ACCESSPRIVACY BY OSLER

IPC Prescribed Entities and Prescribed Persons Manual 2011 and 2024 Comparison: Part 1

The *Personal Health Information Protection Act, 2004* ("**PHIPA**") sets out a framework where certain entities ("**Prescribed Entities and Prescribed Persons**") in the Ontario health care sector, prescribed by regulation, are permitted to collect, use, and disclose personal health information ("**PHI**") without consent, if their practices are approved by the Information and Privacy Commissioner of Ontario ("**IPC**"). Prescribed Entities and Prescribed Persons must seek and obtain the IPC's approval every three years.

The IPC published the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* (the "**Manual**") in 2011.

The Manual sets out the IPC's expectations for Prescribed Entities and Prescribed Persons to demonstrate their accountability as trusted stewards of PHI. The Manual is over 150 pages and sets out the details of the privacy, information security, human resources and organizational policies, practices and procedures that the IPC expects Prescribed Entities and Prescribed Persons to have implemented in order to obtain approval of the IPC.

The Manual was substantially updated on January 19, 2024. The chart below sets out a comprehensive summary for Prescribed Persons and Prescribed Entities to identify and understand the requirements set out in the Manual, and the substantive updates to the Manual, as the 2024 Manual has more detailed and specific requirements and expectations in various sections, such as information security and business continuity.

While the Manual is designed for Prescribed Entities and Prescribed Persons, it can also be of valuable assistance to any organizations who collect, use, and/or disclose personal information as this Manual can act as a checklist for building a robust privacy and data management program and to demonstrate accountability for the personal information under their control.

***

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
PART I	**PRIVACY DOCUMENTATION**	**PRIVACY POLICIES, PROCEDURES AND PRACTICES**
Policy 1. **Privacy Policy In Respect of Its Status as a Prescribed Person or Prescribed Entity**	<u>Status under the *Act*</u>	
	• Must describe the status of the person or organization as a prescribed person or prescribed entity under the *Personal Health Information Protection Act, 2004* ("the *Act*") and the duties and responsibilities that arise as a result of this status.	• The *Privacy Policy* must describe the status of the person or organization as a prescribed person or prescribed entity under PHIPA and the duties and responsibilities that arise as a result of this status.
	• Must indicate that the prescribed person or prescribed entity has implemented policies, procedures and practices to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information and that these policies, procedures and practices are subject to review by the Information and Privacy Commissioner of Ontario every three years.	• The *Privacy Policy* must indicate that the prescribed person or prescribed entity has implemented policies, procedures and practices to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information and that these policies, procedures and practices are subject to review by the Information and Privacy Commissioner of Ontario every three years.
	• Must articulate a commitment by the prescribed person or prescribed entity to comply with the provisions of the *Act* and its regulation applicable to prescribed persons or prescribed entities, as the case may be.	• The *Privacy Policy* must articulate a commitment by the prescribed person or prescribed entity to comply with the provisions of PHIPA and its regulations applicable to prescribed persons or prescribed entities, as the case may be.
	<u>Privacy and Security Accountability Framework</u>	<u>Privacy and Information Security Accountability Framework</u>
	• Must articulate the accountability framework for ensuring compliance with the *Act* and its regulation and for ensuring compliance with the privacy and security policies, procedures and practices implemented by the prescribed person or prescribed entity.	• The *Privacy Policy* must 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 prescribed persons or prescribed entity.
	• Must indicate that the Chief Executive Officer or the Executive Director, as the case may be, is ultimately accountable for ensuring compliance with the *Act* and its regulation and for ensuring compliance with the privacy and security policies, procedures and practices implemented.	• 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: o PHIPA and its regulations; and o The privacy and information security policies, procedures and practices implemented.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must identify the position(s) that have been delegated day-to-day authority to manage the privacy program and the security program and to whom these positions report. It must further identify the duties and responsibilities of the position(s) that have been delegated day-to-day authority to manage the privacy program and the security program and some of the key activities of these programs.	• The *Privacy Policy* must identify the position(s) that have been delegated day-to-day authority to manage the privacy program and the information security program including: o To whom these positions report; o Their duties and responsibilities to manage the privacy program and the information security program; and o Some of the key activities in respect of these programs.
	• Should also identify other positions or committees that support the privacy program and/or the security program and their role in respect of these programs.	• The *Privacy Policy* should identify other positions or committees that support the privacy program and/or the information security program and their role in respect of these programs.
	<u>Collection of Personal Health Information</u>	<u>Collection of Personal Health Information</u>
	• Must identify the purposes for which personal health information is collected, the types of personal health information collected and the persons or organizations from which personal health information is typically collected.	• The *Privacy Policy* must identify the: o Purposes for which personal health information is collected; o Types of personal health information collected; and o Persons or organizations from which personal health information is typically collected.
	• In identifying the purposes for which personal health information is collected, the prescribed person or prescribed entity must ensure that each collection identified in the *Privacy Policy* is consistent with the collections of personal health information permitted by the *Act* and its regulation.	• The *Privacy Policy* must ensure that each purpose for which personal health information is collected, identified in the *Privacy Policy*, is consistent with the collections of personal health information permitted by PHIPA and its regulations.
	• Must articulate a commitment by the prescribed person or prescribed entity not to collect personal health information if other information will serve the purpose and not to collect more personal health information than is reasonably necessary to meet the purpose.	• The *Privacy Policy* must articulate a commitment by the prescribed person or prescribed entity not to collect personal health information if other information will serve the purpose and not to collect more personal health information than is reasonably necessary to meet the purpose.
	• Must outline the policies, procedures and practices implemented by the prescribed person or prescribed entity to ensure that both the amount and the type of personal health information collected is limited to that which is reasonably necessary for its purpose.	• The *Privacy Policy* must outline the policies, procedures and practices implemented by the prescribed person or prescribed entity to ensure that both the amount and the type of personal health information collected is limited to that which is reasonably necessary for its purpose.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must contain a list of the data holdings of personal health information maintained by the prescribed person or prescribed entity and must identify where an individual may obtain further information in relation to the purposes, data elements and data sources for each data holding of personal health information.	• The *Privacy Policy* must contain a list of the data holdings of personal health information maintained by the prescribed person or prescribed entity. • The *Privacy Policy* must identify where an individual may obtain further information in relation to the purposes, elements and sources of each data holding of personal health information.
	<u>Use of Personal Health Information</u>	<u>Use of Personal Health Information</u>
	• The purposes for which the prescribed person or prescribed entity uses personal health information must be identified.	• The *Privacy Policy* must identify the purposes for which the prescribed person or prescribed entity uses personal health information.
	• Must clearly distinguish between the use of personal health information and the use of de-identified and/or aggregate information and between the use of personal health information for purposes of subsection 39(1)(c) or section 45 of the *Act*, as the case may be, and the use of personal health information for research purposes.	• The *Privacy Policy* must clearly distinguish between the use of personal health information and the use of de-identified and/or aggregate information. • The *Privacy Policy* must distinguish between the use of personal health information for purposes of clause 39(1)I or subsection 45(1) of PHIPA, as the case may be, and the use of personal health information for research purposes.
	• Must ensure that each use of personal health information identified in the *Privacy Policy* is consistent with the uses of personal health information permitted by the *Act* and its regulation.	• The *Privacy Policy* must ensure that each use of personal health information identified in the *Privacy Policy* is consistent with the uses of personal health information permitted by PHIPA and its regulations.
	• Must articulate a commitment by the prescribed person or prescribed entity not to use personal health information if other information will serve the purpose and not to use more personal health information than is reasonably necessary to meet the purpose and must identify some of the policies, procedures and practices implemented by the prescribed person or prescribed entity in this regard, including limits on the use of personal health information by agents.	• The *Privacy Policy* must articulate a commitment by the prescribed person or prescribed entity not to use personal health information if other information will serve the purpose and not to use more personal health information than is reasonably necessary to meet the purpose; and • The *Privacy Policy* must identify some of the policies, procedures and practices implemented by the prescribed person or prescribed entity to fulfill these data minimization requirements, including limits on the use of personal health information by agents.
	• Should state that the prescribed person or prescribed entity remains responsible for personal health information used by its agents and should identify the policies, procedures and practices implemented to ensure that its agents only collect, use, disclose, retain and dispose of personal health information in compliance with the *Act* and its regulation and in compliance with the privacy and security policies, procedures and practices implemented.	• The *Privacy Policy* must state that the prescribed person or prescribed entity remains responsible for personal health information used by its agents and identify the policies, procedures and practices implemented to ensure that its agents only collect, use, disclose, retain and dispose of personal health information in compliance with PHIPA and its regulations and in compliance with the privacy and information security policies, procedures and practices.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	<u>Disclosure of Personal Health Information</u>	<u>Disclosure of Personal Health Information</u>
	• Must identify the purposes for which and the circumstances in which personal health information is disclosed, to whom such disclosures are typically made and the statutory or other requirements that must be satisfied prior to such disclosures.	• The *Privacy Policy* must identify the purposes for which and the circumstances in which personal health information is disclosed, to whom such disclosures are typically made and the statutory or other requirements that must be satisfied prior to such disclosures.
	• The prescribed person or prescribed entity must ensure that each disclosure identified in the *Privacy Policy* is consistent with the disclosures of personal health information permitted by the *Act* and its regulation.	• The *Privacy Policy* must ensure that each disclosure identified in the *Privacy Policy* is consistent with the disclosures of personal health information permitted by PHIPA and its regulations.
	• Must clearly distinguish between the purposes for which and the circumstances in which personal health information is disclosed and the circumstances in which and the purposes for which de-identified and/or aggregate information is disclosed.	• The *Privacy Policy* must clearly distinguish between the purposes for which and the circumstances in which personal health information is disclosed and those where de-identified and/or aggregate information is disclosed.
	• Must indicate that the prescribed person or prescribed entity will review all de-identified and/or aggregate information prior to its disclosure in order to ensure that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual.	• The *Privacy Policy* must indicate that the prescribed persons or prescribed entities will review all de-identified and/or aggregate information prior to its disclosure to ensure that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual.
	• Must articulate a commitment by the prescribed person or prescribed entity not to disclose personal health information if other information will serve the purpose and not to disclose more personal health information than is reasonably necessary to meet the purpose and must identify some of the policies, procedures and practices implemented by the prescribed person or prescribed entity in this regard.	• The *Privacy Policy* must articulate a commitment by the prescribed person or prescribed entity not to disclose personal health information if other information will serve the purpose and not to disclose more personal health information than is reasonably necessary to meet the purpose; and • The *Privacy Policy* must identify some of the policies, procedures and practices implemented by the prescribed person or prescribed entity to fulfill these data minimization requirements.
	<u>Secure Retention, Transfer and Disposal of Records of Personal Health Information</u>	<u>Secure Retention, Transfer and Disposal of Records of Personal Health Information</u>
	• Must address the secure retention of records of personal health information in both paper and electronic format, including how long records of personal health information are retained, whether the records are retained in identifiable form and the secure manner in which they are retained.	• The *Privacy Policy* must address the secure retention of records of personal health information in both paper and electronic format, including: o How long records of personal health information are retained; o Whether the records are retained in identifiable form; and o The secure manner in which they are retained.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must address the manner in which records of personal health information in both electronic and paper format will be securely transferred and disposed of.	• The *Privacy Policy* must address the manner in which records of personal health information in both paper and electronic format will be securely transferred and disposed of.
	<u>Implementation of Administrative, Technical and Physical Safeguards</u>	<u>Implementation of Administrative, Technical and Physical Safeguards</u>
	• Must outline some of the administrative, technical and physical safeguards implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, including the steps taken to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.	• The *Privacy Policy* must outline some of the administrative, technical and physical safeguards implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, including the steps taken to protect personal health information against theft, loss and unauthorized collection, use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.
	<u>Inquiries, Concerns or Complaints Related to Information Practices</u>	<u>Inquiries, Concerns or Complaints Related to Information Practices</u>
	• Must identify the agent(s) to whom and the manner in which individuals may direct inquiries, concerns or complaints related to the privacy policies, procedures and practices of the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with the *Act* and its regulation.	• The *Privacy Policy* must identify to whom, and how, individuals may direct inquiries, concerns or complaints related to the privacy policies, procedures and practices of the prescribed person or prescribed entity, or related to the compliance of the prescribed person or prescribed entity with PHIPA and its regulations.
	• Must include the name and/or title, mailing address and contact information for the agent(s) to whom inquiries, concerns or complaints may be directed and the manner and format in which these inquiries, concerns or complaints may be made.	• The *Privacy Policy* must include the name and/or title, mailing address and contact information for the agent(s) to whom inquiries, concerns or complaints may be directed. • The *Privacy Policy* must describe the manner and format in which these inquiries, concerns or complaints may be made.
	• Should state that individuals may direct complaints regarding the compliance of the prescribed person or prescribed entity with the *Act* and its regulation to the Information and Privacy Commissioner of Ontario and provide the mailing address and contact information for the Information and Privacy Commissioner of Ontario.	• The *Privacy Policy* must clarify that individuals may direct complaints regarding the compliance of the prescribed person or prescribed entity with PHIPA and its regulations to the Information and Privacy Commissioner of Ontario and provide the mailing address and contact information for the Information and Privacy Commissioner of Ontario.
	<u>Transparency of Practices in Respect of Personal Health Information</u>	
	• Must identify where individuals may obtain further information in relation to the privacy policies, procedures and practices of the prescribed person or prescribed entity.	• The *Privacy Policy* must identify where individuals may obtain further information in relation to the privacy policies, procedures and practices of the prescribed person or prescribed entity.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Compliance, Audit and Enforcement
		The *Privacy Policy* must: • Require agents to comply with the policy, procedures and practices; • Require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices; • Identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; • Address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and • Stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits*.
Policy 2. **2011 Manual: Policy and Procedures for Ongoing Review of Privacy Policies Procedures and Practices** **2024 Manual: Policy, Procedures and Practices for Ongoing Review of Privacy Policies, Procedures and Practices**	Policy Requirements:	
	• A policy and associated procedures must be developed and implemented for the ongoing review of the privacy policies, procedures and practices put in place by the prescribed person or prescribed entity.	• A policy, procedures and practices must be developed and implemented for the ongoing review of the prescribed person's or prescribed entity's privacy policies, procedures and practices ("*policy, procedures and Practices for ongoing review*"). The purpose of this ongoing review is to determine on a regular basis whether amendments are needed or whether new privacy policies, procedures and practices are required.
	• Must identify the frequency of the review, the agent(s) responsible for undertaking the review, the procedure to be followed in undertaking the review and the time frame in which the review will be undertaken. At a minimum, the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity must be reviewed on an annual basis.	• The policy, procedures and practices for ongoing review must identify the: o frequency of the review of the privacy policies, procedures and practices, which at minimum must be reviewed at least once prior to each three-year review by the Information and Privacy Commissioner of Ontario; o agent(s) responsible and the procedure for undertaking the review; and o timeframe in which the review will be undertaken.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must identify the agent(s) responsible and the procedure to be followed in amending and/or drafting new privacy policies, procedures and practices if deemed necessary as a result of the review, and the agent(s) responsible and the procedure that must be followed in obtaining approval of any amended or newly developed privacy policies, procedures and practices.	• The policy, procedures and practices for ongoing review must identify the agent(s) responsible and the procedure for amending and/or drafting new privacy policies, procedures and practices. • The policy, procedures and practices for ongoing review must identify the agent(s) responsible, and the procedure, for seeking and providing approval of any amendments or newly-developed privacy policies, procedures and practices, if deemed necessary as a result of the review.
	• Must identify the agent(s) responsible and the procedure to be followed in communicating the amended or newly developed privacy policies, procedures and practices, including the method and nature of the communication. • Must identify the agent(s) responsible for and the procedure to be followed in reviewing and amending the communication materials available to the public and other stakeholders as a result of the amended or newly developed privacy policies, procedures and practices.	• The policy, procedures and practices for ongoing review must identify the agent(s) responsible and the procedure for communicating the amended or newly developed privacy policies, procedures and practices. • The policy, procedures and practices for ongoing review must identify the method and nature of the communication to agents, the public, and other stakeholders, as may be relevant, depending on the nature of the subject matter.
	• Must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. • Must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audit*s, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	• The policy, procedures and practices must: o Require agents to comply with the policy, procedures and practices; o Require agents to notify the prescribed or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices; o Identify the agent(s) responsible for ensuring compliance with the policy, procedures, and practices; o Address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and o Stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices in Respect of Privacy Audits.*

