PO seeks to view, handle, or otherwise deal with. 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 employee(s) or other person(s) acting on behalf of the PO in respect of authentication and passwords in order to ensure that the PHI received to develop or maintain the EHR 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, employee(s) or other person(s) acting on behalf of the PO 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 employee or other person acting on behalf of the PO
- prohibited from writing down, displaying, revealing, hinting at, providing, sharing, or otherwise making their password known to any other individual, including another employee or other person acting on behalf of the PO

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

- any directives made by the Minister to the PO with respect to the carrying out of its responsibilities and functions under PHIPA and its regulations
- orders and decisions issued by the IPC under PHIPA and its regulations
- guidelines, fact sheets, and best practices issued by the IPC
- evolving privacy and information security standards and best practices

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

12. Policy, Procedures, and Practices in Respect of Privacy Flags and Notices to Employees and Other Persons Acting on Behalf of the Prescribed Organization

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
- upon the user's initial daily log-in to the PO'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 employee(s) or other person(s) acting on behalf of the PO to acknowledge and agree to certain statements prior to accessing PHI. At a minimum, the privacy flag and notice must:

- indicate that all viewing, handling, and otherwise dealing with of PHI will be logged, audited, and monitored
- require employee(s) or other person(s) acting on behalf of the PO to acknowledge and agree that they:
    - will only view, handle, or otherwise deal with PHI for the purpose of developing and maintaining the EHR
    - will comply with PHIPA and its regulations
    - have read, understood, and will comply with, the privacy and information security policies, procedures, and practices implemented
- set out the consequences for viewing, handling, or otherwise dealing with 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 implemented by the PO.

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**
- 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 employee(s) and other person(s) acting on behalf of the PO 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
- set out the documentation that must be completed, provided, and/or executed in respect of the privacy flags and notices, including the employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing the documentation, including the required content of the documentation
    - to whom this documentation must be provided

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require employee(s) or other person(s) acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) or other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if the employee(s) or other person(s) acting

on behalf of the PO, breaches or believes there may have been a breach of this policy, procedures, or practices

- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Information Security Audits***

13. Policy and Procedures for Acceptable Use Agreements with Employees and Other Persons Acting on Behalf of the Prescribed Organization

A policy, procedures, and practices must be developed and implemented requiring employees or other persons acting on behalf of the PO to acknowledge and agree to comply with an Acceptable Use Agreement that contains the language from the ***Template Acceptable Use Agreement with Employees and Other Persons Acting on Behalf of the Prescribed Organization***.

Timing of Acceptable Use Agreements

The policy, procedures, and practices must set out the timeframe within which employee(s) or other person(s) acting on behalf of the PO must acknowledge and agree to comply with the Acceptable Use Agreement. At a minimum, the policy, procedures, and practices must:

- require these employee(s) or other person(s) acting on behalf of the PO to acknowledge and agree to comply with the Acceptable Use Agreement prior to accessing information systems and technologies involving PHI, including PHI that has been de-identified and/or aggregated, for the first time and on an annual basis thereafter
- identify the timeframe each year in which employee(s) or other person(s) acting on behalf of the PO are required to acknowledge and agree to comply with the Acceptable Use Agreement on an ongoing basis

Process for Ensuring Employees and Other Persons Acting on Behalf of the Prescribed Organization Acknowledge and Agree to Comply with the Acceptable Use Agreement

The policy, procedures, and practices must:

- identify the employees(s) and other person(s) acting on behalf of the PO responsible
- set out the process to be followed in ensuring that employee(s) and other person(s) acting on behalf of the PO acknowledge and agree to comply with the Acceptable Use Agreement

Tracking Acceptable Use Agreements

The policy, procedures, and practices must:

- require that a log be maintained of all Acceptable Use Agreements acknowledged and agreed to by employee(s) or other person(s) acting on behalf of the PO
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for maintaining the log and for tracking that Acceptable Use Agreements have been acknowledged and agreed to
- outline the process to be followed in tracking that all employee(s) or other person(s) acting on behalf of the PO have acknowledged and agreed to comply with the Acceptable Use Agreement
- set out the documentation that must be completed, provided, and/or executed to verify that Acceptable Use Agreements have been acknowledged and agreed to, including the required content of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO:
    - responsible for completing, providing, executing, and ensuring the execution of the documentation,
    - to whom this documentation must be provided
    - responsible for retaining this documentation and where documentation related to the Acceptable Agreements will be retained

The policy, procedures, and practices must further:

- set out the process to be followed and the employee(s) and other person(s) acting on behalf of the PO responsible for identifying employee(s) and other person(s) acting on behalf of the PO who have not acknowledged and agreed to comply with the Acceptable Use Agreement and for ensuring that they do so
- specify the timeframe within which the procedure must be implemented
- address where documentation related to the Acceptable Agreements will be retained and the employee(s) and other person(s) acting on behalf of the PO responsible for retaining this documentation

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

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

14. Template Acceptable Use Agreement with Employees and Other Persons Acting on Behalf of the Prescribed Organization

An Acceptable Use Agreement must be acknowledged and agreed to by each employee or other person acting on behalf of the PO in accordance with the ***Policy, Procedures, and Practices for Acceptable Use Agreements with Employees and Other Persons Acting on Behalf of the Prescribed Organization***. At a minimum, the Acceptable Use Agreement must address the matters set out below.

Obligations with Respect to Viewing, Handling, and Otherwise Dealing with Personal Health Information

Where an employee(s) or other person(s) acting on behalf of the PO are being provided access to information systems and technologies involving PHI, the Acceptable Use Agreement must identify the purposes for which these employees or other persons are permitted to view, handle, or otherwise deal with the PHI.

Where an employee(s) or other person(s) acting on behalf of the PO are being provided access to systems and technologies involving PHI that has been de-identified and/or aggregated, the Acceptable Use Agreement must identify the purposes for which these employees or other persons are permitted to use and disclose the de-identified or aggregated information.

Administrative, Technical, and Physical Safeguards

The Acceptable Use Agreement must set out the administrative, technical, and physical safeguards that employees or other persons acting on behalf of the PO are required to implement to protect PHI, including PHI collected that has been de-identified and/or aggregated.

With respect to PHI, this includes requiring employees or other persons acting on behalf of the PO to:

- only view, handle, or otherwise deal with the PHI if other information, such as de-identified and/or aggregate information, will not serve the purposes
- not view, handle, or otherwise deal with more of the PHI than is reasonably necessary

With respect to PHI that has been de-identified and/or aggregated, this includes requiring the employee(s) or other person(s) acting on behalf of the PO not to use the de-identified or aggregate information, either alone or with other information, to identify an individual. This includes attempting to:

- decrypt information that is encrypted

- identify an individual based on unencrypted information
- identify an individual based on prior knowledge

Consequences of Breach and Monitoring Compliance

The Acceptable Use Agreement must:

- outline the consequences of a breach of the agreement
- address the manner in which compliance with the Acceptable Use Agreement will be enforced
- stipulate that compliance with the Acceptable Use Agreement will be audited
- address the manner in which compliance will be audited

Required Acknowledgements and Agreements

The Acceptable Use Agreement must require the employee(s) or other person(s) acting on behalf of the PO to acknowledge and agree:

- not to view, handle, or otherwise deal with PHI, including PHI that has been de-identified and/or aggregated, except as permitted by the Acceptable Use Agreement and by the privacy policies, procedures, and practices implemented by the PO
- to implement the administrative, technical, and physical safeguards set out in the Acceptable Use Agreement
- to comply with PHIPA and its regulations and the terms of the Acceptable Use Agreement
- that they have read, understood, and agree to comply with the privacy and information security policies, procedures, and practices implemented pursuant to PHIPA and its regulations
- to provide notification at the first reasonable opportunity of a privacy breach, information security breach, suspected privacy breach or information security incident in accordance with the ***Policy, Procedures and Practices for Privacy Breach Management*** and/or ***Policy, Procedures and Practices for Information Security Breach Management***, as the case may be

15. Log of Acceptable Use Agreements

A log of all Acceptable Use Agreements acknowledged and agreed to by the employee(s) or other person(s) acting on behalf of the PO must be maintained. At a minimum, the log must set out:

- the name of the employee(s) or other person(s) acting on behalf of the PO
- for each employee or other person acting on behalf of the PO, the date(s):
    - of commencement of their employment, contractual, or other relationship with the PO
    - the Acceptable Use Agreement was acknowledged and agreed to

16. Policy, Procedures, and Practices for End User Agreements

A policy, procedures, and practices must be developed and implemented requiring each end user (including an end user who is a custodian or an agent of a custodian), who provides PHI to or collects PHI by means of the EHR to acknowledge and agree to comply with an End User Agreement that contains the language from the ***Template End User Agreement***.

Timing of End User Agreement

The policy, procedures, and practices must set out the timeframe within which end users must acknowledge and agree to comply with the End User Agreement. At a minimum, the policy, procedures, and practices must:

- require those end users to acknowledge and agree to comply with the End User Agreement prior to providing PHI to or collecting PHI via the EHR for the first time, and on an annual basis thereafter
- identify the timeframe each year in which end users are required to acknowledge and agree to comply with the End User Agreement on an ongoing basis

Process for Ensuring End Users Agree to Comply with the End User Agreement

The policy, procedures, and practices must identify the employee(s) or other person(s) acting on behalf of the PO responsible for and the process to be followed in ensuring that each custodian and each of their agents agrees to comply with the End User Agreement.

Tracking End User Agreements

The policy, procedures, and practices must:

- require that a log be maintained of all End User agreements acknowledged and agreed to by end users
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for maintaining the log and for tracking that End User Agreements have been acknowledged and agreed to
- outline the process to be followed in tracking that all end users have acknowledged and agreed to comply with the End User Agreement
- set out the documentation that must be completed, provided, and/or executed to verify that End User Agreements have been acknowledged and agreed to, including the required content of the documentation
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for completing, providing, executing, and ensuring the execution of the documentation
- identify the employee(s) or other person(s) to whom this documentation must be provided

The policy, procedures, and practices must further set out the process to be followed and the employee(s) or other person(s) acting on behalf of the PO responsible for:

- identifying end users who have not acknowledged and agreed to comply with the End User Agreement
- ensuring that these custodians and their agents do so, including the timeframe within which the procedure must be implemented

It is also recommended that the policy, procedures, and practices address where documentation related to the End User Agreement will be retained and the employee(s) or other person(s) acting on behalf of the PO responsible for retaining this documentation.

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

17. Template End User Agreements

An End User Agreement must be acknowledged and agreed to by each end user who provides PHI to or collects PHI by means of the EHR, and by each of their agents. At a minimum, the End User Agreement must address the matters set out below.