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• The privacy policies, procedures and practices implemented by the prescribed person or prescribed entity must be reviewed on an annual basis.	
	• In undertaking the review and determining whether amendments and/or new privacy policies, procedures and practices are necessary, the prescribed person or prescribed entity must have regard to any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation; evolving industry privacy standards and best practices; amendments to the *Act* and its regulation relevant to the prescribed person or prescribed entity; and recommendations arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and information security breaches.	• In undertaking the ongoing review and determining whether amendments and/or new privacy policies, procedures and practices are necessary, the prescribed person or prescribed entity must have regard to: o Any relevant orders, decisions, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario and the courts under PHIPA and its regulations; o Evolving industry privacy standards and best practices; Amendments to PHIPA and its regulations relevant to the prescribed person or prescribed entity; Findings, mitigations and other relevant recommendations arising from privacy and information security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and/or information security breaches; and o Findings and associated recommendations arising from prior three-year reviews.
	• Must take into account whether the privacy policies, procedures and practices of the prescribed person or prescribed entity continue to be consistent with its actual practices and whether there is consistency between and among the privacy and security policies, procedures and practices implemented.	• The prescribed person or prescribed entity must have regard to whether the privacy policies, procedures and practices of the prescribed person or prescribed entity continue to be consistent with its actual practices. • The prescribed person or prescribed entity must have regard to whether there is consistency between and among the privacy and information security policies, procedures and practices implemented.
	• This policy and its associated procedures may either be a stand-alone document or may be combined with the *Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices*.	• This policy, procedures and practices may either be a stand-alone document or may be combined with the *Policy, Procedures and Practices for Ongoing Review of Information Security Policies, Procedures and Practices*.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Transparency
Policy 3. **Policy on the Transparency of Privacy Policies, Procedures and Practices**	• Must identify the information made available to the public and other stakeholders relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and that identifies the means by which such information is made available.	• A policy must be developed and implemented that identifies the information made available to the public and other stakeholders relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity ("transparency policy") and that identifies the means by which such information is made available.
	• At a minimum, the policy must require the prescribed person or prescribed entity to make the following information available: 1. Its *Privacy Policy*; 2. Brochures or frequently asked questions related to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity; 3. Documentation related to the review by the Information and Privacy Commissioner of Ontario of the policies, procedures and practices implemented by the prescribed person or prescribed entity to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information; 4. A list of the data holdings of personal health information maintained by the prescribed person or prescribed entity; and 5. The name and/or title, mailing address and contact information of the agent(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the *Act* and its regulation may be directed.	• At a minimum, the transparency policy must require the prescribed person or prescribed entity to make the following information publicly available: o Its *Privacy Policy*; o Brochures, frequently asked questions and/or other plain language tools related to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity; o A list of the data holdings of personal health information maintained by the prescribed person or prescribed entity; and o The name and/or title, mailing address and contact information of the agent(s) to whom inquiries, concerns or complaints may be directed regarding the prescribed person or prescribed entity's compliance with its privacy policies, procedures and practices and with PHIPA and its regulations.
	• It is recommended that privacy impact assessments or a summary of the privacy impact assessments conducted also be made available.	• Privacy impact assessments or summaries of the privacy impact assessments conducted should also be made available.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Brochures, Frequently Asked Questions, and Other Plain Language Tools

	• Must set out the minimum content of the brochures or frequently asked questions described above.
	• The brochures or frequently asked questions must describe the status of the prescribed person or prescribed entity under the *Act*, the duties and responsibilities arising from this status and the privacy policies, procedures and practices implemented in respect of personal health information, including:
	  ○ The types of personal health information collected and the persons or organizations from which this personal health information is typically collected;
	  ○ The purposes for which personal health information is collected;
	  ○ The purposes for which personal health information is used, and if identifiable information is not routinely used, the nature of the information that is used; and
	  ○ The circumstances in which and the purposes for which personal health information is disclosed and the persons or organizations to which it is typically disclosed.
		• The transparency policy must set out the minimum content of the brochures, frequently asked questions and/or other plain language tools and in particular such content must:
		  ○ Must describe the status of the prescribed person or prescribed entity under PHIPA, the duties and responsibilities arising from this status and the privacy policies, procedures and practices implemented in respect of personal health information, including the:
		  ▪ Types of personal health information collected and the persons or organizations from which this personal health information is typically collected;
		  ▪ The purposes for which personal health information is collected;
		  ▪ Purposes for which personal health information is used, and if identifiable information is not routinely used, the nature of the information that is used; and
		  ▪ Circumstances in which and the purposes for which personal health information is disclosed and the persons or organizations to which it is typically disclosed.

	• The brochures or frequently asked questions must also identify some of the administrative, technical and physical safeguards implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, including the steps taken to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.	• The content must identify some of the administrative, technical and physical safeguards implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, including the steps taken to protect personal health information against theft, loss and unauthorized collection, use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.
	• It is recommended that the brochures or frequently asked questions provide the name and/or title, mailing address and contact information of the agent(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the *Act* and its regulation may be directed.	• The content must provide the name and/or title, mailing address and contact information of the agent(s) to whom inquiries, concerns or complaints may be directed regarding the prescribed person's or prescribed entity's compliance with the privacy policies, procedures and practices.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		<u>Statement on Public Website</u>

		• The prescribed person or prescribed entity must have a statement on its website informing the public of the Information and Privacy Commissioner of Ontario's:
		  ○ Role in reviewing and approving the prescribed person or prescribed entity's policies, procedures and practices; and
		  ○ Website where documentation in respect of these reviews and approvals can be found, and provide a link to the website.

		<u>Compliance, Audit and Enforcement</u>
		The policy, procedures and practices must: • Require agents to comply with the policy, procedures and practices; • Require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices; • Identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; • Address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and • Stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits*.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Collection of Personal Health Information and Data Holdings
Policy 4. **2011 Manual: Policy and Procedures for the Collection of Personal Health Information** **2024 Manual: Policy, Procedures and Practices for the Collection of Personal Health Information**	• Must identify the purposes for which personal health information will be collected by the prescribed entity or prescribed person, the nature of the personal health information that will be collected, from whom the personal health information will typically be collected and the secure manner in which personal health information will be collected.	• A policy, procedures and practices must be developed and implemented to identify: o The purposes for which personal health information will be collected by the prescribed person or prescribed entity; o The nature of the personal health information that will be collected; o From whom the personal health information will typically be collected; and o The secure manner in which personal health information will be collected.
	• Must articulate a commitment by the prescribed person or prescribed entity not to collect personal health information unless the collection is permitted by the *Act* and its regulation, not to collect personal health information if other information will serve the purpose and not to collect more personal health information than is reasonably necessary to meet the purpose.	• The policy, procedures and practices must articulate a commitment by the prescribed person or prescribed entity not to collect: o personal health information unless the collection is permitted by PHIPA and its regulations; o personal health information if other information will serve the purpose; and o Any more personal health information than is reasonably necessary to meet the purpose.
	Review and Approval Process	Review and Approval Process for the Collection of Personal Health Information
	• Must identify the agent(s) responsible for reviewing and determining whether to approve the collection of personal health information and the process that must be followed and the requirements that must be satisfied in this regard.	• The policy, procedures and practices must identify: o The agent(s) responsible for reviewing and determining whether to approve the collection of personal health information; o The process that must be followed; o The requirements that must be satisfied; and o The criteria that must be considered.
	• Must set out the criteria that must be considered by the agent(s) responsible for determining whether to approve the collection of personal health information. The criteria must: o Require the agent(s) responsible for determining whether to approve the collection of personal health information to ensure that the collection is permitted by the *Act* and its regulation and that any and all conditions or restrictions set out in the *Act* and its regulation have been satisfied.	• At minimum, the above criteria must require the responsible agent(s) to ensure that: o The collection is permitted by PHIPA and its regulations and that any and all conditions or restrictions set out in PHIPA and its regulations have been satisfied; and o Other information, namely de-identified and/or aggregate information, will not serve the identified purpose and that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	○ Require the agent(s) responsible for determining whether to approve the collection of personal health information to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose and that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.	
	• Should set out the manner in which the decision approving or denying the collection of personal health information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	• The policy, procedures and practices must also set out: ○ The manner of documenting the decision approving or denying the collection of personal health information; ○ The reasons for the decision; ○ The method and format in which the decision will be communicated; and ○ To whom the decision will be communicated.
	<u>Conditions or Restrictions on the Approval</u>	<u>Conditions or Restrictions on the Approval to Collect Personal Health Information</u>
	• Must identify the conditions or restrictions that are required to be satisfied prior to the collection of personal health information, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements. The conditions or restrictions identified in the policy and procedures, including the documentation and/or agreements that must be completed, provided or executed, shall have regard to the requirements of the *Act* and its regulation. • Must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the collection of personal health information have in fact been satisfied.	• The policy, procedures and practices must identify the conditions or restrictions that are required to be satisfied prior to the collection of personal health information, having regard to the requirements of PHIPA and its regulations. Such policy, procedures and practices must include: ○ Any documentation and/or agreements that must be completed, provided or executed; ○ The agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements; and ○ The agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the collection of personal health information have, in fact, been satisfied.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Secure Retention	Secure Retention, Transfer, Return or Disposal of Personal Health Information
	• Must require that the records of personal health information collected by the prescribed person or prescribed entity be retained in a secure manner in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information*.	• The policy, procedures and practices must require: o That records of personal health information collected by the prescribed person or prescribed entity be retained in a secure manner in compliance with the *Policy, Procedures and Practices for Secure Retention of Records of Personal Health Information*; o That records of personal health information collected by an agent of the prescribed person or prescribed entity, such as a chart abstractor, be transferred in a secure manner in compliance with the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information*; and o Identification of the agent(s) responsible for ensuring that the records of personal health information that have been collected are either securely returned or securely disposed of, as the case may be, following the retention period or the date of termination set out in any documentation and/or agreements executed prior to the collection of the personal health information.
	Secure Transfer	
	• If the personal health information is being collected by an agent of the prescribed person or prescribed entity, such as a chart abstractor, the policy and procedures shall require the records of personal health information to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information.*	
	Secure Return or Disposal	
	• Must identify the agent(s) responsible for ensuring that the records of personal health information that have been collected are either securely returned or securely disposed of, as the case may be, following the retention period or the date of termination set out in any documentation and/or agreements executed prior to the collection of the personal health information.	
	• If the records of personal health information are to be returned to the person or organization from which they were collected, the policy and procedures must require the records to be transferred in a secure manner and in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*. If the records are to be disposed of, the policy and procedures must require the records to be disposed of in a secure manner and in compliance with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information*.	• If the records of personal health information are required to be securely returned to the person or organization from which they were collected, the policy, procedures and practices must require the records to be transferred in a secure manner and in compliance with the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information*. If the records are to be disposed of, the policy, procedures and practices must require the records to be disposed of in a secure manner and in compliance with the *Policy, Procedures and Practices for Secure Disposal of Records of Personal Health Information*.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Compliance, Audit and Enforcement
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. • Must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits.* • Must set out the frequency with which the policy and procedures will be audited. • Must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures. • Must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.	The policy, procedures and practices must: ○ Require agents to comply with the policy, procedures and practices; ○ Require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices; ○ Identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; ○ Address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and ○ Stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits*.
Policy 5. **List of Data Holdings Containing Personal Health Information**	• The prescribed person or prescribed entity shall develop and retain an up-to-date list and brief description of the data holdings of personal health information maintained by the prescribed person or prescribed entity.	• The prescribed person or prescribed entity must develop and retain an up-to-date list and brief description of the data holdings of personal health information maintained by the prescribed person or prescribed entity.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
Policy 6. **2011 Manual: Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information** **2024 Manual: Policy, Procedures and Practices for Maintaining statements of Purpose for Data Holdings Containing Personal Health Information**	• A policy and procedures must be developed and implemented with respect to the creation, review, amendment and approval of statements of purpose for data holdings containing personal health information.	• A policy, procedures and practices must be developed and implemented with respect to the creation, review, amendment and approval of statements of purpose for data holdings containing personal health information.
	• Shall require the statements of purpose to set out the purpose of the data holding, the personal health information contained in the data holding, the personal health information contained in the data holding, the source(s) of the personal health information and the need for the personal health information in relation to the identified purpose.	• The policy, procedures and practices must require that the statements of purpose: o Set out the purpose of the data holding; o Describe the personal health information contained in the data holding; o Identify the source(s) of the personal health information; o Explain the need for the personal health information in relation to the identified purpose; and o Explain why de-identified and/or aggregate information will not serve the identified purpose.
	• Must identify the agent(s) responsible and the process that must be followed in completing the statements of purpose for the data holdings containing personal health information, including the agent(s) or other persons or organizations that must be consulted in completing the statements of purpose and the agent(s) responsible for approving the statements of purpose. The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program in respect of the statements of purpose shall also be specified.	• The policy, procedures and practices must specify the agent(s) responsible and the process that must be followed in completing the statements of purpose for the data holdings containing personal health information, including the agent(s) or other persons or organizations that must be consulted in the process. • The policy, procedures and practices must specify the agent(s) responsible for approving the statements of purpose. • The policy, procedures and practices must specify the role of the agent(s) that have been delegated day-to-day authority to manage the privacy program in respect of the statements of purpose.
	• Must identify the persons and organizations that will be provided the statements of purpose. At a minimum, this should include the health information custodians or other persons or organizations from whom the personal health information in the data holding is collected.	• The policy, procedures and practices must specify the person(s) and organization(s) that will be provided the statements of purpose, including, at a minimum, the custodian(s) or other person(s) or organization(s) from whom the personal health information in the data holding is collected.
	• Must require that the statements of purpose be reviewed on an ongoing basis in order to ensure their continued accuracy and in order to ensure that the personal health information collected for purposes of the data holding is still necessary for the identified purposes.	• The policy, procedures and practices must be reviewed on an ongoing basis to ensure their continued accuracy, that the personal health information collected for purposes of the data holding is still necessary for the identified purpose(s), and that de-identified and/or aggregate information will not serve the identified purpose.
	• Must identify the frequency with which and the circumstances in which the statements of purpose are required to be reviewed.	• The policy, procedures and practices must specify the frequency with which and the circumstances in which the statements of purpose must be reviewed.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must document the agent(s) responsible and the process that must be followed in reviewing the statements of purpose and in amending the statements of purpose, if necessary. This shall include the agent(s) or other persons or organizations that must be consulted in reviewing, and if necessary, amending the statements of purpose and the agent(s) responsible for approving the amended statements of purpose.	• The policy, procedures and practices must specify the agent(s) responsible and the process that must be followed in reviewing the statements of purpose and amending them, as necessary. • The policy, procedures and practices must specify the agent(s) or other person(s) or organization(s) that must be consulted in reviewing, and if necessary, amending the statements of purpose. • The policy, procedures and practices must specify the agent(s) responsible for approving the amended statements of purpose.
	• Must identify the persons and organizations that will be provided amended statements of purpose upon approval, including health information custodians or other persons or organizations from whom the personal health information in the data holding is collected.	• The policy, procedures and practices must specify the person(s) and organization(s) that will be provided amended statements of purpose upon approval, including custodians or other persons or organizations from whom the personal health information in the data holding is collected.
		<u>Compliance, Audit and Enforcement</u>
	• The prescribed person or prescribed entity shall require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	• The policy, procedures and practices must require agents to comply with the policy, procedures and practices. • The policy, procedures and practices must address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*.
	• Must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	• The policy, procedures and practices must stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audit*s. • The policy, procedures and practices must identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices.
	• Must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.	• The policy, procedures and practices must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
Policy 7. **Statements of Purpose for Data Holdings Containing Personal Health Information**	• For each data holding containing personal health information, the prescribed person or prescribed entity must draft a statement identifying the purpose of the data holding, the personal health information contained in the data holding, the source(s) of the personal health information and the need for the personal health information in relation to the identified purpose.	• For each data holding containing personal health information, the prescribed person or prescribed entity must complete a statement identifying the purpose of the data holding, the personal health information contained in the data holding, the source(s) of the personal health information, the need for the personal health information in relation to the identified purpose, and why de-identified and/or aggregate information will not serve the identified purpose.
Access and Use of Personal Health Information		
Policy 8. **2011 Manual: Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information** **2024 Manual: Policy, Procedures and Practices for Limiting Agent Access to and Use of Personal Health Information**	• Must be developed and implemented to limit access to and use of personal health information by agents based on the "need to know" principle. The purpose of this policy and its procedures is to ensure that agents of the prescribed person or prescribed entity access and use both the least identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual or other responsibilities.	• A policy, procedures and practices must be developed and implemented to limit access to and use of personal health information by agents based on the "need to know" principle. The purpose of this policy, procedures and practices is to ensure that agents of the prescribed person or prescribed entity access and use the least identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual or other responsibilities.
	• Must identify the limited and narrowly defined purposes for which and circumstances in which agents are permitted to access and use personal health information and the levels of access to personal health information that may be granted.	• The policy, procedures and practices must identify the limited and narrowly defined purposes for which and circumstances in which agents are permitted to access and use personal health information and the levels of access to personal health information that may be granted.
	• The prescribed person or prescribed entity must ensure that the duties of agents with access to personal health information are segregated in order to avoid a concentration of privileges that would enable a single agent to compromise personal health information.	• The policy, procedures and practices must ensure that the duties of agents with access to personal health information are segregated in order to avoid a concentration of privileges that would enable a single agent to compromise personal health information.
	• For all other purposes and in all other circumstances, the policy and procedures must require agents to access and use de-identified and/or aggregate information, as defined in the *Policy and Procedures with Respect to De-Identification and Aggregation*.	• For all other purposes and in all other circumstances, the policy, procedures and practices must require agents to access and use de-identified and/or aggregate information, as defined in the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation*.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must explicitly prohibit access to and use of personal health information if other information, such as de-identified and/or aggregate information, will serve the identified purpose and must prohibit access to or use of more personal health information than is reasonably necessary to meet the identified purpose.	• The policy, procedures and practices must explicitly prohibit access to and use of personal health information if other information, such as de-identified and/or aggregate information, will serve the identified purpose and must prohibit access to or use of more personal health information than is reasonably necessary to meet the identified purpose.
	• Must prohibit agents from using de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.	• The policy, procedures and practices must also prohibit agents from using de-identified and/or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is done in accordance with the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation* and is permitted by PHIPA or another 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.
	<u>Review and Approval Process</u>	<u>Review and Approval Process for Allowing Access and Use by Agents</u>
	• Shall set out the agent(s) responsible and the process to be followed in receiving, reviewing and determining whether to approve or deny a request by an agent for access to and use of personal health information, along with the various level(s) of access that may be granted by the prescribed person or prescribed entity.	• The policy, procedures and practices must identify the agent(s) responsible and the process to be followed in receiving, reviewing and determining whether to approve or deny a request by an agent for access to and use of personal health information, along with the various level(s) of access that may be granted by the prescribed person or prescribed entity.
	• Must set out the requirements to be satisfied in requesting, reviewing and determining whether to approve or deny a request by an agent for access to and use of personal health information; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must set out the: o Requirements to be satisfied in requesting, reviewing and determining whether to approve or deny a request by an agent for access to and use of personal health information; o The policy, procedures and practices must set out the documentation that must be completed, provided and/or executed upon rendering the decision; o The policy, procedures and practices must set out the agent(s) responsible for completing, providing and/or executing the documentation; o The policy, procedures and practices must set out the agent(s) to whom the documentation must be provided; and o The policy, procedures and practices must set out the required content of the documentation.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must set out the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request for access to and use of personal health information and, if the request is approved, the criteria that must be considered in determining the appropriate level of access.	• The policy, procedures and practices must set out the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request for access to and use of personal health information and the criteria for determining the appropriate level of access.
	• At a minimum, the agent(s) responsible for determining whether to approve or deny the request must be satisfied that:	• At a minimum, the agent(s) responsible for determining whether to approve or deny a request for access to and use of personal health information must be satisfied that:
	• The agent making the request routinely requires access to and use of personal health information on an ongoing basis or for a specified period for his or her employment, contractual or other responsibilities;	• The agent making the request routinely requires access to and use of personal health information on an ongoing basis or for a specified period for his or her employment, contractual or other responsibilities;
	• The identified purpose for which access to and use of personal health information is requested is permitted by the *Act* and its regulation;	• The identified purpose for which access to and use of personal health information is being requested is permitted by PHIPA and its regulations;
	• The identified purpose for which access to and use of personal health information is requested cannot reasonably be accomplished without personal health information;	• The identified purpose for which access to and use of personal health information is being requested cannot reasonably be accomplished without personal health information;
	• De-identified and/or aggregate information will not serve the identified purpose; and	• De-identified and/or aggregate information will not serve the identified purpose; and
	• In approving the request, no more personal health information will be accessed and used than is reasonably necessary to meet the identified purpose.	• No more personal health information will be accessed and used than is reasonably necessary to meet the identified purpose.
	• Should set out the manner in which the decision approving or denying the request for access to and use of personal health information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; to whom the decision will be communicated; any documentation that must be completed, provided and/or executed upon rendering the decision; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.	• The policy, procedures and practices must set out the manner of documenting the decision approving or denying the request for access to and use of personal health information and the reasons for the decision; • The policy, procedures and practices must set out the method and format in which the decision will be communicated and to whom; and • The policy, procedures and practices must set out the documentation that must be completed, provided and/or executed upon rendering the decision.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Conditions or Restrictions on the Approval	Conditions or Restrictions on the Approval
	• Must identify the conditions or restrictions imposed on an agent granted approval to access and use personal health information, such as read, create, update or delete limitations, and the circumstances in which the conditions or restrictions will be imposed.	• The policy, procedures and practices must identify the conditions or restrictions imposed on an agent granted approval to access and use personal health information, such as read only, create, edit, update or delete limitations, and the circumstances in which the conditions or restrictions will be imposed.
	• In the event that an agent only requires access to and use of personal health information for a specified period, the policy and procedures must set out the process to be followed in ensuring that access to and use of the personal health information is permitted only for that specified time period.	• In the event that an agent only requires access to and use of personal health information for a specified period, the policy, procedures and practices must set out the process to be followed in ensuring that access to and use of the personal health information is permitted only for that specified time period.
	• Recommended that all approved accesses and uses of personal health information be subject to an automatic expiry, following which an agent is again required to request approval to access and use personal health information in accordance with the policy and its procedures. At a minimum, it is recommended that the expiry date be one year from the date approval is granted.	• All approved accesses and uses of personal health information should be subject to an automatic expiry, following which an agent is again required to request approval to access and use personal health information in accordance with the policy, procedures and practices. At a minimum, the expiry date should be one year from the date approval is granted and agents should seek re-approval on an annual basis.
	• Must prohibit an agent granted approval to access and use personal health information from accessing and using personal health information except as necessary for his or her employment, contractual or other responsibilities; from accessing and using personal health information if other information will serve the identified purpose; and from accessing and using more personal health information than is reasonably necessary to meet the identified purpose.	• The policy, procedures and practices must also prohibit an agent from accessing and using personal health information except as necessary for his or her employment, contractual or other responsibilities; from accessing and using personal health information if other information will serve the identified purpose; and from accessing and using more personal health information than is reasonably necessary to meet the identified purpose.
	• The prescribed person or prescribed entity also ensure that all accesses to and uses of personal health information are permitted by the *Act* and its regulation.	• The prescribed person or prescribed entity must also ensure that all accesses to and uses of personal health information are permitted by PHIPA and its regulations.
	• Must impose conditions or restrictions on the purposes for which and the circumstances in which an agent granted approval to access and use personal health information is permitted to disclose that personal health information. The prescribed person or prescribed entity must ensure that any such disclosures are permitted by the *Act* and its regulation.	• The policy, procedures and practices must impose conditions or restrictions on the purposes for which and the circumstances in which an agent granted approval to access and use personal health information is permitted to disclose that personal health information. The prescribed person or prescribed entity must ensure that any such disclosures are permitted by PHIPA and its regulations.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Notification and Termination of Access and Use	Notification and Termination of Access and Use by Agents
	• Must require an agent granted approval to access and use personal health information, as well as his or her supervisor, to notify the prescribed person or prescribed entity when the agent is no longer employed or retained by the prescribed person or prescribed entity or no longer requires access to or use of the personal health information.	• The policy, procedures and practices must require an agent granted approval to access and use personal health information, or his or her supervisor, to notify the prescribed person or prescribed entity when the agent is no longer employed or retained by the prescribed person or prescribed entity or no longer requires such access.
	• Must identify the procedure to be followed in providing the notification. In particular, the policy and procedures must identify the agent(s) to whom this notification must be provided; the time frame within which this notification must be provided; the format of the notification; the documentation that must be completed, provided and/or executed, if any; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must set out the procedure to be followed in providing the notification; • The policy, procedures and practices must identify the agent(s) to whom this notification must be provided; • The policy, procedures and practices must stipulate the timeframe within which this notification must be provided; • The policy, procedures and practices must specify the nature and format of the notification; • The policy, procedures and practices must set out the documentation that must be completed, provided and/or executed, if any; • The policy, procedures and practices must identify the agent(s) responsible for completing, providing and/or executing the documentation; • Identify the agent(s) to whom the documentation must be provided; and • The policy, procedures and practices must set out the required content of the documentation.
	• Must identify the agent(s) responsible for terminating access to and use of the personal health information, the procedure to be followed in terminating access to and use of the personal health information and the time frame within which access to and use of the personal health information must be terminated.	• The policy, procedures and practices must identify the agent(s) responsible for terminating access to and use of the personal health information; • The policy, procedures and practices must set out the procedure to be followed in terminating access to and use of the personal health information; and • The policy, procedures and practices must specify the method by which access will be terminated and the timeframe within which access to and use of the personal health information must be terminated.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• The prescribed person or prescribed entity must ensure that the procedures implemented in this regard are consistent with the *Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship*.	• The prescribed person or prescribed entity must ensure that the procedures implemented in this regard are consistent with the *Policy, Procedures and Practices upon Termination or Cessation of the Employment or Contractual Relationship*.
	Secure Retention	Secure Retention and Disposal
	• Must require an agent granted approval to access and use personal health information to securely retain the records of personal health information in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information*.	• The policy, procedures and practices must require an agent granted approval to access and use personal health information to securely retain the records of personal health information 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 personal health information in compliance with the *Policy, Procedures and Practices for Secure Disposal of Records of Personal Health Information*.
	Secure Disposal	
	• Must require an agent granted approval to access and use personal health information to securely dispose of the records of personal health information in compliance with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information*.	
	Tracking Approved Access to and Use of Personal Health Information	Tracking Approved Access to and Use of Personal Health Information
	• Must require that a log be maintained of agents granted approval to access and use personal health information and must identify the agent(s) responsible for maintaining such a log.	• The policy, procedures and practices must require the prescribed person or prescribed entity to maintain information with regard to the agent(s) granted approval to access and use personal health information in such a manner that the prescribed person or prescribed entity can promptly generate a log from the information. • The policy, procedures and practices must identify the agent(s) responsible for maintaining the information.
	• Recommended that the policy and procedures address where documentation related to the receipt, review, approval, denial or termination of access to and use of personal health information is to be retained and the agent(s) responsible for retaining this documentation.	• The policy, procedures and practices must address where documentation related to the receipt, review, approval, denial or termination of access to and use of personal health information is to be retained and the agent(s) responsible for retaining this documentation.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Compliance, Audit and Enforcement	Compliance, Audit and Enforcement
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	• The policy, procedures and practices must require agents to comply with the policy, procedures and practices. • The policy, procedures and practices must address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*.
	• In the event that there is no automatic expiry date on the approval to access and use personal health information, regular audits of agents granted approval to access and use personal health information must be conducted in accordance with the *Policy and Procedures In Respect of Privacy Audits.* The purpose of the audit is to ensure that agents granted such approval continue to be employed or retained by the prescribed person or prescribed entity and continue to require access to the same amount and type of personal health information. In this regard, the policy and procedures must identify the agent(s) responsible for conducting the audits and for ensuring compliance with the policy and its procedures and the frequency with which the audits must be conducted. At a minimum, audits must be conducted on an annual basis.	• The policy, procedures and practices must identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices. • The policy, procedures and practices must stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits*.
	• Must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.	• The policy, procedures and practices must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
Policy 9. **Log of Agents Granted Approval to Access and Use Personal Health Information**	• A prescribed person or prescribed entity must maintain a log of agents granted approval to access and use personal health information.	• A prescribed person or prescribed entity must maintain information with regard to agents granted approval to access and use personal health information.
	• The log must include the name of the agent granted approval to access and use personal health information; the data holdings of personal health information to which the agent has been granted approval to access and use; the level or type of access and use granted; the date that access and use was granted; and the termination date or the date of the next audit of access to and use of the personal health information.	• The information must be maintained in such a manner that the prescribed person or prescribed entity can promptly generate a log from the information. At a minimum, the information, and any subsequent log generated from the information, must include the: o Name of the agent granted approval to access and use personal health information; o Data holdings of personal health information to which the agent has been granted approval to access and use; o Level or type of access and use granted; o Date that access and use was granted; and o Termination date or the date of the next audit of access to and use of the personal health information.
Policy 10. **2011 Manual: Policy and Procedures for the Use of Personal Health Information for Research** **2024 Manual: Policy, Procedures and Practices for the Use of Personal Health Information for Research**	• A policy and procedures must be developed and implemented to identify whether and in what circumstances, if any, the prescribed person or prescribed entity permits personal health information to be used for research purposes.	• A policy, procedures and practices must be developed and implemented to identify whether and in what circumstances, if any, the prescribed person or prescribed entity permits personal health information to be used for research purposes. • If the prescribed person or prescribed entity does not permit personal health information to be used for research purposes, the policy, procedures and practices must explicitly prohibit the use of personal health information for research purposes. • If the prescribed person or prescribed entity does not permit de-identified and/or aggregate Information to be used for research purposes, the policy, procedures and practices must explicitly prohibit such use as well.
	• Must articulate a commitment by the prescribed person or prescribed entity not to use personal health information for research purposes if other information will serve the research purpose and not to use more personal health information than is reasonably necessary to meet the research purpose.	• Where the prescribed person or prescribed entity permits personal health information to be used for research purposes, the policy, procedures and practices must articulate a commitment by the prescribed person or prescribed entity not to use personal health information for research purposes if other information will serve the research purpose and not to use more personal health information than is reasonably necessary to meet the research purpose.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Where the Use of Personal Health Information is Permitted for Research	Where the Use of Personal Health Information is Permitted for Research
	• If the prescribed person or prescribed entity permits personal health information to be used for research purposes, the policy and procedures must set out the circumstances in which personal health information is permitted to be used for research purposes.	• The policy, procedures and practices must further set out the circumstances in which personal health information is permitted to be used for research purposes.
	Distinction between the Use of Personal Health Information for Research and Other Purposes	Distinction Between the Use of Personal Health Information for Research and Other Purposes
	• Must clearly distinguish between the use of personal health information for research purposes and the use of personal health information for purposes of subsection 39(1)(c) or section 45 of the Act, as the case may be. The criteria that must be considered in determining when a use of personal health information is for research purposes and when a use is for purposes of subsection 39(1)(c) or section 45 of the Act, as well as the agent(s) responsible and the procedure to be followed in making this determination, must also be addressed.	• The policy, procedures and practices must clearly distinguish between the use of personal health information for research purposes and the use of personal health information for purposes of compiling or maintaining a registry of personal health information under clause 39(1) the or for purposes of analysis or compiling statistical information with respect to managing, evaluating, monitoring, planning for, or allocating resources to, the health system under subsection 45(1) of PHIPA, as the case may be; and • The policy, procedures and practices must identify the criteria that must be considered in distinguishing between these uses, as well as the agent(s) responsible and the procedure to be followed in making this determination.
	Review and Approval Process	Review and Approval Process for Research Purposes
	• Must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the use of personal health information for research purposes and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the use of personal health information for research purposes and the request process that must be followed. At a minimum, the request process must set out the: o Documentation that must be completed, provided and/or executed: o Agent(s) responsible for completing, providing and/or executing the documentation; o Agent(s) to whom this documentation must be provided; and o Required content of the documentation.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request to use personal health information for research purposes. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the *Act* and its regulation.	• The policy, procedures and practices must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request to use personal health information for research purposes, having regard to PHIPA and its regulations.
	• Prior to any approval of the use of personal health information for research purposes, the policy and procedures must require the agent(s) responsible for determining whether to approve or deny the request to review the written research plan to ensure it complies with the requirements in the *Act* and its regulation, to ensure that the written research plan has been approved by a research ethics board and to ensure that the prescribed person or prescribed entity is in receipt of a copy of the decision of the research ethics board approving the written research plan.	• Prior to any approval of the use of personal health information for research purposes the agent(s) responsible for determining whether to approve or deny the request must ensure that: o The written research plan complies with the requirements in PHIPA and its regulations; o The written research plan has been approved by a research ethics board; and o The prescribed person or prescribed entity is in receipt of a copy of the decision of the research ethics board approving the written research plan.
	• Prior to any approval of the use of personal health information for research purposes, the agent(s) responsible for determining whether to approve or deny the request must be required to ensure that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the research ethics board. The responsible agent(s) must also be required to ensure that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal health information is being requested than is reasonably necessary to meet the research purpose.	• Prior to any approval of the use of personal health information for research purposes the agent(s) responsible for determining whether to approve or deny the request must ensure that: o The personal health information being requested is consistent with the personal health information identified in the written research plan approved by the research ethics board; o Other information, namely de-identified and/or aggregate information, will not serve the research purpose; o No more personal health information is being requested than is reasonably necessary to meet the research purpose.
	• Should set out the manner in which the decision approving or denying the request to use personal health information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	• The policy, procedures and practices must address the manner of documenting the decision approving or denying the request to use personal health information for research purposes and the reasons for the decision; and • The policy, procedures and practices must address the method and format in which the decision will be communicated, and to whom.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Conditions or Restrictions on the Approval	Conditions or Restrictions on the Approval for Research Purposes