Obligations with Respect to Collection, Use, and Disclosure of Personal Health Information

The End User Agreement must:

- identify the purposes for which the end user is permitted to provide PHI to, or to collect, use, or disclose PHI by means of the EHR
- require that each provision, collection, use, or disclosure identified in the End User Agreement be permitted by PHIPA and its regulations

Administrative, Technical, and Physical Safeguards

The End User Agreement must set out the administrative, technical, and physical safeguards that the end users are required to implement and adhere to protect the PHI that the custodian or their agent provides to, or collects, uses, or discloses via the EHR.

Consequences of Breach and Monitoring Compliance

The End User Agreement must:

- outline the consequences of a breach of the agreement
- address the manner in which compliance with the End User Agreement will be enforced
- stipulate that compliance with the End User Agreement will be audited
- address the manner in which compliance will be audited

Required Acknowledgements and Agreements

The End User Agreement must require end users to acknowledge and agree to:

- provide, collect, use, disclose, view, handle, or otherwise deal with PHI via the EHR only in accordance with the terms of the End User Agreement and PHIPA and its regulations
- implement and comply with the administrative, technical, and physical safeguards set out in the End User Agreement
- provide the notifications required by the End User Agreement and PHIPA and its regulations
- comply with PHIPA and its regulations and the terms of the End User Agreement

18. Log of End User Agreements

A log of all End User Agreements acknowledged and agreed to by end users who provide PHI to or collect PHI by means of the EHR, and each of their agents must be maintained. At a minimum, the log must set out:

- the name of each custodian or agent
- for each agent, the name of the custodian on whose behalf the agent is acting
- the dates that the End User Agreement was acknowledged and agreed to

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

The PO must develop and implement a policy, procedures, and practices with respect to the logging, monitoring, and auditing of privacy and information security events involving PHI that is accessible by means of the EHR. At a minimum, the logging, monitoring, and auditing of privacy and information security events that must be created, maintained, and reviewed must include the electronic records the PO is required to keep under paragraph 4 of section 55.3 of PHIPA. The policy, procedures, and practices that is applied must also be commensurate with the:

- amount and sensitivity of the PHI maintained
- number and nature of roles played by employee(s) or other person(s) acting on behalf of the PO, or with persons acting on behalf of custodians with access to the PHI
- threats and risks associated with the PHI

In developing the policy, procedures, and practices, the PO 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
    - the PO set out under paragraphs 4 and 7 through 9 of section 55.3 of PHIPA
- findings, mitigations, and other recommendations arising from prior three-year reviews
- evolving privacy and information security standards and best practices

Logging of Privacy and Information Security Events

The policy, procedures, and practices must require the PO to determine which privacy and information security events are mandatory to be logged, and 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 employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO 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

- 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
- employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided
- 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, view, handle, or otherwise deal with PHI, including those events the PO is required to keep under paragraph 4 of section 55.3 of PHIPA
- 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
- 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 name or unique identifier associated with the individual to whom the information relates
- 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
- 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, view, 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, viewed, handled, and/or otherwise dealt with
- any changes to values
- the name or unique identifier associated with the individual to whom PHI relates

Where the PO transmits PHI to a custodian by means of the EHR, upon the request of the custodian, the PO must require the privacy and information security event logs to contain the:

- name or unique identifier associated with the individual to whom the information relates
- type of information that is transmitted
- custodian requesting the information
- date and time that the information was transmitted
- location to which the information was transmitted

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 employee(s) and other person(s) acting on behalf of the PO responsible for retaining the privacy and information security event logs
- 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 PO 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 pursuant to paragraph 7 of section 55.3 of PHIPA, and:

- identify and assess real-time evidence of a privacy breach or suspected privacy breach and/or an information security breach or information security incident
- assist with the notification of the responsible employee(s) and other person(s) acting on behalf of the PO, 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 respond to inquiries and complaints from individuals, support the 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 employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for determining whether to approve or deny monitoring tools and mechanisms
- 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 required content of the documentation
- employee(s) and other person(s) acting on behalf of the PO:
  - responsible for completing, providing, and/or executing the documentation
  - to whom this documentation must be provided

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 PO (e.g., those listed under "Mandatory Events to Log" above)
- logs of privacy and information security events to be audited and monitored pursuant to paragraph 7 of section 55.3
- information security data sources (e.g., network traffic, incoming/outgoing emails, device status monitoring, and alerts)
- physical security data sources (e.g., security card activity, motion sensors, temperature, and humidity measurements)
- human resources data sources (e.g., employee hiring and termination records, and 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
    - 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
- 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
- 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
- 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 employee(s) and other person(s) acting on behalf of the PO 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, including the required content of the documentation
- employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing the documentation
    - to whom this documentation must be provided
- frequency with which the documentation must be provided

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 employee(s) and other person(s) acting on behalf of the PO 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 that is accessible by means of the EHR is collected, created, accessed, used, modified,

transmitted, disclosed, disposed of, viewed, handled, or otherwise handled by the employee(s) and other person(s) acting on behalf of the PO, or by a custodian or an agent of a custodian

- 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
- 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)
- targeted (e.g., activities of a specific employee or other person acting on behalf of the PO, or activities of all employees or other persons acting on behalf of the PO in relation to the PHI of a specific individual)
- random (e.g., activities of a randomly selected employee or other person acting on behalf of the PO or activities of all employees or other persons acting on behalf of the PO in respect of a randomly selected individual)

The policy, procedures, and practices must also set out the circumstances where auditing and monitoring must be conducted on a continuous basis (e.g., every instance where a consent directive is overridden).

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 employee(s) and other person(s) acting on behalf of the PO responsible for:

- assigning other employee(s) and other person(s) acting on behalf of the PO to address the findings
- establishing timelines to address the findings
- monitoring and ensuring the treatment of findings within stated timelines
- 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), including the required content of the documentation

- employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, executing, and/or ensuring the execution of the documentation
- employee(s) and other person(s) acting on behalf of the PO to whom the documentation must be provided
- frequency with which this documentation must be provided
- timeframe within which the documentation must be provided
- 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 employee(s) and other person(s) acting on behalf of the PO:
    - responsible for communicating the findings of the audit of the privacy and information security event logs
    - 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)
    - responsible for tracking that the findings have been addressed within the identified timelines
- timeframe within which the findings of the audit of the privacy and information security event logs must be communicated
- 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

Responding to Requests for Electronic Records

The policy, procedures, and practices must set out the process that must be followed in responding to requests from custodians pursuant to paragraph 9 of section 55.3 of PHIPA for electronic records the PO is required to keep pursuant to paragraph 4 of section 55.3 of PHIPA.

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

- require that the PO provide, upon the request of a custodian that requires the records to audit and monitor its compliance with PHIPA, the electronic records that the PO is required to keep under PHIPA
- set out the process for responding to requests
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for:
    - receiving requests for electronic records from custodians
    - preparing the electronic records requested by custodians
    - providing the requested information to custodians

- set out any documentation that must be completed, provided, and/or executed by the employee(s) or other person(s) acting on behalf of the PO and/or the custodian requesting the electronic records, including the required content of the documentation
- identify the employee(s) or other person acting on behalf of the PO responsible for completing, providing, executing, and ensuring the execution of documentation, and to whom this documentation must be provided
- specify the form, manner, and timeframe within which the electronic records requested by custodians must be provided

The policy, procedures, and practices must also set out the process that must be followed in responding to requests from the IPC pursuant to paragraph 8 of section 55.3 of PHIPA for the electronic records that the PO is required to keep for the purposes of paragraph 4 of section 55.3 of PHIPA. At a minimum, the policy, procedures, and practices must:

- specify that the PO must provide, upon the request of the IPC, the electronic records that the PO is required to keep under PHIPA to the IPC for the purposes of Part VI of PHIPA
- set out the process for responding to the request
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for:
    - receiving requests for electronic records from the IPC
    - preparing the electronic records requested by the IPC
    - providing the requested information to the IPC
- set out any documentation that must be completed, provided, and/or executed by the employee(s) or other person(s) acting on behalf of the PO and/or the IPC, including the required content of the documentation
- identify the employee(s) or other person acting on behalf of the PO responsible for completing, providing, executing, and ensuring the execution of documentation, and to whom this documentation must be provided
- specify the form, manner, and timeframe within which the electronic records requested by the IPC must be provided

Logging

The policy, procedures, and practices must further require that logs be maintained of all requests from:

- custodians, made pursuant to paragraph 9 of section 55.3 of PHIPA, for the electronic records the PO is required to maintain pursuant to paragraph 4 of section 55.3 of PHIPA
- the IPC, made pursuant to paragraph 8 of section 55.3 of PHIPA, for the electronic records the PO is required to maintain pursuant to paragraph 4 of section 55.3 of PHIPA

The policy, procedures, and practices must also:

- ensure that the requests are responded to or provided within the identified timeframe
- address where documentation related to auditing and monitoring will be retained
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for:
    - maintaining each log and for tracking requests for electronic records
    - retaining the documentation

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. Specifically, the policy, procedures, and practices must identify the:

- employee(s) and other person(s) acting on behalf of the PO 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. Where the reviews must include assessments to determine if the logging, monitoring, and auditing practices effectively meet the requirements of the policy, procedures, and practices
- process to be followed when reviewing and updating the types of privacy and information security events that must be logged
- required content of each log of privacy and information security events

Further, the policy, procedures, and practices must require the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for logging, monitoring, and auditing of the privacy and information security events to notify the PO, 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***

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

20. Log of Requests for Electronic Records from Health Information Custodians

The PO must maintain a log of the electronic records that are provided to custodians, pursuant to paragraph 9 of section 55.3 of PHIPA. At a minimum, for each request for electronic records received from a custodian, the log must:

- identify the employee(s) or other person(s) acting on behalf of the PO who received the request for electronic records
- set out the date the request for electronic records was received by the PO
- identify the custodian who made the request for electronic records
- specify the types of electronic records that were requested by the custodian
- identify the employee(s) or other person(s) acting on behalf of the PO who responded to the request
- set out the types of electronic records that were provided to the custodian
- identify the agent of the custodian to whom the electronic records were provided
- specify the form, manner, and date the electronic records were provided to the custodian

21. Log of Requests for Electronic Records from the Information and Privacy Commissioner

The PO must maintain a log of the electronic records that are provided to the IPC pursuant to paragraph 8 of section 55.3 of PHIPA. At a minimum, for each request for electronic records received from the IPC, the log must:

- identify the employee(s) or other person(s) acting on behalf of the PO who received the request for electronic records
- set out the date the request was received
- identify the IPC employee(s) who submitted the request
- specify the types of electronic records that were requested by the IPC
- identify the employee(s) or other person(s) acting on behalf of the PO who responded to the request
- set out the types of electronic records that were provided to the IPC
- identify the IPC employee(s) to whom the electronic records were provided
- specify the form, manner, and date when the electronic records were provided to the IPC

22. Policy, Procedures, and Practices for Vulnerability and Patch Management

A policy, procedures, and practices must be developed and implemented for vulnerability and patch management for all information systems used to develop and maintain the EHR.

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 PO
- define the frequency with which and the circumstances in which the inventory must be updated
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for maintaining and updating the inventory
- set out the documentation required to be completed, provided, and/or executed
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- identify the employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided
- 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 PO 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 PO would apply to the **information security components** within the **information environment**
- purpose of each assessment
- process for how the PO would quantify the severity of any vulnerabilities
- need to develop recommendations and timelines to mitigate those vulnerabilities
- employee(s) and other person(s) acting on behalf of the PO 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, including the required content of the documentation
- employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing the documentation
    - to whom this documentation must be provided

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 PO 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
- identify the employee(s) and other person(s) acting on behalf of the PO 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
- 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
- employee(s) and other person(s) acting on behalf of the PO 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
    - documentation that must be completed, provided, and/or executed
- employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided

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
    - 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 PO is conducting an assessment of each identified vulnerability
    - 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***
- 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
    - documentation that must be completed, provided, and/or executed, including the required content of the documentation
    - employee(s) and other person(s) acting on behalf of the PO:
        - responsible for ensuring the re-scanning is administered
        - responsible for completing, providing, and/or executing this documentation
        - to whom this documentation must be provided

Patch Monitoring

The policy, procedures, and practices must require the PO to monitor for the availability of patches and other mitigation methods, and identify the:

- employee(s) and other person(s) acting on behalf of the PO responsible for monitoring for the availability of patches and other mitigation methods (e.g., configuration changes) on behalf of the PO
- frequency with which such monitoring must be conducted
- 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 employee(s) and other person(s) acting on behalf of the PO responsible for:
    - analyzing the patches and other mitigation methods
    - making a determination as to whether the patches and other mitigation methods should be implemented
- set out the process that must be followed

- specify the criteria that must be considered by the employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO 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, and critical)
- components within the information environment to which the patches and other mitigation methods relate
- 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 employee(s) and other person(s) acting on behalf of the PO 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
- 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 employee(s) and other person(s) acting on behalf of the PO 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
    - employee(s) and other person(s) acting on behalf of the PO responsible for testing

- documentation to be completed, provided, maintained, and/or executed 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
    - employee(s) and other person(s) acting on behalf of the PO responsible for completing, maintaining, providing, and/or executing, this documentation, and to whom this documentation must be provided
    - required content of the 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 employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for testing
- whether or not the testing was successful

Compliance, Audit, and Enforcement

The PO must:

- require the employee(s) or other person(s) acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) or other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if an employee or other person acting on behalf of the PO breaches or believes there may have been a breach of this policy, procedures, or practices

- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Information Security Audits***

23. 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 PO, used to create or maintain the EHR.

Review and Approval Process

The policy, procedures, and practices must identify the:

- employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO 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
    - the impact of executing or not executing the change to the information environment
- manner of documenting the decision approving or denying the request for a change to the information environment
- employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing the documentation, and
    - to whom this documentation must be provided

- 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 employee(s) or other person(s) acting on behalf of the PO requesting the change
    - reasons for the decision to approve or not approve the change
    - the impact of executing or not executing the change
    - timeframe for implementation of the change and the priority assigned to the change
    - the name of the employee(s) and other person(s) acting on behalf of the PO 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:

- employee(s) and other person(s) acting on behalf of the PO 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, and the required content of the documentation
- process for implementation of the approved change(s) to the information environment
- employee(s) and other person(s) acting on behalf of the PO responsible for implementation
- documentation that must be completed, provided, and/or executed by the employee(s) and other person(s) acting on behalf of the PO responsible for implementation, and the required content of the documentation
- 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
- employee(s) and other person(s) acting on behalf of the PO responsible for testing
- documentation that must be completed, provided, and/or executed by the employee(s) and other person(s) acting on behalf of the PO responsible for testing, and the required content of the documentation.

The policy, procedures, and practices must also require documentation to be maintained of changes that have been implemented and identify the employee(s) and other person(s) acting on behalf of the PO responsible for maintaining this documentation. At a minimum, the documentation must include:

- a description of the change requested
- the name of the employee(s) or other person(s) acting on behalf of the PO requesting the change
- the date that the change was requested
- the priority assigned to the change
- the date that the change was implemented
- the employee(s) and other person(s) acting on behalf of the PO responsible for implementing the change
- the date, if any, when the change was tested
- the employee(s) and other person(s) acting on behalf of the PO responsible for testing
- whether or not the testing was successful

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

24. 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 received by the PO to develop or maintain the EHR. The policy, procedures, and practices must identify the:

- nature and types of back-up storage devices maintained by the PO
- frequency with which records of PHI are backed-up
- process that must be followed and the requirements that must be satisfied
- documentation that must be completed, provided, and/or executed, including the required content of the documentation
- employee(s) and other person(s) acting on behalf of the PO:
    - responsible for the back-up and recovery of records of PHI
    - responsible for completing, providing, and/or executing the documentation
    - to whom this documentation must be provided

Testing Procedures for Back-Up and Recovery, and Retention of Records

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

- testing of the procedure for back-up and recovery of records of PHI
- employee(s) and other person(s) acting on behalf of the PO 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, and the required content of this documentation
- the employee(s) and other person(s) acting on behalf of the PO responsible for testing
- employee(s) and other person(s) acting on behalf of the PO 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
- 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 Personal Health Information***, and identify the employee(s) and other person(s) acting on behalf of the PO 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
- circumstances in which the backed-up records are required to be made available

Third-Party Service Providers

If a TPSP is contracted, or otherwise engaged to receive transferred records of PHI, and/or 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 Secure Transfer of Records of Personal Health Information***
- ***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***

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

25. 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 PO.

The policy, procedures, and practices of the PO must set out the uses that are:

- permitted without exception
- prohibited without exception
- 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:

- employee(s) and other person(s) acting on behalf of the PO 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
- employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- required content of the documentation
- employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided

The policy and procedures must further set out the:

- criteria that must be considered by the employee(s) and other person(s) acting on behalf of the PO responsible for determining whether to approve or deny the request
- conditions or restrictions that apply to the employee(s) or other person(s) acting on behalf of the PO whose requests have been approved
- manner of documenting the decision approving or denying the request and the reasons for the decision
- method by which and the format in which the decision will be communicated and to whom this decision will be communicated

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

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

26. Policy, Procedures, and Practices for Threat and Risk Assessments

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

Circumstances in which Threat Risk Assessments are Required to be Conducted

In identifying the circumstances in which threat and risk assessments are required to be conducted, the policy, procedures, and practices must, at a minimum, specify that a threat and risk assessment must be conducted:

- for all existing and proposed systems used to develop or maintain the EHR, including each system that retrieves, processes, or integrates PHI in the EHR
- whenever a change to an existing information system, technology, or program involving PHI is contemplated
- for each type of PHI that is proposed, or that is requested or required by regulation to be provided to the PO to develop or maintain the EHR

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

- determining if and when threat risk assessments must be completed and reviewed and the employee(s) and other person(s) acting on behalf of the PO responsible for making this determination
- ensuring that threat risk assessments are in fact conducted, completed, reviewed, and amended, as necessary, and the employee(s) or other person(s) acting on behalf of the PO responsible for conducting the required follow-up

A written copy of the results of the threat and risk assessments that relate to the PHI the custodian provided to the PO must be made available to each custodian that provided PHI to the PO to develop or maintain the EHR.

Timing of Conducting and Reviewing Threat Risk Assessments

The policy, procedures, and practices must also address the timing of threat and risk assessments. With respect to:

- proposed systems, and proposed changes to existing systems, the policy, procedures, and practices must require that threat and risk assessments be:
    - conducted at the conceptual design stage, before the PHI is requested or required to be provided to the PO

    - reviewed and amended, if necessary, during the detailed design and implementation stage

- existing systems, the policy, procedures, and practices must require:
    - a timetable be developed to ensure threat and risk assessments are conducted as and when necessary, and updated, as and when necessary
    - the identification of the employee(s) or other person(s) acting on behalf of the PO responsible for developing the timetable

Once threat and risk assessments have been completed, the policy, procedures, and practices must require the:

- review of threat risk 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 security practices of the PO
- identification of the circumstances in which and the frequency with which the threat and risk assessments are required to be reviewed and amended, if necessary

Required Content of Threat Risk Assessments

The policy, procedures, and practices must also stipulate the required content of threat and risk assessments for existing or proposed systems that retrieve, process, or integrate PHI that is accessible by means of the EHR developed or maintained by the PO. At a minimum, the threat and risk assessments must include:

- scope of the threat and risk assessment, including risk tolerance level
- asset identification
- asset valuation
- identification of safeguards (both existing and those pending implementation)
- identification of threats and vulnerabilities
- assessment of the likelihood of threats
- assessment of the potential impact of threats
- risk analysis, based on both threat likelihood and size of impact, including prioritized list of threats
- risk treatment, including recommendations to mitigate, transfer or avoid risk
- residual risk analysis and acceptance

A threat and risk assessment methodology that does not include each of the above elements may be acceptable provided that the PO can demonstrate that the methodology used by the PO is consistent with alternative well-established threat and risk assessment methodologies and standards.

Threat Risk Assessment Findings and Recommendations

The policy, procedures, and practices must also outline the process for documenting the findings, and reviewing and addressing the recommendations arising from threat and risk assessments, including the employee(s) or other person(s) acting on behalf of the PO responsible for:

- assigning other employee(s) or other person(s) acting on behalf of the PO to address the mitigations, and any other relevant recommendations
- establishing timelines to address the mitigations, findings, and any other relevant recommendations
- monitoring and ensuring the treatment of the mitigations, findings, and any other relevant recommendations within stated timelines
- evaluating the residual risk remaining after implementation

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the PO responsible for maintaining a log of threat risk assessments that have been:

- completed
- undertaken, but not completed
- not undertaken

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

27. Log of Threat and Risk Assessments

The PO must maintain a log of threat and risk assessments that have been completed and of threat and risk assessments that have been undertaken, but that have not been completed. The log must describe the:

- system that is at issue
- date the threat and risk assessment was completed or is expected to be completed
- employee(s) and other person(s) acting on behalf of the PO responsible for completing or ensuring the completion of the threat and risk assessment
- recommendations arising from the threat and risk assessment
- employee(s) and other person(s) acting on behalf of the PO responsible for addressing each recommendation
- date that each recommendation was or is expected to be addressed
- manner in which each recommendation was or is expected to be addressed

The PO must also maintain a log of new and proposed changes to existing systems for which threat and risk assessments have not been undertaken. For each such system, the log must set out the:

- date that the threat and risk assessment is expected to be completed
- employee(s) and other person(s) acting on behalf of the PO responsible for completing or ensuring the completion of the threat and risk assessment

Information Security Audit Program

28. 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 PO
- 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)
- audits of privacy and information security event logs, including the electronic records required to be kept pursuant to paragraph 4 of section 55.3 of PHIPA, and to be audited and monitored pursuant to paragraph 7 of section 55.3 of PHIPA