	• Must identify the conditions or restrictions that will be imposed on the approval to use personal health information for research purposes, including any documentation that must be completed, provided or executed and the agent(s) responsible for completing, providing or executing the documentation.
	• In determining the conditions or restrictions that will be imposed, the policy and procedures shall have regard to the *Act* and its regulation.
		• The policy, procedures and practices must have regard to PHIPA and its regulations.
		• The policy, procedures and practices must identify the conditions or restrictions that will be imposed on the approval to use personal health information for research purposes.
		• The policy, procedures and practices must also:
		  ○ set out any documentation that must be completed, provided or executed to record such conditions or restrictions;
		  ○ The policy, procedures and practices must identify the agent(s) responsible for completing, providing or executing the documentation.

	• At a minimum, the agent(s) granted approval to use personal health information for research purposes must be required to comply with subsections 44(6) (a) to (f) of the Act.	• Must at a minimum, the agent(s) granted approval to use personal health information for research purposes must be required to comply with clauses 44(6) (a) to (f) of PHIPA.
	• Must identify the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of personal health information for research purposes are in fact being satisfied.	• The policy, procedures and practices must identify the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of personal health information for research purposes are in fact being satisfied.
	Secure Retention	
	• Must require the agent granted approval to use personal health information for research purposes to retain the records of personal health information in compliance with the written research plan approved by the research ethics board and in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information*.	• The policy, procedures and practices must require the agent who is granted approval to use personal health information for research purposes to retain the records of personal health information in compliance with the written research plan approved by the research ethics board and in compliance with the *Policy, Procedures and Practices for Secure Retention of Records of Personal Health Information*.
	Secure Return or Disposal	
	• Must address whether an agent granted approval to use personal health information for research purposes is required to securely return or securely dispose of the records of personal health information or is permitted to de-identify and retain the records following the retention period in the written research plan approved by the research ethics board.	• The policy, procedures and practices must address whether and in what circumstances an agent who is granted approval to use personal health information for research purposes is required to securely return or securely dispose of the records of personal health information or is permitted to de-identify and retain the records following the retention period in the written research plan approved by the research ethics board.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		<u>Secure Return of Records of Personal Health Information</u>
	• If records of personal health information are required to be securely returned to the prescribed person or prescribed entity, the policy and procedures must stipulate the time frame following the retention period set out in the written research plan within which the records must be securely returned, the secure manner in which the records must be returned and the agent to whom the records must be securely returned.	• If the records of personal health information are required to be securely returned to the prescribed person or prescribed entity, the policy, procedures and practices must require the records to be transferred in a secure manner and in compliance with the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information.* • The policy, procedures and practices must further stipulate the timeframe following the retention period set out in the written research plan within which the records must be securely returned, the secure manner in which the records must be returned and the agent to whom the records must be securely returned.
		<u>Secure Disposal of Records of Personal Health Information</u>
	• If records of personal health information are required to be disposed of in a secure manner, the policy and procedures must require the records to be disposed of in accordance with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information.*	• If the records of personal health information are required to be disposed of in a secure manner, the policy, procedures and practices must require the records to be disposed of in accordance with the *Policy, Procedures and Practices for Secure Disposal of Records of Personal Health Information.*
		<u>Certificate of Destruction</u>

	• Must stipulate the time frame following the retention period in the written research plan within which the records must be securely disposed of, must require a certificate of destruction to be provided, must identify the agent of the prescribed person or prescribed entity to whom the certificate of destruction must be provided and must identify the time frame following secure disposal within which the certificate of destruction must be provided. The certificate of destruction confirming the secure disposal must be required to identify the records of personal health information securely disposed of and the date, time and method of secure disposal employed and must be required to bear the name and signature of the agent who performed the secure disposal.	• The policy, procedures and practices must identify the:
		  ○ Agent of the prescribed person or prescribed entity to whom the certificate of destruction must be provided;
		  ○ Timeframe following the retention period in the written research plan within which the records must be securely disposed of and require a certificate of destruction to be provided; and
		  ○ Required content of the certificate of destruction.
		• A certificate that evidences the destruction of records of personal health information must, at a minimum:
		  ○ Identify the records of personal health information securely disposed of;
		  ○ Indicate the date, time and method of secure disposal employed; and
		  ○ Bear the name and signature of the agent who performed the secure disposal.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		<u>De-identification of Records of Personal Health Information</u>
	• If records of personal health information are required to be de-identified and retained by the agent rather than being securely returned or disposed of, the policy and procedures shall require the records of personal health information to be de-identified in compliance with the *Policy and Procedures With Respect to De-Identification and Aggregation*. The policy and procedures must further stipulate the time frame following the retention period set out in the written research plan within which the records must be de-identified.	• If the records of personal health information are required to be de-identified and retained by the agent rather than being securely returned or disposed of, the policy, procedures and practices must: o Require the records of personal health information to be de-identified in compliance with the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation*; and o Stipulate the timeframe following the retention period set out in the written research plan within which the records must be de-identified.
	• Must identify the agent(s) responsible for ensuring that records of personal health information used for research purposes are securely returned, securely disposed of or de-identified within the stipulated time frame following the retention period set out in the written research plan and the process to be followed in the event that the records of personal health information are not securely returned, a certificate of destruction is not received or the records of personal health information are not de-identified within the time frame identified.	• The policy, procedures and practices must also identify the agent(s) responsible for ensuring that records of personal health information used for research purposes are securely returned, securely disposed of or de- identified within the stipulated timeframe following the retention period set out in the written research plan and the process to be followed in the event of non-compliance with these requirements.
	<u>Tracking Approved Uses of Personal Health Information for Research</u>	<u>Tracking Approved Uses of Personal Health Information for Research</u>
	• Must require that a log be maintained of the approved uses of personal health information for research purposes and must identify the agent(s) responsible for maintaining such a log.	• The policy, procedures and practices must: o Require that a log be maintained of the approved uses of personal health information for research purposes; and o Identify the agent(s) responsible for maintaining such a log;
	• Recommended that the policy and procedures address where written research plans, copies of the decisions of research ethics boards, certificates of destruction and other documentation related to the receipt, review, approval or denial of requests for the use of personal health information for research purposes will be retained and the agent(s) responsible for retaining this documentation.	• The policy, procedures and practices must: o address where written research plans, copies of the decisions of research ethics boards, certificates of destruction and other documentation related to the receipt, review, approval or denial of requests for the use of personal health information for research purposes will be retained; and o identify the agent(s) responsible for retaining this documentation.
	<u>Where the Use if Personal Health Information is not Permitted for Research</u>	<u>Use of De-identified and/or Aggregate Information for Research</u>

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• If the prescribed person or prescribed entity does not permit personal health information to be used for research purposes, the policy and procedures must expressly prohibit the use of personal health information for research purposes and must indicate whether or not de-identified and/or aggregate information may be used for research purposes.	• The policy, procedures and practices must indicate whether or not de-identified and/or aggregate information may be used for research purposes. • If the prescribed person or prescribed entity permits de-identified and/or aggregate information to be used for research purposes, the policy, procedures and practices must set out the circumstances in which de-identified and/or aggregate information is permitted to be used for research purposes and require that the records of personal health information to be de-identified in compliance with the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation*.
	<u>Review and Approval Process</u>	<u>Review and Approval Process</u>
	• If the prescribed person or prescribed entity permits de-identified and/or aggregate information to be used for research purposes, the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the use of de-identified and/or aggregate information for research purposes and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	• If the prescribed person or prescribed entity permits de-identified and/or aggregate information to be used for research purposes, the policy, procedures and practices must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the use of de- identified and/or aggregate information for research purposes and the request process that must be followed. At a minimum, the request process must set out the: o Documentation that must be completed, provided and/or executed, including the: ▪ Agent(s) responsible for completing, providing and/or executing the documentation; ▪ Agent(s) to whom this documentation must be provided; and ▪ Required content of the documentation.
	• Must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request to use de-identified and/or aggregate information for research purposes. At a minimum, the policy and procedures must require the de-identified and/or aggregate information to be reviewed prior to the approval and use of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for undertaking this review shall also be identified.	• The policy, procedures and practices must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request to use de- identified and/or aggregate information for research purposes; • The policy, procedures and practices must require the de-identified and/or aggregate information to be reviewed prior to the approval and use of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual; and

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		• The policy, procedures and practices must identify the agent(s) responsible for undertaking this prior review.
	• Should set out the manner in which the decision approving or denying the request for the use of de-identified and/or aggregate information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	• The policy, procedures and practices must address the manner of documenting the decision approving or denying the request for the use of de- identified and/or aggregate information for research purposes and the reasons for the decision; and • The policy, procedures and practices must address the method and the format in which the decision will be communicated, and to whom.
	Conditions or Restrictions on the Approval	Conditions or Restrictions on the Approval
	• Must identify the conditions or restrictions that will be imposed on the approval to use de-identified and/or aggregate information for research purposes, including any documentation that must be completed, provided or executed and the agent(s) responsible for completing, providing or executing the documentation.	• The policy, procedures and practices must also identify the conditions or restrictions that will be imposed on the approval to use de-identified and/or aggregate information for research purposes, including any documentation that must be completed, provided or executed and the agent(s) responsible for completing, providing or executing the documentation.
	• Must prohibit an agent granted approval to use de-identified and/or aggregate information for research purposes from using that information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.	• The policy, procedures and practices must prohibit an agent who is granted approval to use de-identified and/or aggregate information for research purposes from using that information, either alone or with other information, to identify an individual, unless the re- identification is done in accordance with the *Policy, Procedures and Practices with Respect to De- Identification and Aggregation* and is permitted by PHIPA or another 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.
	• Must identify the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of de-identified and/or aggregate information for research purposes are in fact being satisfied.	• The policy, procedures and practices must identify the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of de-identified and/or aggregate information for research purposes are in fact being satisfied.
		Compliance, Audit and Enforcement
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	The policy, procedures and practices must: • Require agents to comply with the policy, procedures and practices;

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits,* must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures. Must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of the policy or its procedures.	• Require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the P*olicy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices; • Identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; • Address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and o Stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits*.
Policy 11. **Log of Approved Uses of Personal Health Information for Research**	• A prescribed person or prescribed entity that permits the use of personal health information for research purposes must maintain a log of the approved uses that includes:	• A prescribed person or prescribed entity that permits the use of personal health information for research purposes must maintain a log of the approved uses that, at a minimum, includes:
	• The name of the research study;	• The name of the research study;
	• The name of the agent(s) to whom the approval was granted;	• The name of the agent(s) to whom the approval was granted;
	• The date of the decision of the research ethics board approving the written research plan;	• The date of the decision of the research ethics board approving the written research plan;
	• The date that the approval to use personal health information for research purposes was granted by the prescribed person or prescribed entity;	• The date that the approval to use personal health information for research purposes was granted by the prescribed person or prescribed entity;
	• The date that the personal health information was provided to the agent(s);	• The date that the personal health information was provided to the agent(s);
	• The nature of the personal health information provided to the agent(s);	• The nature of the personal health information provided to the agent(s);
	• The retention period for the records of personal health information identified in the written research plan approved by the research ethics board;	• The retention period for the records of personal health information identified in the written research plan approved by the research ethics board;
	• Whether the records of personal health information will be securely returned, securely disposed of or de-identified and retained following the retention period; and	• Whether the records of personal health information will be securely returned, securely disposed of or de- identified and retained following the retention period;