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
- employee(s) and other person(s) acting on behalf of the PO responsible for conducting the information security audit
- 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
    - identify the employee(s) and other person(s) acting on behalf of the PO responsible for developing and ensuring the implementation of the information security audit schedule

At a minimum, audits of employees or other persons acting on behalf of the PO granted access to the premises of the PO 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
- 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 PO 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, including the required content of the documentation
- employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing the documentation
    - to whom this documentation must be provided

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 employee(s) and other person(s) acting on behalf of the PO responsible for:

- assigning other employee(s) and other person(s) acting on behalf of the PO 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
- evaluating the residual risks remaining after implementation

Required Documentation

The policy, procedures, and practices of the PO 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
- employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- required content of the documentation
- employee(s) and other person(s) acting on behalf of the PO to whom the documentation must be provided

Risk Reporting

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

29. Log of Information Security Audits

A PO 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
- employee(s) and other person(s) acting on behalf of the PO responsible for completing the information security audit
- findings arising from the information security audit, mitigations, and other relevant recommendations
- employee(s) and other person(s) acting on behalf of the PO responsible for addressing each mitigation and other relevant recommendation
- date that each mitigation and relevant recommendation was or is expected to be addressed
- 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, or critical)
- a description of the vulnerability
- the number of **information security components** within the **information environment** with or affected by the identified vulnerability
- the following details for each component with the identified vulnerability, the:
    - date that each recommendation was or is expected to be addressed
    - employee(s) and other person(s) acting on behalf of the PO responsible for addressing each recommendation
    - manner in which each recommendation was or is expected to be addressed

Information Security Breaches

30. 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
- 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 PO, related to the requirements of the Manual

The policy, procedures, and practices of a PO 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 PO. 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 an employee or other person acting on behalf of the PO and electronic service providers of the PO, a custodian as well as information security audits, privacy complaints, and inquiries and
- auditing and monitoring are required to be performed by the PO in accordance with the:
    - ***Policy, Procedures, and Practices for Logging, Monitoring, and Auditing Privacy and Information Security Events***
    - ***Policy, Procedures, and Practices in Respect of Information Security Audits***

The policy, procedures, and practices must require the employee(s) or other person(s) acting on behalf of the PO to notify the PO 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 employee(s) or other person(s) acting on behalf of the PO 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, including the required content of the documentation
- identify the employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing the documentation
    - to whom this documentation must be provided

Information Security Breaches Caused by One or More Health Information Custodian(s)

The policy, procedures, and practices must specify that where the PO identifies an information security breach or information security incident that was caused by one or more custodian(s), the PO must notify the custodian(s) of the information security breach or information security incident.

The policy, procedures, and practices must specify that, when requested or directed to do so by the Minister, the PO must:

- cooperate with the custodian(s) to develop a policy and procedures to make a determination of whether an information security breach has in fact occurred and if so, to contain, investigate, and remediate the information security breach in circumstances where the information security breach or information security incident was caused by one or more custodian(s)

- assist custodians to determine whether an information security breach has in fact occurred and if so, assist in containing, investigating, and remediating the information security breach where the information security breach or information security incident was caused by one or more custodian(s)

Information Security Breaches Caused by the Prescribed Organization or an Unauthorized Person

The policy, procedures, and practices must require the PO to take the following steps in any instance in which an information security breach or information security incident is caused by an:

- employee or other person acting on behalf of the PO
- a system that retrieves, processes, or integrates PHI that is accessible by means of the EHR or
- unauthorized person who is not an employee or other person acting on behalf of the PO or an agent of a custodian

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 the PO to determine:

- 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

The policy, procedures, and practices must also identify the employee(s) and other person(s) acting on behalf of the PO 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
- the extent at which PHI may be affected

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

- procedures that must be followed to approve the prioritization framework, including:
    - any documentation that must be completed, provided, and/or executed by the employee(s) and other person(s) acting on behalf of the PO responsible for developing and approving the prioritization framework
    - required content of the documentation
- employee(s) and other person(s) acting on behalf of the PO responsible for:
    - the prioritization framework
    - approving the prioritization framework
    - 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 employee(s) and other person(s) acting on behalf of the PO responsible for notifying senior management
- the timeframe within which notification must be provided
- the manner in which this notification must be provided
- the nature of the information 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 the PO initiate containment immediately and must identify the employee(s) and other person(s) acting on behalf of the PO:

- responsible for containment and the procedure that must be followed, including any documentation that must be completed, provided, and/or executed
- responsible for completing, providing, and/or executing the documentation
- to which the notification must be provided

The policy, procedures and practices must also specify the 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, disclosure, viewing, handling or otherwise dealing with PHI
- additional information security breaches cannot occur through the same means

The policy, procedures, and practices must identify the:

- employee(s) and other person(s) acting on behalf of the PO 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, including the required content of the documentation
- employee(s) and other person(s) acting on behalf of the PO responsible for reviewing the containment measures and ensuring the execution of the documentation
- employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided

Breach Notification to Custodians or Other Persons or Organizations

The policy, procedures, and practices must require the PO to determine the parties to be notified of an information security breach. At minimum, the PO must notify the custodian(s) that provided the PHI to the PO, to develop or maintain the EHR, at the first reasonable opportunity whenever PHI is or is believed to be stolen, lost, collected, used, or disclosed without authority and whenever required pursuant to the agreement with the custodian.

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

- employee(s) and other person(s) acting on behalf of the PO responsible for notifying the custodian(s)
- format of the notification
- 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

  - further actions that will be undertaken with respect to the information security breach, including investigation and remediation

The policy, procedures, and practices must also set out whether any other persons or organizations must be notified of the information security breach and must set out the:

- employee(s) or other person(s) acting on behalf of the PO responsible for notifying these other persons or organizations
- format of the notification
- nature of the information that must be provided upon notification
- timeframe for notification

At a minimum, the policy, procedures, and practices must require the PO to notify the IPC, in writing, immediately after becoming aware that PHI in the EHR:

- has been viewed, handled, or otherwise dealt with by the PO or a third party retained by the PO other than in accordance with PHIPA or its regulations or
- has been made available or released by the PO or a third party retained by the PO, other than in accordance with PHIPA and its regulations

Breach Notification to the Information and Privacy Commissioner

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:

- employee(s) and other person(s) acting on behalf of the PO responsible for providing such notification
- format of the notification
- nature of the information that must be provided upon notification
- timeframe for notification

At a minimum, the policy and procedures must require the PO to notify the IPC, in writing, immediately after becoming aware that PHI in the EHR has been:

- viewed, handled, or otherwise dealt with by the PO or a third-party retained by the PO other than in accordance with PHIPA or its regulations or
- made available or released by the PO or a third-party retained by the PO, other than in accordance with PHIPA and its regulations

Breach Notification to Affected Individuals

The policy, procedures, and practices must also set out that the PO 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). However, the policy, procedures, and practices must specify that the PO must also assist one or more

custodian(s) in fulfilling their obligations to notify individuals under PHIPA to the greatest extent possible, when requested or directed to do so by the Minister.

Investigation and Recommendations

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

- employee(s) and other person(s) acting on behalf of the PO 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, including the required content of the documentation and
    - employee(s) and other person(s) acting on behalf of the PO:
        - responsible for completing, providing, and/or executing the documentation
        - to whom this documentation must be provided

The policy, procedures, and practices must also identify the employee(s) and other person(s) acting on behalf of the PO responsible for:

- assigning other employee(s) and other person(s) acting on behalf of the PO 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
- 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:

- employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing this documentation and
    - to whom this documentation must be provided
- 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 employee(s) and other person(s) acting on behalf of the PO responsible for communicating the findings of the investigation
- the mechanism and format for communicating the findings of the investigation, including the level of detail for communicating the findings
- the timeframe within which the findings of the investigation must be communicated
- to whom the findings of the investigation must be communicated, including whether the findings must be communicated to the chief executive officer or the executive director (or equivalent position)

Tracking Information Security Breaches

The policy, procedures, and practices must require that a log be maintained of **information security breaches** and must:

- identify the employee(s) and other person(s) acting on behalf of the PO 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
- address where documentation related to the identification, reporting, containment, notification, investigation, and remediation of information security breaches will be retained
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for retaining this documentation

Relationship to *Policy, Procedures, and Practices for Privacy Breach Management*

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

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require the employee(s) or other person(s) acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) or other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if an employee or other person acting on behalf of the PO breaches or believes there may have been a breach of this policy, procedures, or practices

- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of Information Security Audits***

31. Log of Information Security Breaches

The PO 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 by:
    - one or more custodian(s) or an agent or electronic service provider of a custodian, and the name of each custodian and of each agent and electronic service provider of the custodian identified as the cause, if applicable
    - one or more employee(s) or other person(s) acting on behalf of the PO, including the name of each employee and other person acting on behalf of the PO that identified the cause, if applicable
    - a system that retrieves, processes, or integrates PHI in the EHR created or maintained by the PO or the name of each system that caused the information security breach, if applicable or
    - an unauthorized person who is not an employee or other person acting on behalf of the PO or electronic service provider and the name or a description of the unauthorized person, if applicable
- the name of each custodian that provided the PHI to the PO, 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 applicable
- the date that the information security breach was contained and the nature of the containment measures

- the name of the employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for conducting the investigation
- the findings, mitigations, and any other relevant recommendations arising from the investigation
- the employee(s) and other person(s) acting on behalf of the PO 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 status of the implementation of each recommendation
- 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(s) that notification was provided to:
    - the custodian that:
        - caused the information security breach or information security incident, if applicable
        - provided the PHI to the PO to develop and maintain the EHR, if applicable
    - the IPC, if applicable and/or
    - 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 employees and other persons acting on behalf of the PO to attend initial and ongoing privacy training.