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• The date the records of personal health information were securely returned or a certificate of destruction was received or the date by which they must be returned or disposed of, if applicable.	• The date the records of personal health information were securely returned or a certificate of destruction was received or the date by which the records of personal health information must be returned or disposed of, if applicable.
		<u>Disclosure of Personal Health Information for Purposes Other Than Research</u>
2011 Manual: Policy 12. Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research **2024 Manual: Policy 15. Policy, Procedures and Practices for Disclosure of Personal Health Information for Purposes Other than Research**	• A policy and procedures must be developed and implemented to identify whether and in what circumstances, if any, personal health information is permitted to be disclosed for purposes other than research.	• A policy, procedures, and practices must be developed and implemented to identify whether and in what circumstances, if any, personal health information is permitted to be disclosed for purposes other than research. • If the prescribed person or prescribed entity does not permit personal health information to be disclosed for purposes other than research, the policy, procedures and practices must explicitly prohibit the disclosure of personal health information for non-research purposes, except where required by law. • If the prescribed person or prescribed entity does not permit de-identified and/or aggregate information to be disclosed for purposes other than research, the policy, procedures and practices must explicitly prohibit such disclosure as well.
	• Must articulate a commitment by the prescribed person or prescribed entity not to disclose personal health information if other information will serve the purpose and not to disclose more personal health information than is reasonably necessary to meet the purpose.	• The policy, procedures and practices must articulate a commitment by the prescribed person or prescribed entity not to disclose personal health information if other information will serve the purpose and not to disclose more personal health information than is reasonably necessary to meet the purpose.
	<u>Where the Disclosure of Personal Health Information is Permitted</u>	<u>Where the Disclosure of Personal Health Information is Permitted</u>
	• If the prescribed person or prescribed entity permits personal health information to be disclosed for purposes other than research, the policy and procedures must set out the purposes for which and the circumstances in which the disclosure of personal health information is permitted.	• The policy, procedures and practices must set out the purposes other than research for which and the circumstances in which the disclosure of personal health information is permitted.
	• Must require that all disclosures of personal health information comply with the *Act* and its regulation.	• The policy, procedures and practices must require that all such disclosures comply with PHIPA and its regulations.
	<u>Review and Approval Process</u>	<u>Review and Approval Process</u>

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of personal health information for purposes other than research and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of personal health information for purposes other than research and the process that must be followed. At a minimum, the request process must set out the: o Documentation that must be completed, provided and/or executed; o Agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; o Agent(s) to whom this documentation must be provided; and o Required content of the documentation.
	• Must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request for the disclosure of personal health information for purposes other than research. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the *Act* and its regulation.	• Having regard to PHIPA and its regulations, the policy, procedures and practices must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request for the disclosure of personal health information for purposes other than research.
	• The agent(s) responsible for determining whether to approve or deny the request for the disclosure of personal health information for purposes other than research must be required to ensure that the disclosure is permitted by the *Act* and its regulation and that any and all conditions or restrictions set out in the *Act* and its regulation have been satisfied. For example, if a prescribed entity is requested to disclose personal health information to a health information custodian who provided the personal health information directly or indirectly to the prescribed entity, the prescribed entity must ensure that the personal health information does not contain any additional identifying information.	• The agent(s) responsible for determining whether to approve or deny the request for the disclosure of personal health information for purposes other than research must be required to ensure that: o The disclosure is permitted by PHIPA and its regulations and that any and all conditions or restrictions set out in PHIPA and its regulations have been satisfied.
	• The criteria must require the agent(s) responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose of the disclosure and that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.	• The agent(s) responsible for determining whether to approve or deny the request for the disclosure of personal health information for purposes other than research must be required to ensure that: o Other information, namely de-identified and/or aggregate information, will not serve the identified purpose of the disclosure.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		○ No more personal health information is being requested than is reasonably necessary to meet the identified purpose.
	• Should set out the manner in which the decision approving or denying the request for the disclosure of personal health information for purposes other than research and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	• The policy, procedures and practices must also set out: ○ The reasons for the decision; ○ The manner of documenting the decision approving or denying the request for the disclosure of personal health information for purposes other than research; ○ The method by which and the format in which the decision will be communicated; and ○ To whom the decision will be communicated.
	<u>Conditions or Restrictions on the Approval</u>	<u>Conditions or Restrictions on the Approval</u>
	• Must identify the conditions or restrictions that are required to be satisfied prior to the disclosure of personal health information for purposes other than research, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements.	• The policy, procedures and practices must identify the conditions or restrictions that are required to be satisfied prior to the disclosure of personal health information for purposes other than research, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements.
	• Must require a data sharing agreement to be executed in accordance with the *Policy and Procedures for the Execution of Data Sharing Agreements* and the *Template Data Sharing Agreement* prior to any disclosure of personal health information for purposes other than research.	• The policy, procedures and practices must require a data sharing agreement to be executed in accordance with the *Policy, Procedures and Practices for the Execution of Data Sharing Agreements* and the *Template Data Sharing Agreement* prior to any disclosure of personal health information for purposes other than research.
	• Must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal health information have in fact been satisfied, including the execution of a data sharing agreement.	• The policy, procedures and practices must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal health information have, in fact, been satisfied, including the execution of a data sharing agreement.
	<u>Secure Transfer</u>	
	• Must require records of personal health information to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.	• The policy, procedures and practices must require records of personal health information to be transferred in a secure manner in compliance with the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information.*

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Secure Return or Disposal	Secure Return or Disposal of Records of Personal Health Information
	• Must identify the agent(s) responsible for ensuring that records of personal health information disclosed to a person or organization for purposes other than research are either securely returned or securely disposed of, as the case may be, following the retention period in the data sharing agreement or the date of termination of the data sharing agreement.	• The policy, procedures and practices must identify the agent(s) responsible for ensuring that records of personal health information disclosed to a person or organization for purposes other than research are either securely returned or securely disposed of, as the case may be, following the retention period in the data sharing agreement or the date of termination of the data sharing agreement.
	• Must address the process to be followed where records of personal health information are not securely returned or a certificate of destruction is not received within a reasonable period of time following the retention period in the data sharing agreement or the date of termination of the data sharing agreement. This shall include the agent(s) responsible for implementing this process and the stipulated time frame following the retention period or the date of termination within which this process must be implemented.	• The policy, procedures and practices must address the process to be followed where records of personal health information are not securely returned or a certificate of destruction is not received within a reasonable period of time following the retention period in the data sharing agreement or the date of termination of the data sharing agreement; and • The policy, procedures and practices must identify the agent(s) responsible for implementing this process and the stipulated timeframe following the retention period or the date of termination within which this process must be implemented.
	Documentation Related to Approved Disclosures of Personal Health Information	Documentation Related to Approved Disclosures of Personal Health Information
	• It is recommended that the policy and procedures address where documentation related to the receipt, review, approval or denial of requests for the disclosure of personal health information for purposes other than research will be retained and the agent(s) responsible for retaining this documentation.	• The policy, procedures and practices must address where documentation related to the receipt, review, approval or denial of requests for the disclosure of personal health information for purposes other than research will be retained and the agent(s) responsible for retaining this documentation.
	Where the Disclosure of Personal Health Information is not Permitted	Disclosure of De-Identified and/or Aggregate Information