Timing and Method of Initial and Ongoing Privacy Training

The policy, procedures, and practices must set out the timeframe within which employees and other persons acting on behalf of the PO 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 employees or other persons acting on behalf of the PO to complete the initial privacy training prior to viewing, handling, or otherwise dealing with PHI received to develop or maintain the EHR, including PHI that has been de-identified and/or aggregated
- require employees or other persons acting on behalf of the PO to complete ongoing privacy training provided by the PO on an annual basis thereafter
- specify 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 employee(s) or other person(s) acting on behalf of the PO 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 annually, and updated, as needed
- specify the frequency with which the training will be reviewed
- identify the employee(s) or other person(s) acting on behalf of the PO responsible for reviewing and updating the training
- set out the process that must be followed in notifying the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring the delivery of the initial privacy training when an employee or other person acting on behalf of the PO has commenced or will commence an employment, contractual, or other relationship with the PO
- identify the employee(s) and other person(s) acting on behalf of the PO 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 PO under Part V.1 of PHIPA and the duties and responsibilities that arise as a result of this status
- a description of the purposes for which custodians provide PHI to the PO
- a description of the nature of the PHI custodians provide to the PO
- an explanation of the purposes for which employees and any other person acting on behalf of the PO may view, handle, or otherwise deal with PHI received to develop or maintain the EHR
- limitations placed on viewing, handling, or otherwise dealing with PHI by employees and other persons acting on behalf of the PO
- a description of the manner in which the employees and any other person acting on behalf of the PO'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 viewing, handling, or otherwise dealing with PHI if other information, such as de-identified and/or aggregate information, will serve the purpose identified, and more PHI than is reasonably necessary
- a description of the procedure that must be followed in the event that an employee or other person acting on behalf of the PO is requested to apply a consent directive to PHI in the EHR developed or maintained by the PO
- a description of the procedure that must be followed in the event that the PO receives a Minister request or direction to provide PHI to the Minister or another person
- an overview of the privacy policies, procedures, practices that have been implemented by the PO and the obligations arising from these policies, procedures, and practices
- the consequences of a 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 employee(s) and other person(s) acting on behalf of the PO that have been delegated day-to-day authority to manage the privacy program
- the administrative, technical, and physical safeguards implemented by the PO to ensure that PHI accessible by means of the EHR is protected 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 employees and other persons acting on behalf of the PO in implementing the administrative, technical, and physical safeguards implemented by the PO
- the purposes for which de-identified or aggregated information derived from PHI provided to the PO to develop or maintain the EHR may be viewed, handled, or otherwise dealt with by employees or other persons acting on behalf of the PO, and a prohibition on using de-identified or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is permitted by PHIPA or another Act, and a notice that compliance with this prohibition will be audited and monitored
- the nature and purpose of Privacy Notices and Confidentiality Agreements and End User Agreements that employees and other persons acting on behalf of the PO must execute, 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 employees and other persons acting on behalf of the PO in identifying, reporting, containing, and participating in the investigation and remediation of privacy breaches, including the duty to notify the PO, at the first reasonable opportunity, of a privacy breach or a suspected privacy breach
- an explanation of the mandatory nature of privacy training, including the:
    - prohibition on all employees and other persons acting on behalf of the PO 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 employees and other persons acting on behalf of the PO 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
- 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

- amendments to PHIPA and its regulations relevant to the PO

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:

- employee(s) and other person(s) acting on behalf of the PO 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, including the required content of the documentation
- where documentation related to completion of the initial and ongoing privacy training will be retained
- employee(s) and other person(s) acting on behalf of the PO:
  - responsible for completing, providing, and/or executing the documentation
  - to whom this documentation must be provided
  - responsible for retaining this documentation

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

- employee(s) and other person(s) acting on behalf of the PO responsible for identifying employee(s) and other person(s) acting on behalf of the PO 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
- consequences for employees and other persons acting on behalf of the PO failing to complete the required privacy training within the identified timeframe, which must include the PO's refusal or withdrawal of the permission for an employee or other person acting on behalf of the PO to view, handle, or otherwise deal with PHI

Other Mechanisms to Foster a Privacy Culture

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

- other mechanisms implemented by the PO to foster a culture of privacy and to raise awareness of PHIPA, the privacy program, and the privacy policies, procedures, and practices implemented
- frequency with which the PO communicates with its employees and other persons acting on behalf of the PO in relation to privacy
- method and nature of the communication

- employee(s) and other person(s) acting on behalf of the PO and other persons acting on behalf of the PO responsible for the communication

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

Relationship to Policy, Procedures, and Practices for 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 PO must maintain a log of the completion of the initial and ongoing privacy training by the employee(s) or other person(s) acting on behalf of the PO. At a minimum, the log must set out the:

- name of each employee or other person acting on behalf of the PO
- date that the employee(s) or other person(s) acting on behalf of the PO commenced their employment, contractual, or other relationship with the PO
- date that the employee(s) or other person(s) acting on behalf of the PO completed the initial privacy training
- each date that the employee(s) or other person(s) acting on behalf of the PO 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 the employee(s) or other person(s) acting on behalf of the PO 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 the employee(s) or other person(s) acting on behalf of the PO 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 the employee(s) or other person(s) acting on behalf of the PO to complete the initial information security training prior to viewing, handling, or otherwise dealing with PHI received to develop or maintain the EHR, including PHI that has ben de-identified and/or aggregated
- require the employee(s) or other person(s) acting on behalf of the PO to complete ongoing information security training provided by the PO on an annual basis thereafter
- 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 employee(s) and other person(s) acting on behalf of the PO 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 annually, and updated, as needed
- specify the frequency with which the training will be reviewed
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for reviewing and updating the training
- set out a process that must be followed in notifying the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring the delivery of the initial information security training when an employee or other person acting on behalf of the PO has commenced or will commence an employment, contractual, or other relationship with the PO
- identify the employee(s) and other person(s) acting on behalf of the PO and other person(s) acting on behalf of the PO responsible for providing such notification
- specify the timeframe within which notification must be provided including 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 PO and the obligations arising from these policies, procedures, and practices
- the consequences of a breach of PHIPA or its regulations or a 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 employee(s) and other person(s) acting on behalf of the PO who have been delegated day-to-day authority to manage the information security program
- the administrative, technical, and physical safeguards implemented by the PO to ensure that PHI accessible by means of the EHR is protected 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 employees and other persons acting on behalf of the PO in implementing the administrative, technical, and physical safeguards implemented by the PO
- an explanation of the ***Policy, Procedures, and Practices for Information Security Breach Management*** and the related duties and responsibilities imposed on employees and other persons acting on behalf of the PO in identifying, reporting, containing, and participating in the investigation and remediation of information security breaches, including the duty to provide notification to the PO at the first reasonable opportunity of an information security breach or information security incident
- an explanation of the mandatory nature of information security training, including the prohibition on all employees and other persons acting on behalf of the PO 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 employees and other persons acting on behalf of the PO 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
- 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
        - 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
    - amendments to PHIPA and its regulations relevant to the PO

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:

- the employee(s) and other person(s) acting on behalf of the PO responsible for maintaining such a log
- the process to be followed in tracking completion of the initial and ongoing information security training
- the documentation that must be completed, provided, and/or executed to verify completion, including the required content of the documentation
- where documentation related to the completion of the initial and ongoing information security training will be retained
- the employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing the documentation
    - to whom this documentation must be provided
    - responsible for retaining this documentation

The policy, procedures, and practices must also:

- identify the employee(s) and other person(s) acting on behalf of the PO responsible for identifying employee(s) and other person(s) acting on behalf of the PO 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
- set out the consequences for employees and other persons acting on behalf of the PO failing to complete the required information security training within the identified timeframe, which must include the PO's refusal or withdrawal of employee or other person acting on behalf of the PO's permission to view, handle, or otherwise deal with PHI

Other Mechanisms to Raise Information Security Awareness

The policy, procedures, and practices must also address:

- other mechanisms implemented by the PO to raise awareness of the information security program and the information security policies, procedures, and practices implemented
- frequency with which the PO communicates with its employees and other persons acting on behalf of the PO in relation to information security
- the method and nature of the communication
- employee(s) and other person(s) acting on behalf of the PO responsible for the communication

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require the employee(s) or other person(s) acting on behalf of the PO to comply with the policy, procedures, and practices
- require the employee(s) and other person(s) acting on behalf of the PO to notify the PO at the first reasonable opportunity, in accordance with the ***Policy, Procedures, and Practices for Information Security Breach Management***, if an employee or other person acting on behalf of the PO breaches or believes there may have been a breach of this policy, procedures, or practices
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices in Respect of 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 PO must maintain a log of the completion of the initial and ongoing information security training by employees and other persons acting on behalf of the PO. At a minimum, the log must set out the:

- name of the employee(s) or other person(s) acting on behalf of the PO
- date that the employee(s) or other person(s) acting on behalf of the PO commenced their employment, contractual, or other relationship with the PO
- dates that the employee(s) or other person(s) acting on behalf of the PO completed the initial information security training
- each date the employee(s) or other person(s) acting on behalf of the PO completed ongoing information security training

Confidentiality Agreements

5. Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Employees and Other Persons Acting on Behalf of the Prescribed Organization

A policy, procedures, and practices must be developed and implemented requiring employees and other persons acting on behalf of the PO to execute a Confidentiality Agreement that contains the requirements set out in the ***Template Confidentiality Agreement with Employees and Other Persons Acting on Behalf of the Prescribed Organization***.

Timing of Confidentiality Agreements

The policy, procedures, and practices must set out the timeframe within which employees and other persons acting on behalf of the PO must execute the Confidentiality Agreement. At a minimum, the policy, procedures, and practices must:

- require employees and other persons acting on behalf of the PO to execute a Confidentiality Agreement prior to viewing, handling, or otherwise dealing with PHI, including PHI that has been de-identified and/or aggregated, and on an annual basis thereafter
- identify the timeframe each year within which employees and other persons acting on behalf of the PO 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:

- employee(s) and other person(s) acting on behalf of the PO responsible for ensuring that each employee or other person acting on behalf of the PO executes a Confidentiality Agreement in compliance with the policy, procedures, and practices of the PO

- process for notifying the responsible employee(s) and other person(s) acting on behalf of the PO each time an employee or other person acting on behalf of the PO has commenced or will commence an employment, contractual, or other relationship with the PO
- employee(s) and other person(s) acting on behalf of the PO responsible for providing such notification
- timeframe within which such notification must be provided
- 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 employee(s) and other person(s) acting on behalf of the PO responsible for maintaining the log and for tracking and ensuring that the Confidentiality Agreements have been executed
- outline the process that must be followed by the responsible employee(s) and other person(s) acting on behalf of the PO in tracking and ensuring the execution of Confidentiality Agreements, including the process that must be followed:
    - where an employee or other person acting on behalf of the PO'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, including the required content of the documentation
- where documentation related to the Confidentiality Agreements will be retained and
- the employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, executing, and ensuring the execution of the documentation
    - to whom this documentation must be provided
    - responsible for retaining this documentation

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

6. Template Confidentiality Agreement with Employees and Other Persons Acting on Behalf of the Prescribed Organization

A **Confidentiality Agreement** must be executed by each employee or other person acting on behalf of the PO in accordance with the ***Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Employees and Other Persons Acting on Behalf of the Prescribed Organization*** that, at a minimum, addresses the matters set out below.