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• If the prescribed person or prescribed entity does not permit personal health information to be disclosed in these circumstances, the policy and procedures must expressly prohibit the disclosure of personal health information for non-research purposes, except where required by law, and must indicate whether or not de-identified and/or aggregate information may be disclosed.	• The policy, procedures and practices must indicate whether de-identified and/or aggregate information may be disclosed for purposes other than research, and if so, must set out the circumstances in which de-identified and/or aggregate information is permitted to be disclosed for non-research purposes and comply with the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation*.
	<u>Review and Approval Process</u>	<u>Review and Approval Process</u>
	• If the prescribed person or prescribed entity permits de-identified and/or aggregate information to be disclosed for non-research purposes, the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of de-identified and/or aggregate information and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	• If the prescribed person or prescribed entity permits de-identified and/or aggregate information to be disclosed for non-research purposes, the policy, procedures and practices must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of de-identified and/or aggregate information and the process that must be followed. At a minimum, the request process must set out the: o Documentation that must be completed, provided and/or executed; o Agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; o Agent(s) to whom this documentation must be provided; and o Required content of the documentation.
	• Must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for purposes other than research.	• The policy, procedures and practices must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for purposes other than research.
	• Must require the de-identified and/or aggregate information to be reviewed prior to the disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for undertaking this review shall also be identified.	• The policy, procedures and practices must require the de-identified and/or aggregate information to be reviewed prior to the approval and the subsequent disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual; and • The policy, procedures and practices must identify the agent(s) responsible for undertaking this review.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Should set out the manner in which the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for purposes other than research and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	• The policy, procedures and practices must also specify the manner of documenting the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for purposes other than research and the reasons for the decision; and • The policy, procedures and practices must also specify the method by which and the format in which the decision will be communicated and to whom.
	<u>Conditions or Restrictions on the Approval</u>	<u>Conditions or Restrictions on the Approval</u>
	• Must identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for non-research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements.	• The policy, procedures and practices must identify the conditions or restrictions that are required to be satisfied prior to the approval and the subsequent disclosure of de-identified and/or aggregate information for non-research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements.
	• The prescribed person or prescribed entity must require the person or organization to which the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the person or organization will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.	• The prescribed person or prescribed entity must require the person or organization to which the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the person or organization will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is permitted by 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. ▪ Note: Where the policies, procedures and practices of a prescribed entity or prescribed person address different release models and the calculated risk of re-identification has met the threshold for the data release to be made "public," such written acknowledgement may not be necessary.
	• Must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have in fact been satisfied, including the execution of the written acknowledgement.	• The policy, procedures and practices must also identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have, in fact, been satisfied, including the execution of the written acknowledgement.
	• Must require the responsible agent(s) to track receipt of the executed written acknowledgments and must set out the procedure that must be followed and the documentation that must be maintained in this regard.	• The policy, procedures and practices must require the responsible agent(s) to track receipt of the executed written acknowledgments and must set out the procedure that must be followed and the documentation that must be maintained.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		<u>Compliance, Audit and Enforcement</u>
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. • Must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures. • Must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.	• The policy, procedures and practices must: o Require agents to comply with the policy, procedures and practices; o Require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices; o Identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; o Address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and, o Stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits*.
		<u>Disclosure of Personal Health Information for Research</u>
2011 Manual: Policy 13. Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements **2024 Manual: Policy 12. Policy, Procedures and Practices for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements.**	• Must be developed and implemented to identify whether and in what circumstances, if any, the prescribed person or prescribed entity permits personal health information to be disclosed for research purposes.	• A policy, procedures and practices must be developed and implemented to identify whether and in what circumstances, if any, the prescribed person or prescribed entity permits personal health information to be disclosed for research purposes. • If the prescribed person or prescribed entity does not permit personal health information to be disclosed for research purposes, the policy, procedures and practices must explicitly prohibit the disclosure of personal health information for research purposes and indicate whether or not de-identified and/or aggregate information may be disclosed for research purposes. • If the prescribed person or prescribed entity does not permit de-identified and/or aggregate information to be disclosed for research purposes, the policy, procedures and practices must explicitly prohibit the disclosure of de-identified and/or aggregate information as well.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Where the Disclosure of Personal Health Information is Permitted for Research	Where the Disclosure of Personal Health Information is Permitted for Research
	• Must articulate a commitment by the prescribed person or prescribed entity not to disclose personal health information for research purposes if other information will serve the research purpose and not to disclose more personal health information than is reasonably necessary to meet the research purpose. • If the prescribed person or prescribed entity permits personal health information to be disclosed for research purposes, the policy and procedures must set out the circumstances in which personal health information is permitted to be disclosed for research purposes.	• Where the prescribed person or prescribed entity permits the disclosure of personal health information for research purposes, the policy, procedures and practices must articulate a commitment by the prescribed person or prescribed entity not to disclose personal health information for research purposes if other information will serve the research purpose and not to disclose more personal health information than is reasonably necessary to meet the research purposes. • Where the prescribed person or prescribed entity permits the disclosure of personal health information for research purposes, the policy, procedures and practices must set out the circumstances in which personal health information is permitted to be disclosed for research purposes.
	Review and Approval Process	Review and Approval Process
	• Must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of personal health information for research purposes, as well as the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed by agent(s) of the prescribed person or prescribed entity or by the researcher; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of personal health information for research purposes, as well as the process that must be followed. At a minimum, the request process must set out the: o Documentation that must be completed, provided and/or executed by agent(s) of the prescribed person or prescribed entity or by the researcher; o Agent(s) to whom this documentation must be provided; and o Required content of the documentation.
	• Must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request for the disclosure of personal health information for research purposes. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the *Act* and its regulation.	• The policy, procedures and practices must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request for the disclosure of personal health information for research purposes.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Prior to any approval of the disclosure of personal health information for research purposes, must require the agent(s) responsible for determining whether to approve or deny the request to ensure that the prescribed person or prescribed entity is in receipt of a written application, a written research plan and a copy of the decision of the research ethics board approving the written research plan and that the written research plan complies with the requirements in the *Act* and its regulation.	• Prior to any approval of the disclosure of personal health information for research purposes, the policy, procedures and practices must require the agent(s) responsible for determining whether to approve or deny the request to ensure that: o The prescribed person or prescribed entity is in receipt of a written application accompanied by a written research plan and a copy of the decision of the research ethics board approving the written research plan; and o The written research plan complies with the requirements in PHIPA and its regulations.
	• Prior to any approval of the disclosure of personal health information for research purposes, the agent(s) responsible for determining whether to approve or deny the request must be required to ensure that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the research ethics board.	• Prior to any approval of the disclosure of personal health information for research purposes, the policy, procedures and practices must require the agent(s) responsible for determining whether to approve or deny the request to ensure that: o the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the research ethics board;
	• The responsible agent(s) must be required to ensure that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal health information is being requested than is reasonably necessary to meet the research purpose.	• Prior to any approval of the disclosure of personal health information for research purposes, the policy, procedures and practices must require the agent(s) responsible for determining whether to approve or deny the request to ensure that: o Other information, namely de-identified and/or aggregate information, will not serve the research purpose; and o No more personal health information is being requested than reasonably necessary to meet the research purpose.
	• Should also set out the manner in which the decision approving or denying the request for the disclosure of personal health information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	• The policy, procedures and practices must also set out: o The manner of documenting the decision approving or denying the request for the disclosure of personal health information for research purposes and the reasons for the decision; o The method by which and the format in which the decision will be communicated; and o To whom the decision will be communicated.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Conditions or Restrictions on the Approval	Conditions or Restrictions on the Approval
	• Must identify the conditions or restrictions that are required to be satisfied prior to the disclosure of personal health information for research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or researcher responsible for completing, providing or executing the documentation and/or agreements.	• The policy, procedures and practices must identify the conditions or restrictions that are required to be satisfied prior to the approval of disclosure of personal health information for research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or researcher responsible for completing, providing or executing the documentation and/or agreements.
	• Must require that a research agreement be executed in accordance with the *Template Research Agreement* prior to the disclosure of personal health information for research purposes.	• The policy, procedures and practices must require that a research agreement be executed in accordance with the template research agreement prior to the disclosure of personal health information for research purposes.
	• Must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal health information for research purposes have in fact been satisfied, including the execution of a research agreement.	• The policy, procedures and practices must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal health information for research purposes have, in fact, been satisfied, including the execution of a research agreement.
	Secure Transfer	
	• Must require the records of personal health information disclosed for research purposes to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.	• The policy, procedures and practices must require the records of personal health information disclosed for research purposes to be transferred in a secure manner in compliance with the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information*.
	Secure Return or Disposal	Secure Return, Disposal or De-Identification of Records of Personal Health Information for Research
	• Must identify the agent(s) responsible for ensuring that records of personal health information disclosed to a researcher for research purposes are either securely returned, securely disposed of or de-identified, as the case may be, following the retention period set out in the research agreement.	• The policy, procedures and practices must identify the agent(s) responsible for ensuring that records of personal health information disclosed to a researcher for research purposes are either securely returned, securely disposed of or de-identified in compliance with the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation*, as the case may be, within a specific timeframe following the retention period set out in the research agreement.
	• Must address the process to be followed by the responsible agent(s) where records of personal health information are not securely returned, a certificate of destruction is not received or written confirmation of de- identification is not received within the time set out in the research agreement.	• The policy, procedures and practices must address the process to be followed by the responsible agent(s) where records of personal health information are not securely returned, a certificate of destruction is not received or written confirmation of de-identification is not received within the time set out in the research agreement.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	<u>Documentation Related to Approved Disclosures of Personal Health Information for Research</u>	<u>Documentation Related to Approved Disclosures of Records of Personal Health Information for Research</u>
	• It is recommended that the policy and procedures also address where written applications, written research plans, copies of the decisions of research ethics boards, research agreements, certificates of destruction and other documentation related to the receipt, review, approval or denial of requests for the disclosure of personal health information for research purposes will be retained and the agent(s) responsible for retaining this documentation.	• The policy, procedures and practices must also: o Address where documentation related to the receipt, review, approval, or denial of requests for the disclosure of personal health information for research purposes will be retained, including written applications, written research plans, copies of the decisions of research ethics boards, research agreements, and certificates of destruction; and o Identify the agent(s) responsible for retaining this documentation.
	<u>Where the Disclosure of Personal Health Information is not Permitted for Research</u>	<u>Disclosure of De-Identified and/or Aggregate Information for Research Purposes</u>
	• If the prescribed person or prescribed entity does not permit personal health information to be disclosed for research purposes, the policy and procedures must expressly prohibit the disclosure of personal health information for research purposes and must indicate whether or not de- identified and/or aggregate information may be disclosed for research purposes.	• If the prescribed person or prescribed entity permits de-identified and/or aggregate information to be disclosed for research purposes, the policy, procedures and practices must set out the circumstances in which de-identified and/or aggregate information is permitted to be disclosed for research purposes.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Review and Approval Process	Review and Approval Process
	• If the prescribed person or prescribed entity permits de-identified and/or aggregate information to be disclosed for research purposes, the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of de-identified and/or aggregate information for research purposes, as well as the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed by agent(s) of the prescribed person or prescribed entity or by a researcher; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of de- identified and/or aggregate information for research purposes, and the request process that must be followed. At a minimum, the request process must set out the: o Documentation that must be completed, provided and/or executed by agent(s) of the prescribed person or prescribed entity or by a researcher, having regard to PHIPA and its regulations; o Agent(s) to whom this documentation must be provided; and o Required content of the documentation.
	• For example, the policy and procedures should address whether the prescribed person or prescribed entity requires the preparation of a written research plan in accordance with the *Act* and its regulation and/or requires research ethics board approval of the written research plan prior to the disclosure of de-identified and/or aggregate information for research purposes.	• The policy, procedures and practices should address whether the prescribed person or prescribed entity requires the preparation of a written research plan in accordance with PHIPA and its regulations and/or requires research ethics board approval of the written research plan prior to the approval and the subsequent disclosure of de-identified and/or aggregate information for research purposes.
	• Must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for research purposes.	• The policy, procedures and practices must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for research purposes.
	• Must require the de-identified and/or aggregate information to be reviewed prior to the approval and disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for undertaking this review shall also be identified.	• The policy, procedures and practices must require the de-identified and/or aggregate information to be reviewed prior to the approval and the subsequent disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual; • The policy, procedures and practices must identify the agent(s) responsible for undertaking the review.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Should also set out the manner in which the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	• The policy, procedures and practices must set out the manner of documenting the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for research purposes and the reasons for the decision; • The policy, procedures and practices must set out the method and format in which the decision will be communicated, and to whom.
	<u>Conditions or Restrictions on the Approval</u>	<u>Conditions or Restrictions on the Approval</u>
		• The policy, procedures and practices must comply with the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation.*
	• Must identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or researcher responsible for completing, providing or executing the documentation and/or agreements.	• The policy, procedures and practices must identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for research purposes, including: o Any documentation and/or agreements that must be completed, provided or executed; and o The agent(s) or researcher responsible for completing, providing or executing the documentation and/or agreements.
	• The prescribed person or prescribed entity must require the researcher to whom the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the researcher will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.	• The prescribed person or prescribed entity must require the researcher to whom the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the researcher will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is permitted by PHIPA or another Act and is in accordance with the written research plan approved by the research ethics board. This must include prohibiting any attempt to decrypt information that is encrypted or identifying an individual based on unencrypted information and/or prior knowledge. • Note: Where the policies, procedures and practices of a prescribed person or a prescribed entity address different release models and the calculated risk of re-identification has met the threshold for the data release to be made "public," such written acknowledgement may not be necessary.
	• Must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have in fact been satisfied, including the execution of the written acknowledgement.	• The policy, procedures and practices must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have, in fact, been satisfied, including the execution of the written acknowledgement and agreement.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must require the responsible agent(s) to track receipt of the executed written acknowledgments and set out the procedure that must be followed and the documentation that must be maintained in this regard.	• The policy, procedures and practices must require the responsible agent(s) to track receipt of the executed written acknowledgements and agreements; and • The policy, procedures and practices must set out the procedure that must be followed and related documentation that must be maintained.
		• The policy, procedures and practices must identify the documentation and/or agreements that must be completed, provided or executed and the agent(s) or researcher responsible for completing, providing or executing the documentation and/or agreements.
		<u>Compliance, Audit and Enforcement</u>
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. • Must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures. Must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.	• The policy, procedures and practices must: o Require agents to comply with the policy, procedures and practices; o Require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices; o Identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; o Address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and o Stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits*.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
2011 Manual: Policy 14. Template Research Agreement **2024 Manual: Policy 13. Template Research Agreement**	• A research agreement must be executed with the researchers to whom personal health information will be disclosed prior to the disclosure of the personal health information for research purposes.	• A research agreement must be executed with the researchers to whom personal health information will be disclosed prior to the disclosure of the personal health information for research purposes.
	<u>General Provisions</u>	
	• The research agreement must describe the status of the prescribed person or prescribed entity under the *Act* and the duties and responsibilities arising from this status.	• The research agreement must describe the status of the prescribed person or prescribed entity under PHIPA and the duties and responsibilities arising from this status;
	• The research agreement must specify the precise nature of the personal health information that will be disclosed by the prescribed person or prescribed entity for research purposes and must provide a definition of personal health information that is consistent with the *Act* and its regulation.	• The research agreement must provide a definition of personal health information that is consistent with PHIPA and its regulations; • The research agreement must specify the precise nature of the personal health information that will be disclosed by the prescribed person or prescribed entity for research purposes; and
		• The research agreement must, where applicable, set out any restrictions with respect to small cell-sizes (e.g. less than five), having regard to the *Policy, Procedures and Practices with Respect to De- Identification and Aggregation* implemented by the prescribed person or prescribed entity and the written research plan.
	<u>Purposes of Collection, Use and Disclosure</u>	<u>Purposes of Collection, Use and Disclosure</u>
	• The research agreement must identify the research purpose for which the personal health information is being disclosed by the prescribed person or prescribed entity and the purposes for which the personal health information may be used or disclosed by the researcher.	• The research agreement must identify the research purpose for which the personal health information is being disclosed by the prescribed person or prescribed entity; • The research agreement must identify the purposes for which the personal health information may be used or disclosed by the researcher;
	• The research agreement must identify the statutory authority for each collection, use and disclosure identified.	• The research agreement must specify the statutory authority for each collection, use and disclosure identified; and
		• The research agreement must explicitly state whether the personal health information may be linked to other information.
	• The research agreement must only permit the researcher to use the personal health information for the purposes set out in the written research plan approved by the research ethics board and must prohibit the use of the personal health information for any other purpose.	• The research agreement must only permit the researcher to use the personal health information for the purposes set out in the written research plan approved by the research ethics board and must prohibit the use of the personal health information for any other purpose.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• The research agreement must prohibit the researcher from permitting persons to access and use the personal health information except those persons described in the written research plan approved by the research ethics board.	• The research agreement must prohibit the researcher from permitting any person to access and use the personal health information except those persons described in the written research plan approved by the research ethics board.
	• In identifying the purposes for which the personal health information may be used, the research agreement must explicitly state whether or not the personal health information may be linked to other information and must prohibit the personal health information from being linked except in accordance with the written research plan approved by the research ethics board.	• In identifying the purposes for which the personal health information may be used, the research agreement must explicitly: o State whether the personal health information may be linked to other information; and o Prohibit the personal health information from being linked except in accordance with the written research plan approved by the research ethics board.
	• Must require the researcher to acknowledge that the personal health information that is being disclosed pursuant to the research agreement is necessary for the identified research purpose and that other information, namely de-identified and/or aggregate information, will not serve the research purpose.	• The research agreement must require the researcher to acknowledge that the personal health information that is being disclosed pursuant to the research agreement is necessary for the identified research purpose(s) and that other information, namely de-identified and/or aggregate information, will not serve the research purpose.
	• The researcher must be required to acknowledge that no more personal health information is being collected and will be used than is reasonably necessary to meet the research purpose.	• The research agreement must require the researcher to acknowledge that no more personal health information is being collected and will be used than is reasonably necessary to meet the research purpose.
	• Must impose restrictions on the disclosure of personal health information.	• The research agreement must impose restrictions on the disclosure of personal health information.
	• Must require the researcher to acknowledge and agree not to disclose the personal health information except as required by law and subject to the exceptions and additional requirements prescribed in the regulation to the *Act*; not to publish the personal health information in a form that could reasonably enable a person to ascertain the identity of the individual; and not to make contact or attempt to make contact with the individual to whom the personal health information relates, directly or indirectly, unless the consent of the individual to being contacted is first obtained in accordance with subsection 44(6) of the *Act*.	• The research agreement must require the researcher to acknowledge and agree not to: o Disclose the personal health information except as required by law and subject to the exceptions and additional requirements prescribed in PHIPA's regulations; o Publish the personal health information in a form that could reasonably enable a person to ascertain the identity of the individual; or o Make contact or attempt to make contact with the individual to whom the personal health information relates, directly or indirectly, unless the consent of the individual to being contacted is first obtained in accordance with subsection 44(6) of PHIPA.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	<u>Compliance with the Statutory Requirements for the Disclosure for Research Purposes</u>	<u>Compliance with the Statutory Requirements for the Disclosure for Research Purposes</u>
	• Must require the researcher and the prescribed person or prescribed entity to acknowledge and agree that the researcher has submitted an application in writing, a written research plan that meets the requirements of the *Act* and its regulation, and a copy of the decision of the research ethics board approving the written research plan.	• The research agreement must require the researcher and the prescribed person or prescribed entity to acknowledge and agree that the researcher has submitted an application in writing, a written research plan, and a copy of the decision of the research ethics board approving the written research plan, that meets the requirements of PHIPA and its regulations.
	• Must require the researcher to acknowledge and agree that the researcher will comply with the research agreement, with the written research plan approved by the research ethics board and with the conditions, if any, specified by the research ethics board in respect of the written research plan.	• The research agreement must require the researcher to also acknowledge and agree that the researcher will comply with the: o Research agreement; o Written research plan approved by the research ethics board; and o Conditions, if any, specified by the research ethics board in respect of the written research plan.
	<u>Secure Transfer</u>	<u>Secure Transfer of Records of Personal Health Information</u>
	• Must require the secure transfer of records of personal health information that will be disclosed pursuant to the research agreement.	• The research agreement must require the secure transfer of records of personal health information that will be disclosed pursuant to the research agreement.
	• Must set out the secure manner in which records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that will be followed in ensuring that the records of personal health information are transferred in a secure manner.	• The research agreement must set out the secure manner in which records of personal health information will be transferred, including: o Under what conditions and to whom the records will be transferred; and o The procedure that will be followed in ensuring that the records of personal health information are transferred in a secure manner.
	• In identifying the secure manner in which the records of personal health information will be transferred, the research agreement must have regard to the *Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.	• In identifying the secure manner in which the records of personal health information will be transferred, the research agreement must have regard to the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Secure Retention	Secure Retention of Records of Personal Health Information
	• Must identify the retention period for the records of personal health information subject to the research agreement, including the length of time that the records of personal health information will be retained in identifiable form. The retention period identified must be consistent with that set out in the written research plan approved by the research ethics board.	• The research agreement must identify the retention period for the records of personal health information subject to the research agreement, including the length of time that the records of personal health information will be retained in identifiable form (the retention period identified must be consistent with that set out in the written research plan approved by the research ethics board).
	• Must require the researcher to ensure that the records of personal health information are retained in a secure manner and must identify the precise manner in which the records of personal health information in paper and electronic format will be securely retained.	• The research agreement must require the researcher to ensure that the records of personal health information are retained in a secure manner and must identify the precise manner in which the records of personal health information in paper and electronic format will be securely retained.
	• In identifying the secure manner in which the records of personal health information will be retained, the research agreement may have regard to the *Policy and Procedures for Secure Retention of Records of Personal Health Information* and shall have regard to the written research plan approved by the research ethics board.	• In identifying the secure manner in which the records of personal health information will be retained, the research agreement may have regard to the *Policy, Procedures and Practices for Secure Retention of Records of Personal Health Information* and must have regard to the written research plan approved by the research ethics board.
	• Must require the researcher to take steps that are reasonable in the circumstances to ensure that the personal health information subject to the research agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information subject to the research agreement are protected against unauthorized copying, modification or disposal.	• The research agreement must require the researcher to take steps that are reasonable in the circumstances to ensure that the records of personal health information subject to the research agreement are: o Protected against theft, loss and unauthorized collection, use or disclosure; and o Protected against unauthorized copying, modification or disposal;
	• Must detail the reasonable steps that are required to be taken by the researcher and must include those set out in the written research plan approved by the research ethics board.	• The research agreement must detail the reasonable steps that the researcher is required to take, which, at a minimum, must include those set out in the written research plan approved by the research ethics board.
	Secure Return or Disposal	
	• Must address whether the records of personal health information subject to the research agreement will be returned in a secure manner, will be disposed of in a secure manner or will be de-identified and retained by the researcher following the retention period set out in the research agreement. In this regard, the provisions in the research agreement must be consistent with the written research plan approved by the research ethics board.	• The research agreement must also address whether the records of personal health information subject to the research agreement will be returned in a secure manner, will be disposed of in a secure manner or will be de-identified and retained by the researcher following the retention period set out in the research agreement. In this regard, the provisions in the research agreement must be consistent with the written research plan approved by the research ethics board.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		<u>Secure Return of Records of Personal Health Information</u>
	• If the records of personal health information are required to be returned in a secure manner, the research agreement must stipulate the time frame following the retention period within which the records must be securely returned, the secure manner in which the records must be returned and the agent of the prescribed person or prescribed entity to whom the records must be securely returned.	• If the records of personal health information are required to be returned in a secure manner, the research agreement must stipulate the: o Timeframe following the retention period within which the records must be securely returned; o Secure manner in which the records must be returned; and o Agent of the prescribed person or prescribed entity to whom the records must be securely returned.
	• In identifying the secure manner in which the records of personal health information will be returned, regard may be had to the *Policy and Procedures for Secure Transfer of* Records *of Personal Health Information* implemented by the prescribed person or prescribed entity.	• In identifying the secure manner in which the records of personal health information will be returned, regard may be had to the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.
	• If the records of personal health information are required to be disposed of in a secure manner, the research agreement must provide a definition of secure disposal that is consistent with the *Act* and its regulation and must identify the precise manner in which the records of personal health information subject to the research agreement must be securely disposed of.	• If the records of personal health information subject to the research agreement are required to be disposed of in a secure manner, the research agreement must: o Provide a definition of secure disposal that is consistent with PHIPA and its regulations; o Identify the precise manner in which the records of personal health information must be securely disposed of; and
	• Must stipulate the time frame following the retention period set out in the research agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided.	• The research agreement must stipulate the timeframe following the retention period set out in the research agreement within which: o The records of personal health information must be securely disposed of; and o A certificate of destruction must be provided.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• In identifying the secure manner in which the records of personal health information will be disposed of, it must be ensured that the method of secure disposal identified is consistent with the *Act* and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including *Fact Sheet 10: Secure Destruction of Personal Information*. In addition, regard may be had to the *Policy and Procedures for Secure Disposal of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.	• In identifying the secure manner in which the records of personal health information will be disposed of, the method of secure disposal identified must at a minimum be consistent with: ○ PHIPA and its regulations; ○ Orders and decisions issued by the Information and Privacy Commissioner of Ontario under PHIPA and its regulations, including Order HO-001 and Order HO-006; ○ Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to PHIPA and its regulations, including Fact Sheet 10: Secure Destruction of Personal Information; and ○ Policies, procedures and practices implemented by the prescribed person or prescribed entity, such as the *Policy, Procedures and Practices for Secure Disposal of Records of Personal Health Information*.
		Certificate of Destruction
	• Must identify the agent of the prescribed person or prescribed entity to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided and the required content of the certificate of destruction.	• The Research Agreement must identify the: ○ Agent of the prescribed person or prescribed entity to whom the certificate of destruction must be provided; ○ Timeframe following secure disposal within which the certificate of destruction must be provided; and ○ Required content of the certificate of destruction.
	• The certificate of destruction must be required to identify the records of personal health information securely disposed of; to stipulate the date, time, location and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.	• A certificate that evidences the destruction of records of personal health information must, at a minimum: ○ Identify the records of personal health information securely disposed of; ○ Stipulate the date, time, location and method of secure disposal employed; and ○ Bear the name and signature of the person who performed the secure disposal.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		<u>Where Records are De-identified and Retained</u>
	• If the records of personal health information are required to be de-identified and retained by the researcher rather than being securely returned or disposed of, the manner and process for de- identification must be set out in the research agreement.	• If the records of personal health information are required to be de-identified and retained by the researcher rather than being securely returned or disposed of, the manner and process for de-identification must be set out in the research agreement.
	• In identifying the manner and process for de-identification, regard may be had to the *Policy and Procedures with Respect to De- Identification and Aggregation* implemented by the prescribed person or prescribed entity.	• In identifying the manner and process for de-identification, regard may be had to the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation* implemented by the prescribed person or prescribed entity.
	• Must require the researcher to submit written confirmation that the records were de-identified and shall stipulate the time frame following the retention period set out in the research agreement within which the written confirmation must be provided and the agent of the prescribed person or prescribed entity to whom the written confirmation must be provided.	• The Research Agreement must also: o Require the researcher to submit written confirmation that the records were de-identified; o Stipulate the timeframe following the retention period set out in the research agreement within which the written confirmation must be provided; and o Specify the agent of the prescribed person or prescribed entity to whom the written confirmation must be provided.
		• The research agreement must also require the researcher to whom the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the researcher will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is permitted by PHIPA or another Act and is in accordance with the written research plan approved by the research ethics board. This must include prohibiting any attempt to decrypt information that is encrypted or identifying an individual based on unencrypted information and/or prior knowledge.
		• In accordance with the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation*, a prescribed person or prescribed entity may address different release models (i.e. public, semi-public, and non- public) in its policies, procedures and practices. Where the policies, procedures and practices of a prescribed person or prescribed entity address different release models and the calculated risk of re-identification has met the threshold for the data release to be made "public," such written acknowledgement may not be necessary.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Notification	Breach Notification to Prescribed Person or Prescribed Entity
	• Must require the researcher to notify the prescribed person or prescribed entity immediately, in writing, if the researcher becomes aware of a breach or suspected breach of the research agreement, a breach or suspected of subsection 44(6) of the *Act* or if personal health information subject to the research agreement is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons.	• The research agreement must require the researcher to notify the prescribed person or prescribed entity immediately, in writing, if the researcher becomes aware: o Of a breach or suspected breach of the research agreement; o A breach or suspected breach of subsection 44(6) of PHIPA; and o If personal health information subject to the research agreement is stolen, lost or collected, used or disclosed without authority or is believed to have been stolen, lost or collected, used or disclosed without authority.
	• Should identify the agent of the prescribed person or prescribed entity to whom notification must be provided and must require the researcher to take steps that are reasonable in the circumstances to contain the breach and to contain the theft, loss or access by unauthorized persons.	• The research agreement should identify the agent of the prescribed person or prescribed entity to whom notification must be provided and must require the researcher to take steps that are reasonable in the circumstances to contain the breach.
	Consequences of Breach and Monitoring Compliance	Consequences of Breach and Monitoring Compliance
	• Must outline the consequences of breach of the agreement and must indicate whether compliance with the research agreement will be audited by the prescribed person or prescribed entity and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.	• The Research Agreement must also: o Provide the prescribed person or prescribed entity with the right to audit the researcher's compliance with the agreement; o Set out the manner and circumstances in which compliance will be audited and the notice, if any, that will be provided to the researcher of the audit; and o Outline the consequences of breach of the agreement.
	• Must require the researcher to ensure that all persons who will have access to the personal health information, as identified in the written research plan approved by the research ethics board, are aware of and agree to comply with the terms and conditions of the research agreement prior to being given access to the personal health information.	• The research agreement must require the researcher to ensure that all persons who will have access to the personal health information, as identified in the written research plan approved by the research ethics board, are aware of and agree to comply with the terms and conditions of the research agreement prior to being given access to the personal health information.
	• Must set out the method by which this will be ensured by the researcher, such as requiring the persons identified in the written research plan to sign an acknowledgement prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the research agreement.	• The research agreement must set out the method by which this will be ensured by the researcher, such as requiring the persons identified in the written research plan to sign an acknowledgement prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the research agreement.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
2011 Manual: Policy 15. Log of Research Agreements **2024 Manual: Policy 14. Log of Research Agreements**	• A prescribed person or prescribed entity must maintain a log of executed research agreements. At a minimum, the log must include:	• A prescribed person or prescribed entity must maintain a log of executed research agreements. At a minimum, the log must include:
	• The name of the research study;	• The name of the research study;
	• The name of the principal researcher to whom the personal health information was disclosed pursuant to the research agreement;	• The name of the principal researcher to whom the personal health information was disclosed pursuant to the research agreement;
	• The date(s) of receipt of the written application, the written research plan and the written decision of the research ethics board approving the research plan;	• The date(s) of receipt of the written application, the written research plan and the written decision of the research ethics board approving the research plan;
	• The date that the approval to disclose the personal health information for research purposes was granted by the prescribed person or prescribed entity;	• The date that the approval to disclose the personal health information for research purposes was granted by the prescribed person or prescribed entity;
	• The date that the research agreement was executed;	• The date that the research agreement was executed;
	• the date that the personal health information was disclosed;	• The date that the personal health information was disclosed;
	• The nature of the personal health information disclosed;	• The nature of the personal health information disclosed;
	• The retention period for the records of personal health information as set out in the research agreement;	• The retention period for the records of personal health information as set out in the research agreement;
	• Whether the records of personal health information will be securely returned, securely disposed of or de-identified and retained by the researcher following the retention period set out in the research agreement; and	• Whether the records of personal health information will be securely returned, securely disposed of or de- identified and retained by the researcher following the retention period set out in the research agreement; and
	• The date that the records of personal health information were securely returned, a certificate of destruction was received or written confirmation of de-identification was received or the date by which they must be returned, disposed of or de-identified.	• The date that the records of personal health information were securely returned, a certificate of destruction was received or written confirmation of de-identification was received or the date by which they must be returned, disposed of or de-identified.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
Policy 16. **2011 Manual: Policy and Procedures for the Execution of Data Sharing Agreements** **2024 Manual: Policy, Procedures and Practices for the Execution of Data Sharing Agreements**	• Must be developed and implemented to identify the circumstances requiring the execution of a data sharing agreement and the process that must be followed and the requirements that must be satisfied prior to the execution of a data sharing agreement.	• A policy, procedures and practices must be developed and implemented to identify the: o Circumstances requiring the execution of a data sharing agreement; o Process that must be followed when executing a data sharing agreement; and o Requirements that must be satisfied prior to the execution of a data sharing agreement.
	• Must set out the circumstances requiring the execution of a data sharing agreement prior to the collection of personal health information for purposes other than research and must require the execution of a data sharing agreement prior to any disclosure of personal health information for purposes other than research.	• The policy, procedures and practices must set out the circumstances requiring the execution of a data sharing agreement prior to the collection of personal health information for purposes other than research. • The policy, procedures and practices must require the execution of a data sharing agreement prior to any disclosure of personal health information for purposes other than research.
	• Must identify the agent(s) responsible for ensuring that a data sharing agreement is executed, as well as the process that must be followed and the requirements that must be satisfied in this regard. This must include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must identify the agent(s) responsible for ensuring that a data sharing agreement is executed; and • The policy, procedures and practices must set out the process that must be followed and the requirements that must be satisfied, which, at a minimum, must set out the: o Documentation that must be completed, provided and/or executed; o Agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; o Agent(s) to whom the documentation must be provided; and o Required content of the documentation.
	• In relation to the disclosure of personal health information for purposes other than research, the agent(s) responsible for ensuring that a data sharing agreement is executed must be satisfied that the disclosure was approved in accordance with the *Policy and Procedures for Disclosure of Personal Health Information For Purposes Other Than Research*.	• In relation to the disclosure of personal health information for purposes other than research, the agent(s) responsible for ensuring that a data sharing agreement is executed must be satisfied that the disclosure was approved in accordance with the *Policy, Procedures and Practices for Disclosure of Personal Health Information For Purposes Other Than Research*.
	• In relation to the collection of personal health information for purposes other than research, the agent(s) responsible for ensuring that a data sharing agreement is executed must be satisfied that the collection was approved in accordance with the *Policy and Procedures for the Collection of Personal Health Information.*	• In relation to the collection of personal health information for purposes other than research, the agent(s) responsible for ensuring that a data sharing agreement is executed must be satisfied that the collection was approved in accordance with the *Policy, Procedures and Practices for the Collection of Personal Health Information*.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must require that a log of data sharing agreements be maintained and must identify the agent(s) responsible for maintaining such a log.	• The policy, procedures and practices must require that a log of data sharing agreements be maintained; • The policy, procedures and practices must identify the agent(s) responsible for maintaining such a log;
	• It is recommended that the policy and procedures address where documentation related to the execution of data sharing agreements will be retained and the agent(s) responsible for retention.	• The policy, procedures and practices must address where documentation related to the execution of data sharing agreements will be retained. • The policy, procedures and practices must identify the agent(s) responsible for retention of executed data sharing agreements.
		<u>Compliance, Audit and Enforcement</u>
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	• The policy, procedures and practices must require agents to comply with the policy, procedures and practices; and • The policy, procedures and practices must address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*;
	• Must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	• The policy, procedures and practices must stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits*. • The policy, procedures and practices must identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices.
	• Must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedure.	• The policy, procedures and practices must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
Policy 17. **Template Data Sharing Agreement**	• A prescribed person or prescribed entity must ensure that a data sharing agreement is executed in the circumstances set out in the *Policy and Procedures for the Execution of Data Sharing Agreements* that, at a minimum, addresses the matters set out below.	• A prescribed person or prescribed entity must ensure that a data sharing agreement is executed in the circumstances set out in the *Policy, Procedures and Practices for the Execution of Data Sharing Agreements* that, at a minimum, addresses the matters set out below.
	<u>General Provisions</u>	<u>General Provisions</u>
	• Must describe the status of the prescribed person or prescribed entity under the Act and the duties and responsibilities arising from this status.	• The data sharing agreement must describe the status of the prescribed person or prescribed entity under PHIPA and the duties and responsibilities arising from this status.
	• Must specify the precise nature of the personal health information subject to the data sharing agreement.	• The data sharing agreement must specify the precise nature of the personal health information subject to the data sharing agreement. Where it is not reasonably possible for a prescribed person or prescribed entity to list or itemize every data element or variable, the prescribed person or prescribed entity may identify categories of data elements or variables.
	• Must provide a definition of personal health information that is consistent with the Act and its regulation.	• The data sharing agreement must provide a definition of personal health information that is consistent with PHIPA and its regulations.
	• Shall identify the person or organization that is collecting personal health information and the person or organization that is disclosing personal health information pursuant to the data sharing agreement.	• The data sharing agreement must identify the person or organization that is collecting personal health information or disclosing personal health information pursuant to the data sharing agreement.
	<u>Purposes of Collection, Use and Disclosure</u>	<u>Purposes of Collection, Use and Disclosure</u>
	• Must identify the purposes for which the personal health information subject to the data sharing agreement is being collected and for which the personal health information will be used.	• The data sharing agreement must identify the purposes for which the personal health information subject to the data sharing agreement is being collected and for which purposes the personal health information will be used.
	• In identifying these purposes, the data sharing agreement must explicitly state whether or not the personal health information collected pursuant to the data sharing agreement will be linked to other information. If the personal health information will be linked to other information, the data sharing agreement must identify the nature of the information to which the personal health information will be linked, the source of the information to which the personal health information will be linked, how the linkage will be conducted and why the linkage is required for the identified purposes.	• In identifying these purposes, the data sharing agreement must explicitly state whether or not the personal health information collected pursuant to the data sharing agreement will be linked to other information. If the personal health information will be linked to other information, the data sharing agreement must identify and describe: ○ The nature of the information to which the personal health information will be linked;

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		○ The source of the information to which the personal health information will be linked; ○ How the linkage will be conducted; and ○ Why the linkage is required for the identified purpose(s).
	• Must contain an acknowledgement that the personal health information collected pursuant to the data sharing agreement is necessary for the purpose for which it was collected and that other information, namely de-identified and/or aggregate information, will not serve the purpose and that no more personal health information is being collected and will be used than is reasonably necessary to meet the purpose.	• The data sharing agreement must contain an acknowledgement that: ○ The personal health information collected pursuant to the data sharing agreement is necessary for the purpose for which it was collected; ○ Other information, namely de-identified and/or aggregate information, will not serve the purpose; and ○ No more personal health information is being collected and will be used than is reasonably necessary to meet the purpose.
	• Must identify the purposes, if any, for which the personal health information subject to the data sharing agreement may be disclosed and any limitations, conditions or restrictions imposed thereon.	• The data sharing agreement must identify the purposes, if any, for which the personal health information subject to the data sharing agreement may be further disclosed and any limitations, conditions or restrictions imposed thereon.
	• Must require the collection, use and disclosure of personal health information subject to the data sharing agreement to comply with the *Act* and its regulation and must set out the specific statutory authority for each collection, use and disclosure contemplated in the data sharing agreement.	• The data sharing agreement must require the collection, use and disclosure of personal health information subject to the data sharing agreement to comply with PHIPA and its regulations. • The data sharing agreement must set out the specific statutory authority for each collection, use and disclosure contemplated in the data sharing agreement.
		• The data sharing agreement must set out any restrictions with respect to small cell-sizes (e.g. less than five), having regard to the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation* implemented by the prescribed person or prescribed entity.
	<u>Secure Transfer</u>	<u>Secure Transfer of Records of Personal Health Information</u>
	• Must require the secure transfer of the records of personal health information subject to the data sharing agreement.	• The data sharing agreement must require the secure transfer of the records of personal health information subject to the data sharing agreement.
	• Must set out the secure manner in which the records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that must be followed in ensuring that the records are transferred in a secure manner.	• The data sharing agreement must set out the secure manner in which the records of personal health information will be transferred, including under what conditions and to whom the records will be transferred; and