General Provisions

The **Confidentiality Agreement** must:

- describe the status of the PO under PHIPA and the duties and responsibilities arising from this status
- state that individuals executing the agreement are acting on behalf of the PO 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” that are consistent with PHIPA and its regulations

Required Compliance

The **Confidentiality Agreement** must require employees and other persons acting on behalf of the PO to:

- comply with the:
    - provisions of PHIPA and its regulations relating to the role of the PO
    - terms of the Confidentiality Agreement as may be amended from time to time
- acknowledge that they have read, understood, and agree to comply with:

- the privacy and information security policies, procedures, and practices implemented by the PO
- 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 Viewing, Handling, or Otherwise Dealing with Personal Health Information

The **Confidentiality Agreement** must:

- identify the purposes for which employees and other persons acting on behalf of the PO are permitted to view, handle, or otherwise deal with PHI received by the PO to develop or maintain the EHR and any limitations, conditions, or restrictions imposed thereon. In identifying the purposes, the PO must ensure that each instance of viewing, handling, or otherwise dealing with PHI identified in the Confidentiality Agreement is permitted by:
  - PHIPA and its regulations
  - the policies, procedures, and practices implemented by the PO pursuant thereto
- prohibit employees and other persons acting on behalf of the PO from viewing, handling, or otherwise dealing with PHI except as permitted in the Confidentiality Agreement or as required by law
- prohibit employees and other persons acting on behalf of the PO from viewing, handling, or otherwise dealing with:
  - PHI if other information will serve the purpose
  - 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 the employee(s) or other person(s) acting on behalf of the PO are permitted to use and disclose PHI which has been de-identified or aggregated, as the case may be
- prohibit employees and other persons acting on behalf of the PO from using the de-identified or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is permitted by PHIPA or another Act. This must include prohibiting any attempt to:
  - decrypt information that is encrypted or
  - identify an individual based on unencrypted information and/or prior knowledge

Termination of the Contractual, Employment or Other Relationship

The **Confidentiality Agreement** must:

- require the employee(s) or other person(s) acting on behalf of the PO to securely return all property of the PO, including records of PHI and all identification cards, access cards, and/or keys, on or before the date of termination or 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*** and
- stipulate the:
    - timeframe within which the property of the PO must be securely returned
    - secure manner in which the property must be returned
    - employee(s) or other person(s) acting on behalf of the PO to whom the property must be securely returned

Breach Notification to Prescribed Organization

At a minimum, the Confidentiality Agreement must require the employee(s) or other person(s) acting on behalf of the PO to notify the PO 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 employee(s) or other person(s) acting on behalf of the PO breaches or believes that there may have been a breach of the Confidentiality Agreement, or if the employee(s) or other person(s) acting on behalf of the PO breaches or believes that there may have been a breach of the privacy or information security policies, procedures, and practices implemented by the PO.

Consequences of Breach and Monitoring Compliance

The **Confidentiality Agreement** must:

- outline the consequences of a 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
- address the manner in which compliance will be audited

7. Log of Executed Confidentiality Agreements with Employees and Other Persons Acting on Behalf of the Prescribed Organization

A PO must maintain a log of **Confidentiality Agreements** that have been executed by the employee(s) or other person(s) acting on behalf of the PO at the commencement of their employment, contractual, or other relationship with the PO and on an annual basis thereafter. At a minimum, the log must include the:

- name of the employee(s) or other person(s) acting on behalf of the PO

- date of commencement of the employment, contractual, or other relationship with the PO
- 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 PO 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
- 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 the employee(s) or other person(s) acting on behalf of the PO are aware of PHIPA and its regulations and their duties thereunder
    - ensuring the employee(s) or other person(s) acting on behalf of the PO are aware of the privacy policies, procedures, and practices implemented by the PO 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
    - receiving and responding to requests to make, withdraw, or modify a consent directive in relation to PHI accessible by means of the EHR pursuant to the ***Policy, Procedures, and Practices for Managing Consent in the Electronic Health Record***
    - receiving and responding to directions from the Minister for the provision of PHI accessible by means of the EHR pursuant to the ***Policy, Procedures, and Practices for the Provision of Personal Health Information Pursuant to a Direction Issued by the Minister***
    - receiving and responding to request for access and correction of records of PHI accessible by means of the EHR pursuant to the ***Policy, Procedures, and Practices for Responding to Request for Access and Correction of Records of Personal Health Information***

- ensuring the EHR is audited and monitored pursuant to the ***Policy, Procedures, and Practices for Logging, Monitoring, and Auditing Privacy and Information Security Events***
- receiving and responding to requests from custodians and the IPC for the electronic records that the PO is required to maintain pursuant to the ***Policy, Procedures, and Practices for Logging, Monitoring, and Auditing Privacy and Information Security Events***
- 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***
- 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 PO must be developed. The job description must:

- set out the reporting relationship of the position(s) to the chief executive officer or the executive director (or equivalent position), as the case may be
- 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 the employee(s) or other person(s) acting on behalf of the PO are aware of the information security policies, procedures, and practices implemented by the PO 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***
- 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 the employee(s) or other person(s) acting on behalf of the PO, as well as their supervisors, to notify the PO of the termination or cessation of the employment, contractual, or other relationship
- identify the:
  - employee(s) and other person(s) acting on behalf of the PO to whom notification must be provided
  - nature and format of the notification
  - timeframe within which notification must be provided
  - process that must be followed in providing notification

Secure Return of All Property

The policy, procedures, and practices must also require employees and other persons acting on behalf of the PO to securely return all property of the PO 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, de-identified and aggregate information that has been derived from PHI, computing equipment, mobile devices, identification cards, access cards and/or keys.

The policy, procedures, and practices must identify the:

- employee(s) and other person(s) acting on behalf of the PO 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

- employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation, including the required content of the documentation
- procedure to be followed in the event that the property of the PO is not securely returned upon termination or cessation of the employment, contractual, or other relationship
- employee(s) and other person(s) acting on behalf of the PO 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 PO, to locations within the premises where records of PHI are retained, to components within the information environment, be immediately terminated upon the termination or cessation of the employment, contractual or other relationship
- identify the:
    - employee(s) and other person(s) acting on behalf of the PO 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
    - employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

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

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

Discipline and Corrective Action

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

The PO must develop and implement a policy, procedures, and practices for discipline and corrective action taken with respect to employees and other persons acting on behalf of the PO who breach obligations and responsibilities in respect of protecting the privacy and confidentiality of individuals whose PHI the PO receives.

The policy, procedures, and practices must address:

- the investigation of disciplinary matters, including the employee(s) or other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or executing the documentation
- the required content of the documentation
- the employee(s) and other person(s) acting on behalf of the PO 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 PO on its employee(s) and other person(s) acting on behalf of the PO
- factors that must be considered in determining the appropriate discipline and corrective action to be taken
- employee(s) and other person(s) acting on behalf of the PO responsible for determining the appropriate discipline and corrective action
- procedure to be followed in making this determination
- employee(s) and other person(s) acting on behalf of the PO who must be consulted in making this determination
- 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
- the employee(s) and other person(s) acting on behalf of the PO 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
- the privacy policies, procedures, and practices implemented by the PO

Accountability for Compliance

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 PO and its employees and other persons acting on behalf of the PO comply with:

- PHIPA and its regulations
- the privacy policies, procedures, and practices implemented by the PO

Individuals, Committees and Teams that Support the Privacy Program

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 employees and other persons acting on behalf of the PO
- identify the employee(s) and other person(s) acting on behalf of the PO 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 on the privacy program which, at a minimum, should be annually, and preferably in the form of a written report
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for providing such updates
- set out the method and manner by which the Board of Directors is required to be updated
- identify the type of matters the Board of Directors is required to be updated on

The update provided to the Board of Directors must, at a minimum, address risks that may negatively affect the PO's ability to protect the privacy and confidentiality of individuals whose PHI is received 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 PO
- privacy related issues that have been identified through whistle-blowers
- 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 PO must be established.

Accountability for Compliance

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
- PO and its employee(s) and other person(s) acting on behalf of the PO comply with the information security policies, procedures, and practices implemented

Individuals, Committees and Teams that Support the Security Program

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 employees and other persons acting on behalf of the PO
- identify the employee(s) and other person(s) acting on behalf of the PO 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 provided 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
- employee(s) and other person(s) acting on behalf of the PO responsible for providing such updates

The update provided to the Board of Directors must, at a minimum, address risks that may negatively affect the PO's ability to protect the privacy and confidentiality of individuals whose PHI is received 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 PO, and the measures that have been implemented 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 PO
- information security related issues that have been identified through whistle-blowers
- 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 PO 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
- 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
- the frequency of these reports

Risk Management

4. Corporate Risk Management Framework

A PO 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 and confidentiality of individuals whose PHI is received for the purpose of developing of maintaining the EHR.

Risk Identification, Assessment and Ranking

The corporate risk management framework must address the:

- employee(s) and other person(s) acting on behalf of the PO responsible and
- process that must be followed and criteria that must be considered in identifying privacy and information security-related risks that may negatively affect the ability of the PO to protect the privacy and confidentiality of individuals whose PHI is received to develop or maintain the EHR, and ranking them in terms of their likelihood of occurrence and their potential impact, which must include a discussion of the:
    - employee(s) or other person(s) acting on behalf of the PO 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
    - employee(s) and other person(s) acting on behalf of the PO responsible for completing, providing, and/or ensuring the execution of the documentation
    - required content of the documentation, including a description of the rationale underlying the assessment and ranking of risks
    - employee(s) and other person(s) acting on behalf of the PO to whom this documentation must be provided

Risk Mitigation

The corporate risk management framework must identify the:

- employee(s) and other person(s) acting on behalf of the PO responsible
- process that must be followed
- 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:

- employee(s) and other person(s) acting on behalf of the PO or other persons or organizations that must be consulted in identifying and implementing the mitigation strategies
- employee(s) and other person(s) acting on behalf of the PO, and other persons or organizations responsible for:
    - assigning other employee(s) and other person(s) acting on behalf of the PO 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
    - evaluating the residual risks remaining after implementation
- documentation that must be completed, provided, and/or executed
- employee(s) and other person(s) acting on behalf of the PO 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
- employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for determining whether to approve and endorse, or to not approve and endorse, the results of the risk management process
- 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
    - employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO 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
    - 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)
- outline the process that must be followed for the approval and endorsement of the results of the risk management process, including the employee(s) and other person(s) acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO responsible for the review
- 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 PO must:

- ensure that the risks identified in the corporate risk management framework are addressed in the policies, procedures, and practices of the PO and in the projects undertaken by the PO
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring that the risks are addressed

Compliance, Audit, and Enforcement

The policy, procedures, and practices must:

- require the employee(s) or other person(s) acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) and other person(s) acting on behalf of the PO to notify the PO 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 employee or other

person acting on behalf of the PO breaches or believes there may have been breach of this policy, procedures, or practices

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

5. Corporate Risk Register

A PO 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 PO to protect the privacy and confidentiality of individuals whose PHI is received for the purpose of developing and maintaining the EHR
- 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
        - employee(s) and other person(s) acting on behalf of the PO responsible for implementation of the mitigation strategy
        - residual risk likely to remain despite implementation of the mitigation strategy

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

A PO 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

- sets out the:
    - frequency with which and the circumstances in which the consolidated and centralized log must be reviewed
    - employee(s) and other person(s) acting on behalf of the PO responsible for reviewing and amending the log
    - 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
- one or more recommendation(s), order(s), or decision(s), 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 mitigation(s)/recommendation(s), order(s), and decision(s), 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 employees and other persons acting on behalf of the PO to comply with the policy, procedures, and practices
- require employee(s) and other person(s) acting on behalf of the PO to notify the PO 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 employee or other person acting on behalf of the PO breaches or believes there may have been breach of this policy, procedures, or practices
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices In Respect of Privacy Audits***

7. Consolidated Log of Recommendations

The consolidated log of recommendations of a PO 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
- 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, order or decision, 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
        - employee(s) and other person(s) acting on behalf of the PO 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 PO in the event of:

- short and long-term business interruptions
- threats to the operating capabilities of the PO, 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
- 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:

- employee(s) and other person(s) acting on behalf of the PO 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 PO
- employee(s) and other person(s) acting on behalf of the PO responsible for providing such notification
- timeframe within which notification must be provided, including the manner and format of the notification
- nature of the information that must be provided upon notification
- process for developing and maintaining an updated contact list of all custodians, employees, and other persons acting on behalf of the PO, service providers, stakeholders, and other persons or organizations that must be notified
- employee(s) and other person(s) acting on behalf of the PO responsible for creating and maintaining this contact list
- 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:

- the employee(s) and other person(s) acting on behalf of the PO responsible for the assessment
- the criteria pursuant to which this assessment is to be made
- the employees and other persons acting on behalf of the PO 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 employee(s) and other person(s) acting on behalf of the PO to whom the documentation must be provided
- 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:

- employee(s) and other person(s) acting on behalf of the PO responsible for the business continuity and disaster recovery plan
- 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 PO

In outlining the initial impact assessment process to be followed, the business continuity and disaster recovery plan must identify the:

- employee(s) and other person(s) acting on behalf of the PO and other person(s) or organization(s) that must 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
- employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing the documentation
    - to whom the documentation must be provided
    - 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:

- employee(s) and other person(s) acting on behalf of the PO 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
- employee(s) and other person(s) acting on behalf of the PO 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
- employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing the documentation
    - to whom the documentation must be provided
    - 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:

- employee(s) and other person(s) acting on behalf of the PO 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
- employee(s) or other person(s) acting on behalf of the PO 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, including the required content of the documentation
- employee(s) and other person(s) acting on behalf of the PO:
    - responsible for completing, providing, and/or executing this documentation
    - to whom the documentation must be provided
    - to whom the results of these activities must be communicated

Documenting Business Interruptions and Threats

The policy, procedures, and practices must detail:

- how decisions are made, and actions taken during business interruptions and threats to the operating capabilities of the PO will be documented and communicated
- the employee(s) and other person(s) acting on behalf of the PO responsible
- 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:

- employee(s) and other person(s) acting on behalf of the PO responsible for developing and maintaining the inventory
- employee(s) and other person(s) acting on behalf of the PO and other person(s) and organization(s) that must be consulted in developing the inventory
- 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
- procedure to be followed in testing, maintaining, assessing, and amending the business continuity and disaster recovery plan
- employee(s) and other person(s) acting on behalf of the PO responsible for:
    - ensuring that the business continuity and disaster recovery plan is tested, maintained, and assessed
    - amending the business continuity and disaster recovery plan as a result of the testing
    - 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 employee(s) and other person(s) acting on behalf of the PO responsible and the procedure to be followed in communicating the business continuity and disaster recovery plan to all employees and other persons acting on behalf of the PO, including:
    - any amendments thereto
    - the method and nature of the communication
- the employee(s) and other person(s) acting on behalf of the PO 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 the employee(s) or other person(s) acting on behalf of the PO to comply with the policy, procedures, and practices

- require employee(s) and other person(s) acting on behalf of the PO to notify the PO 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 employee or other person acting on behalf of the PO breaches or believes there may have been breach of this policy, procedures, or practices
- identify the employee(s) and other person(s) acting on behalf of the PO responsible for ensuring compliance with the policy, procedures, and practices
- address how and by whom compliance will be enforced and the consequences of a breach, in accordance with the ***Policy, Procedures, and Practices for Discipline and Corrective Action***
- stipulate that compliance will be audited in accordance with the ***Policy, Procedures, and Practices In Respect of Privacy Audits***

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 PO 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 the employee(s) or other person(s) acting on behalf of the PO and, for each amended and newly developed privacy policy, procedure, and practice communicated to employee(s) or other person(s) acting on behalf of the PO, 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.
Receiving Personal Health Information	• The number of repositories containing PHI that are accessible by means of the EHR. • The number of descriptions of types of PHI received by the PO to develop or maintain the EHR. • The number and a list of the descriptions of types of PHI received by the PO to develop or maintain the EHR that were reviewed since the prior review by the IPC. • Whether existing descriptions of types of PHI were updated as a result of the review, including a brief description of the updates made.

Categories	Privacy Indicators
Consent Management in the Electronic Health Record	• The number of instances in which a consent directive has been made, modified, or withdrawn since the prior review by the IPC. • The number of instances in which a notice of a consent directive has been provided to a custodian in accordance with subsection 55.6(7) of PHIPA since the prior review by the IPC. • The number of instances in which a custodian has overridden a consent directive pursuant to section 55.7 of PHIPA since the prior review by the IPC and the number of occasions on which each of subsection 55.7(1), (2) or (3) of PHIPA was invoked to override the consent directive. • The number of instances in which a notice of a consent override has been provided to a custodian in accordance with subsection 55.7(6) of PHIPA since the prior review by the IPC. • The dates on which reports of consent overrides were made to the IPC pursuant to paragraph 16 of section 55.3 of PHIPA since the prior review by the IPC. • The number of requests received from custodians pursuant to paragraph 9 of section 55.3 of PHIPA for the electronic records of consent directives and consent overrides since the prior review by the IPC. • The number of requests received from the IPC pursuant to paragraph 8 of section 55.3 for the electronic records of consent directives and consent overrides since the prior review by the IPC.
Viewing, Handling, or Otherwise Dealing with Personal Health Information	• The number of employee(s) or other person(s) acting on behalf of the PO granted approval to view, handle, or otherwise deal with PHI since the prior review by the IPC.
Provision of Personal Health Information Pursuant to Direction	• The number of directions issued by a member of a MDIU pursuant to subsection 55.9(3) of PHIPA requiring the PO to provide to the member of the MDIU PHI that is accessible by means of the EHR since the prior review by the IPC. • The number of directions issued by the Minister requiring the PO to provide PHI that is accessible by means of the EHR to a person for the purposes of subsection 55.10(1) of PHIPA since the prior review by the IPC. • The number of directions issued by the Minister requiring the PO to provide PHI that is accessible by means of the EHR to a prescribed person for the purposes of clause 39(1)(c) of PHIPA since the prior review by the IPC.

Categories	Privacy Indicators
Provision of Personal Health Information Pursuant to Direction (Cont'd)	• The number of directions issued by the Minister requiring the PO to provide PHI that is accessible by means of the EHR to a person for the purposes of subsection 39(2) of PHIPA since the prior review by the IPC. • The number of directions issued by the Minister requiring the PO to provide PHI that is accessible by means of the EHR to a researcher for the purposes of section 44 of PHIPA since the prior review by the IPC. • The number of directions issued by the Minister requiring the PO to provide PHI that is accessible by means of the EHR to a prescribed entity for the purposes of section 45 of PHIPA since the prior review by the IPC.
Access and Correction	• The number of requests made by individuals to access records of PHI that are accessible by means of the EHR since the prior review by the IPC. • The number of requests made by individuals to correct records of PHI that are accessible by means of the EHR since the prior review by the IPC. • The number of refusals under PHIPA of a request for access to a record, the provisions of PHIPA under which access was refused, and the number of occasions on which each provision was invoked. • The number of refusals under PHIPA of a request to correct a record, the provisions of PHIPA under which the correction was refused, and the number of occasions on which each provision was invoked. • The amount of fees collected by the PO under subsection 54(10) of PHIPA, if any.
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.

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:
	  ○ a description of the existing or proposed system that retrieves, processes, or integrates PHI that is accessible by means of the EHR, as the case may be
	  ○ a description of the type(s) of PHI that will be provided to the PO to develop or maintain the EHR, as the case may be
	  ○ for each system that retrieves or will retrieve, process, or integrate PHI, a description of the types of PHI that is or will be retrieved, processed, or integrated

Categories	Privacy Indicators
Privacy Impact Assessments (Cont'd)	○ the date of completion of the privacy impact assessment ○ a brief description of each finding, mitigation, or other recommendation ○ the date each mitigation or other recommendation was addressed or is expected to be addressed ○ the manner in which each mitigation or other recommendation was addressed or is expected to be addressed • The number and a list of privacy impact assessments undertaken but not completed since the prior review by the IPC and the proposed date of completion. • The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion. • The number of determinations made since the prior review by the IPC that a privacy impact assessment is not required and, for each determination, the existing or proposed system that retrieves, processes, or integrates PHI, and a description of the types of PHI that is or will be retrieved, processed, or integrated that is 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	• For the electronic records the PO is required to keep pursuant to paragraphs 5 and 6 of section 55.3 and to audit and monitor pursuant to paragraph 7 of section 55.3 of PHIPA, since the prior review by the IPC: ○ 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, type, and scope of each audit conducted - the date of completion of the audit - a brief description of each recommendation made - the date each recommendation was addressed or is expected to be addressed - the manner in which each recommendation was addressed or is expected to be addressed

Categories	Privacy Indicators
Privacy Audit Program (Cont'd)	• The dates of audits of employee(s) or other person(s) acting on behalf of the PO granted approval to view, handle, or otherwise deal with PHI since the prior review by the IPC and for each audit conducted: ○ the date of completion of the audit ○ a brief description of each recommendation made ○ the date each recommendation was addressed or is expected to be addressed ○ the manner in which each recommendation was addressed or is expected to be addressed • The number and a list of audits completed to assess compliance with the privacy policies, procedures, and practices implemented by the PO completed since the prior review by the IPC and for each audit: ○ the date of completion of the audit ○ a brief description of each recommendation made ○ the date each recommendation was addressed or is expected to be addressed ○ the manner in which each recommendation was addressed or is expected to be addressed • The number and a list of all other privacy audits completed since the prior review by the IPC and for each audit: ○ a description of the nature and type of audit conducted ○ the date of completion of the audit ○ a brief description of each recommendation made ○ the date each recommendation was addressed or is expected to be addressed ○ the manner in which each recommendation was addressed or is expected to be addressed.

Categories	Privacy Indicators
Privacy Breaches	• The total number of notifications of privacy breaches or suspected privacy breaches received by the PO since the prior review by the IPC. This indicator may be further subdivided to distinguish between privacy breaches that constitute: ○ a custodian's collection, use, or disclosure of PHI that is not in compliance with PHIPA or its regulations ○ an instance where PHI is viewed, handled, or otherwise dealt with by an employee or other person acting on behalf of the PO, in a way that does not comply with PHIPA or its regulations ○ a contravention of the privacy policies, procedures, or practices implemented by the PO, related to the requirements of the Manual ○ a contravention of written acknowledgments, Confidentiality Agreements and TPSP Agreements, related to the requirements of the Manual ○ 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 number of privacy breaches identified by the PO since the prior review by the IPC ○ The number of privacy breaches caused by one or more custodian(s) ○ The number of privacy breaches caused by the PO or a system that retrieves, processes, or integrates PHI in the EHR ○ The number of privacy breaches caused by a person who is not an employee or other person acting on behalf of the PO or an agent or electronic service provider of a custodian • 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

Categories	Privacy Indicators
Privacy Breaches (Cont'd)	○ 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 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 ○ whether an unauthorized person who is not an employee or other person acting on behalf of the PO, or an agent or electronic service provider of a custodian 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 ○ 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
	  ○ the date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint
	• Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the IPC, and with respect to each privacy complaint not investigated:
	  ○ the date that the privacy complaint was received
	  ○ the nature of the privacy complaint
	  ○ the date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter

Part 2 – Information Security Indicators

Categories	Information Security Indicators
General Information Security Policies, Procedures, and Practices	• The completion date of each review of each information security policy, procedure, and practice by the PO 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 employees and other persons acting on behalf of the PO and, for each amended and newly developed information security policy, procedure, and practice communicated to employees and other persons acting on behalf of the PO, and 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 employees and other persons acting on behalf of the PO 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 finding, mitigation and any other recommendation made ○ the date each finding, mitigation and any other recommendation was addressed or is expected to be addressed ○ the manner in which each finding, mitigation, and any other recommendation was addressed or is expected to be addressed
Acceptable Use Agreements	• The number of Acceptable Use Agreements acknowledged and agreed to by the employee(s) or other person(s) acting on behalf of the PO since the prior review by the IPC.

Categories	Information Security Indicators
End User Agreements	• The number of End User Agreements acknowledged and agreed to by end users who provide PHI to or collect PHI by means of the EHR.
Information Security	• The number of instances in which the PO failed to conduct vulnerability scanning in accordance with the ***Policy, Procedures, and Practices for Vulnerability and Patch Management*** since the prior review by the IPC, and for each instance the: ○ time and date of the failure to conduct vulnerability scanning ○ nature of the failure ○ reason for the failure ○ time and date at which vulnerability scanning resumed • The number of instances in which any patches or other mitigation methods were not implemented within the required timelines to address risks rated with high severity or critical severity or for which a decision was made to not implement a patch or other mitigation method, and for each instance: ○ the severity level of the patch or other mitigation method ○ a description of the patch or other mitigation method ○ a brief description of the reason why the patch or other mitigation method was not implemented within the required timeframe or why a decision was made to not implement the patch or other mitigation method.
Information Security Audit Program	• The number of requests received from custodians pursuant to paragraph 9 of section 55.3 for the electronic records that the PO is required to keep pursuant to paragraph 4 of section 55.3 of PHIPA, since the prior review by the IPC. • The number of requests received from the IPC pursuant to paragraph 8 of section 55.3 for the electronic records that the PO is required to keep pursuant to paragraph 4 of section 55.3 of PHIPA, since the prior review by the IPC. • For the electronic records the PO is required to keep pursuant to paragraph 4 of section 55.3 and to audit and monitor pursuant to paragraph 7 of section 55.3 of PHIPA, since the prior review by the IPC: ○ the number of audits conducted or the frequency with which the audits have been conducted ○ the nature and scope of each audit conducted ○ the date of completion of the audit ○ a brief description of each recommendation made

Categories	Information Security Indicators
Information Security Audit Program (Cont'd)	○ 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 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 PO were unavailable, unattended or there was otherwise a failure to monitor in accordance with the ***Policy, Procedures, and Practices for Logging, Monitoring, and Auditing Privacy and Information Security Events*** since the prior review by the IPC, and for each instance the: ○ time and date of the monitoring failure ○ nature of the failure ○ reason for the failure ○ time and date at which monitoring resumed • The number of high vulnerabilities and the number of critical vulnerabilities identified by vulnerability assessments conducted on the results of vulnerability scans since the prior review by the IPC. • The number of instances in which recommendations to mitigate high or critical vulnerabilities identified by vulnerability assessments conducted on the results of vulnerability scans since the prior review by the IPC were not implemented in accordance with the required timeframe and, if so, for each instance: ○ the risk severity of the vulnerability ○ a description of the vulnerability ○ a brief description of the reason why each recommendation to mitigate the vulnerability was not implemented in accordance with the timeframe ○ the number of information security components within the information environment for which each recommendation was not implemented in accordance with the timeframe

Categories	Information Security Indicators
Information Security Audit Program (Cont'd)	• The number and a list of all other 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 finding, mitigation, or other recommendation made ○ the date that each finding, mitigation, or other recommendation was addressed or is expected to be addressed ○ the manner in which each finding, mitigation or other recommendation was addressed or is expected to be addressed
Threat and Risk Assessments	• The date of all threat and risk assessments that have been completed since the prior review by the IPC and for each threat and risk assessment: ○ the system that is at issue ○ the date the threat and risk assessment was completed or is expected to be completed ○ a brief description of the findings, mitigations or other recommendations arising from the threat and risk assessment ○ the date each finding, mitigation or other recommendation was or is expected to be addressed ○ the manner in which each finding, mitigation or other recommendation was 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 PO 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 ○ 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 PO, related to the requirements of the Manual

Categories	Information Security Indicators

Information Security Breaches (Cont'd)	• The number of information security breaches identified since the prior review by the IPC.
	• The number of information security breaches caused by one or more custodian(s).
	• The number of information security breaches caused by the PO or a system that retrieves, processes, or integrates PHI in the EHR.
	• The number of information security breaches caused by a person who is not an employee or other person acting on behalf of the PO or an agent or electronic service provider of a custodian.
	• 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
	  ○ whether the information security breach or information security incident was caused by the PO
	  ○ whether the information security breach or information security incident was caused by a system that retrieves, processes, or integrates PHI in the EHR
	  ○ whether an unauthorized person who is not an employee or other person acting on behalf of the PO or an agent or electronic service provider of a custodian 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

Categories	Information Security Indicators
Information Security Breaches (Cont'd)	○ 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 ○ 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 employees and other persons acting on behalf of the PO 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 employee(s) or other person(s) acting on behalf of the PO who have yet to complete initial privacy training and the scheduled date of the initial privacy training. • The number of employee(s) or other person(s) acting on behalf of the PO 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 the employee(s) or other person(s) acting on behalf of the PO by the PO 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 employee(s) or other person(s) acting on behalf of the PO 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 employee(s) or other person(s) acting on behalf of the PO who have yet to complete initial information security training and the scheduled date of the initial information security training. • The number of employee(s) or other person(s) acting on behalf of the PO 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 employee(s) or other person(s) acting on behalf of the PO by the PO in relation to information security since the prior review by the IPC.
Confidentiality Agreements	• The number of employee(s) or other person(s) acting on behalf of the PO 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 employee(s) or other person(s) acting on behalf of the PO 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 employee(s) or other person(s) acting on behalf of the PO since the prior review by the IPC related to termination or cessation of their employment, contractual, or other relationship with the PO.

Part 4 – Organizational Indicators

Categories	Organizational Indicators
Risk Management	• The dates that the corporate risk register was reviewed by the PO 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 ORGANIZATION] 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 ORGANIZATION] who have more direct knowledge of the relevant matters.

2. [INSERT NAME OF PRESCRIBED ORGANIZATION] 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 ORGANIZATION] comply with the *Manual for the Review and Approval of Prescribed Organizations* 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 ORGANIZATION] in compliance with the *Manual for the Review and Approval of Prescribed Organizations*.

5. [INSERT NAME OF PRESCRIBED ORGANIZATION] 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	In relation to a health information custodian, means a person that, with the authorization of a custodian, acts for or on behalf of the custodian in respect of PHI for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian, and whether or not the agent is being remunerated. As defined in PHIPA
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 • 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 Executing Agreements with Third-Party Service Providers in Respect of Personal Health Information*** • ***Template Agreement for Third-Party Service Providers*** • ***Log of Agreements with Third-Party Service Providers*** • ***Policy, Procedures, and Practices for Secure Disposal of Records of Personal Health Information***
Confidentiality agreement	An agreement that is executed between the PO and each employee and other person acting on its behalf in accordance with the ***Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Employees and Other Persons Acting on Behalf of the Prescribed Organization*** and the ***Template Confidentiality Agreement with Employees and Other Persons Acting on Behalf of the Prescribed Organization***. 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***

Term	Definition
Confidentiality agreement (Cont'd)	• ***Policy, Procedures, and Practices for the Execution of Confidentiality Agreements by Employees and Other Persons Acting on Behalf of the Prescribed Organization*** • ***Template Confidentiality Agreement with Employees and Other Persons Acting on Behalf of the Prescribed Organization*** • ***Log of Executed Confidentiality Agreements with Employees and Other Persons Acting on Behalf of the Prescribed Organization***
EHR	Electronic health record.
Electric health record	Means the electronic systems that are developed and maintained by the PO to enable custodians to collect, use, and disclose PHI by means of the systems in accordance with Part V.1 of PHIPA and its regulations.
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 Complaints*** • ***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***
Employees and other persons acting on behalf of the Prescribed Organization	For purposes of this Manual, the term employee(s) and/or other person(s) acting on behalf of the prescribed organization(PO) is used to refer to individuals or organizations who act on behalf of the PO in respect of PHI for the purposes of the developing and maintaining the EHR, and not the employee or other person's own purposes, whether or not the employee or other person: • has the authority to bind the PO • is employed by the PO • is being remunerated

Term	Definition
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 are developed and maintained by the PO to enable custodians to collect, use, and disclose PHI by way of the EHR, 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 PO
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 Organizations* (this document).
MDIU	Ministry Data Integration Unit.
Minister	Minister of Health.
Ministry Data Integration Unit	Means a ministry data integration unit, as defined in section 49.1(1) of FIPPA, that is located within the Ministry of Health and is authorized to collect PHI by means of the EHR pursuant to section 55.9 of PHIPA.
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 organization	The organization or organizations prescribed for the purposes of Part V.1 of PHIPA, and that are prescribed in section 18.1 of PHIPA's regulations.
PO	Prescribed organization/prescribed organizations.
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 prescribed organization/prescribed organizations • a contravention of written acknowledgments, 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 PO and related to the compliance of the PO 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.
Should	Anytime the word 'should' appears in the Manual, it indicates a recommendation.
Statement of Requested Exceptions	A PO 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 PO must submit a written Statement of Inapplicability where one or more of the requirements in **appendix "A"** or **appendix "B"** is inapplicable to a PO. 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 contracted or otherwise engaged to provide services to or for the prescribed organization/prescribed organizations .
TPSP Agreement	An agreement executed between the PO 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 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 Organizations

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

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

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

June, 2024