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		• The data sharing agreement must set out the procedure that must be followed in ensuring that the records are transferred in a secure manner.
	• In identifying the secure manner in which the records of personal health information will be transferred, regard may be had to the *Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.	• In identifying the secure manner in which the records of personal health information will be transferred, regard should be had to the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.
	<u>Secure Retention</u>	<u>Secure Retention of Records of Personal Health Information</u>
	• Must identify the retention period for the records of personal health information subject to the data sharing agreement. In identifying the relevant retention period, it must be ensured that the records of personal health information are retained only for as long as necessary to fulfill the purposes for which the records of personal health information were collected.	• The data sharing agreement must specify the retention period for the records of personal health information subject to the data sharing agreement. In identifying the relevant retention period, the records of personal health information must be retained only for as long as necessary to fulfill the purposes for which the records of personal health information were collected.
	• Must require the records of personal health information to be retained in a secure manner and shall identify the precise manner in which the records of personal health information in paper and electronic format will be securely retained, including whether the records will be retained in identifiable form.	• The data sharing agreement must require the records of personal health information to be retained in a secure manner; and • The data sharing agreement must specify the manner in which the records of personal health information in paper and electronic format will be securely retained, including whether the records will be retained in identifiable form.
	• In identifying the secure manner in which the records of personal health information will be retained, the data sharing agreement may have regard to the *Policy and Procedures for Secure Retention of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.	• In identifying the secure manner in which the records of personal health information will be retained, the data sharing agreement should have regard to the *Policy, Procedures and Practices for Secure Retention of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.
	• Must require reasonable steps to be taken to ensure that the personal health information subject to the data sharing agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be taken shall also be detailed in the data sharing agreement.	• The data sharing agreement must require reasonable steps to be taken to ensure that the records of personal health information subject to the data sharing agreement are protected against: o Theft, loss and unauthorized collection, use or disclosure; and o Unauthorized copying, modification or disposal; and o The data sharing agreement must detail the reasonable steps that are required to be taken.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	<u>Secure Return or Disposal</u>	
	• Must address whether the records of personal health information subject to the data sharing agreement will be returned in a secure manner or will be disposed of in a secure manner following the retention period set out in the data sharing agreement or following the date of termination of the data sharing agreement, as the case may be.	• The data sharing agreement must address whether the records of personal health information subject to the data sharing agreement will be returned or disposed of in a secure manner following the: o Retention period set out in the data sharing agreement; or o Date of termination of the data sharing agreement, as the case may be.
		<u>Secure Return of Records of Personal Health Information</u>
	• If the records of personal health information are required to be returned in a secure manner, the data sharing agreement must stipulate the time frame following the retention period or following the date of termination of the data sharing agreement within which the records of personal health information must be securely returned, the secure manner in which the records must be returned and the person to whom the records must be securely returned.	• If the records of personal health information are required to be returned in a secure manner, the data sharing agreement must stipulate the: o Timeframe following the retention period or following the date of termination of the data sharing agreement within which the records of personal health information must be securely returned; and o Agent to whom the records must be securely returned.
	• In identifying the secure manner in which the records of personal health information will be returned, regard may be had to the *Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.	• Secure manner in which the records must be returned, having regard to the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.
	• If the records of personal health information are required to be disposed of in a secure manner, the data sharing agreement must provide a definition of secure disposal that is consistent with the *Act* and its regulation and must identify the precise manner in which the records of personal health information subject to the data sharing agreement must be securely disposed of.	• If the records of personal health information are required to be disposed of in a secure manner, the data sharing agreement must: o Provide a definition of secure disposal that is consistent with PHIPA and its regulations; o Specify the manner in which the records of personal health information subject to the data sharing agreement must be securely disposed of;
	• Must stipulate the time frame following the retention period or following the date of termination of the data sharing agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided.	• The data sharing agreement must stipulate the timeframe following the retention period or following the date of termination of the data sharing agreement within which the records of personal health information must be securely disposed of; and • The data sharing agreement must specify the timeframe within which a certificate of destruction must be provided.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• In identifying the secure manner in which the records of personal health information will be disposed of, it must be ensured that the method of secure disposal identified is consistent with the *Act* and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including *Fact Sheet 10: Secure Destruction of Personal Information*. In addition, regard may be had to the *Policy and Procedures for Secure Disposal of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.	• In identifying the secure manner in which the records of personal health information will be disposed of, the method of secure disposal identified must at a minimum be consistent with: o PHIPA and its regulations; o Orders and decisions issued by the Information and Privacy Commissioner of Ontario under PHIPA and its regulations, including Order HO-001 and Order HO-006; o Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to PHIPA and its regulations, including Fact Sheet 10: Secure Destruction of Personal Information; and o The *Policy, Procedures and Practices for Secure Disposal of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.
	• Must identify the person to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided and the required content of the certificate of destruction.	• The data sharing agreement must identify the person to whom the certificate of destruction must be provided; o The data sharing agreement must identify the timeframe following secure disposal within which the certificate of destruction must be provided; and o The data sharing agreement must identify the required content of the certificate of destruction.
	• The certificate of destruction must be required to identify the records of personal health information securely disposed of; to stipulate the date, time, location and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.	• A certificate that evidences the destruction of records of personal health information must, at a minimum: o Identify the records of personal health information securely disposed of; o Stipulate the date, time, location and method of secure disposal employed; and o Bear the name and signature of the person who performed the secure disposal.
	<u>Notification</u>	<u>Breach Notification to prescribed person or prescribed entity</u>
	• Must require that notification be provided at the first reasonable opportunity if the data sharing agreement has been breached or is suspected to have been breached or if the personal health information subject to the data sharing agreement is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons.	• The data sharing agreement must require that notification be provided at the first reasonable opportunity if: o The data sharing agreement has been breached or is suspected to have been breached; or

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		○ The personal health information subject to the data sharing agreement is stolen, lost or collected, used or disclosed without authority or is believed to have been stolen, lost or collected, used or disclosed without authority.
	• Should identify whether the notification must be verbal and/or in writing and to whom the notification must be provided.	• The data sharing agreement should also identify whether the notification of breach must be oral and/or in writing and to whom the notification must be provided.
	• Must require that reasonable steps be taken to contain the breach of the data sharing agreement and to contain the theft, loss or access by unauthorized persons.	• The data sharing agreement must also require that reasonable steps be taken to contain the breach.
	<u>Consequences of Breach and Monitoring Compliance</u>	<u>Consequences of Breach and Monitoring Compliance</u>
		• The data sharing agreement must provide the prescribed person or prescribed entity with the right to audit compliance with the agreement.
	• Must outline the consequences of breach of the agreement and must indicate whether compliance with the data sharing agreement will be audited and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.	• The data sharing agreement must outline the consequences of breach of the agreement. • The data sharing agreement set out the manner and circumstances in which compliance will be audited and the notice, if any, that will be provided of the audit.
	• Must require that all persons who will have access to the personal health information are aware of and agree to comply with the terms and conditions of the data sharing agreement prior to being given access to the personal health information.	• The data sharing agreement must require that all persons who will have access to the personal health information are aware of and agree to comply with the terms and conditions of the data sharing agreement prior to being given access to the personal health information.
	• Must set out the method by which this will be ensured. This may include requiring the persons that will have access to the personal health information to sign an acknowledgement, prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the data sharing agreement.	• The data sharing agreement must set out the method by which this will be ensured. This may include requiring the persons who will have access to the personal health information to sign an acknowledgement, prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the data sharing agreement.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
Policy 18. **Log of Data Sharing Agreements**	• A prescribed person or prescribed entity must maintain a log of executed data sharing agreements. At a minimum, the log must include:	• A prescribed person or prescribed entity must maintain a log of executed data sharing agreements. At a minimum, the log must include:
	• The name of the person or organization from whom the personal health information was collected or to whom the personal health information was disclosed;	• The name of the person or organization from whom the personal health information was collected or to whom the personal health information was disclosed;
	• The date that the collection or disclosure of personal health information was approved, as the case may be;	• The date that the collection or disclosure of personal health information was approved, as the case may be;
	• The date that the data sharing agreement was executed;	• The date that the data sharing agreement was executed;
	• The date the personal health information was collected or disclosed, as the case may be;	• The date the personal health information was collected or disclosed, as the case may be;
	• The nature of the personal health information subject to the data sharing agreement;	• The nature of the personal health information subject to the data sharing agreement;
	• The retention period for the records of personal health information set out in the data sharing agreement or the date of termination of the data sharing agreement;	• The retention period for the records of personal health information set out in the data sharing agreement or the date of termination of the data sharing agreement;
	• Whether the records of personal health information will be securely returned or will be securely disposed of following the retention period set out in the data sharing agreement or the date of termination of the data sharing agreement; and	• Whether the records of personal health information will be securely returned or will be securely disposed of following the retention period set out in the data sharing agreement or the date of termination of the data sharing agreement; and
	• The date the records of personal health information were securely returned or a certificate of destruction was provided or the date by which they must be returned or disposed of.	• The date the records of personal health information were securely returned or a certificate of destruction was provided or the timeframes by which they must be returned or disposed of.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Third Party Service Agreements
Policy 19. **2011 Manual: Policy and Procedures for Executing Agreements with Third Party Service Providers in Respect of Personal Health Information** **2024 Manual: Policy, Procedures and Practices for Executing Agreements with Third Party Service Providers in Respect of Personal Health Information**	• Must be developed and implemented requiring written agreements to be entered into with third party service providers prior to permitting third party service providers to access and use the personal health information of the prescribed person or prescribed entity.	• A policy, procedures and practices for executing agreements with third party service providers must require written agreements to be entered into with third party service providers contracted or otherwise engaged to provide services to the prescribed person or prescribed entity prior to permitting third party service providers to access and use the personal health information of the prescribed person or prescribed entity.
	• Must require the written agreements to contain the relevant language from the *Template Agreement for Third Party Service Providers.*	• A policy, procedures and practices for executing agreements with third party service providers must require the written agreements to contain the relevant language from the *Template Agreement for Third Party Service Providers*; and
	• Must identify the agent(s) responsible for ensuring that an agreement is executed, as well as the process that must be followed and the requirements that must be satisfied prior to the execution of such an agreement.	• A policy, procedures and practices for executing agreements with third party service providers must identify the agent(s) responsible for ensuring that an agreement is executed, as well as the process that must be followed and the requirements that must be satisfied prior to the execution of a third party service provider Agreement.
		Limitations on Access to and Use of Personal Health Information
	• Must state that the prescribed person or prescribed entity shall not provide personal health information to a third party service provider if other information, namely de-identified and/or aggregate information, will serve the purpose and will not provide more personal health information than is reasonably necessary to meet the purpose. • Must identify the agent responsible for making this determination.	• The policy, procedures and practices with respect to third party service provider agreements must require the prescribed person or prescribed entity to: o Prohibit a third party service provider from accessing or using personal health information if other information, namely de-identified and/or aggregate information, will serve the purpose or from accessing or using more personal health information to be accessed or used than is reasonably necessary to meet the purpose; o Must require the prescribed person or prescribed entity to identify the agent responsible for making this determination; o Ensure that third party service providers agree to comply with the restrictions and conditions that are necessary to enable the prescribed person or prescribed entity to comply with PHIPA and its regulations. This includes prohibiting third party service providers from accessing or using the personal health information of the prescribed person or prescribed entity unless the third party service provider is permitted to do so in the third party service provider agreement and agrees to comply with the restrictions that apply to the prescribed person or prescribed entity;

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		○ Outline the process to be followed by the prescribed entity or prescribed person in auditing the third party service provider'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 third party service provider of the audit; and ○ Outline the consequences of breach of the agreement.
		<u>Vulnerability Management Practices</u>
		• The policy, procedures and practices should ensure that third party service providers have vulnerability management practices that meet a standard of protection that is at least equivalent to that of the prescribed person or prescribed entity, in accordance with the *Policy, Procedures and Practices for Vulnerability and Patch Management*.
		<u>Secure Transfer, Retention, Back-Up and Disposal</u>
		The policy, procedures and practices must also: • Identify any purposes for which and circumstances in which records of personal health information of the prescribed person or prescribed entity may be transferred to third party service providers, including for secure retention or secure disposal; and • Detail the procedure to be followed in securely transferring records of personal health information to the third party service provider and in securely retrieving records from the third party service provider, including the: ○ Secure manner in which the records will be transferred and retrieved; ○ Conditions pursuant to which the records will be transferred and retrieved; ○ Agent(s) responsible for ensuring the secure transfer and retrieval of the records; and ○ Require the records to be transferred in a secure manner in compliance with the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information*.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must identify the agent(s) responsible for ensuring that records of personal health information provided to a third party service provider are either securely returned to the prescribed person or prescribed entity or are securely disposed of, as the case may be, following the termination of the agreement.	• A policy, procedures and practices must address the documentation that is required to be maintained in relation to the transfer of records of personal health information to a third party service provider for secure retention and/or secure disposal. In particular, the policy, procedures and practices must require: o The agent(s) responsible for ensuring the secure transfer to document the date, time, mode of transfer and whether the records are transferred for secure retention and/or secure disposal; o The maintenance of a repository of written confirmations received from the third party service provider upon receipt of the records of personal health information; o A detailed inventory to be maintained of records of personal health information being securely retained by the third party service provider and of records of personal health information retrieved by the prescribed person or prescribed entity; and o The identification of the agent(s) responsible for maintaining the detailed inventory.
	• Must address the process to be followed where records of personal health information are not securely returned or a certificate of destruction is not received following the termination of the agreement, including the agent(s) responsible for implementing this process and the time frame following termination within which this process must be implemented.	The policy, procedures and practices must: • Outline the procedure to be followed in tracking the dates that certificates of destruction are received from the third party service provider and the agent(s) responsible for conducting such tracking; • Set out the process to be followed where a certificate of destruction is not received within the time set out in the agreement with the third party service provider; • Identify the agent(s) responsible for implementing the procedure and processes related to certificates of destruction; and • Set out the process to be followed where records of personal health information are not securely returned or a certificate of destruction is not received following the termination of the agreement, including: o The agent(s) responsible for implementing this process; o The timeframe following termination of the agreement within which this process must be implemented; and

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		○ The agent(s) responsible for ensuring that records of personal health information provided to a third party service provider are either securely returned to the prescribed person or prescribed entity or are securely disposed of, as the case may be, following the termination of the agreement.
		• Where a third party service provider is contracted to securely retain or securely dispose of records of personal health information of the prescribed person or prescribed entity, the policy, procedures and practices must further: ○ Require that a written agreement be executed with the third party service provider containing the relevant language from the *Template Agreement for Third Party Service Providers*; and ○ Identify the agent(s) responsible for ensuring that the third party service provider agreement has been executed prior to transferring the records of personal health information for secure retention and/or secure disposal. • These requirements apply where a third party service provider is contracted to retain backed-up records of personal health information of the prescribed person or prescribed entity, or where a third party service provider backs-up records of personal health information of the prescribed person or prescribed entity it has been contracted to retain, regardless of whether the third party service provider uses remote-based (cloud) systems or on-premise systems.
		<u>Tracking Agreements</u>
	• Must require that a log be maintained of all agreements executed with third party service providers and must identify the agent(s) responsible for maintaining such a log. • It is recommended that the policy and procedures address where documentation related to the execution of agreements with third party service providers will be retained and the agent(s) responsible for retaining this documentation.	• The policy, procedures and practices must require that a log be maintained of all third party service provider agreements executed with third party service providers who are permitted to access or use personal health information. • The policy, procedures and practices must further: ○ Identify the agent(s) responsible for maintaining such a log and for tracking the third party service provider Agreements; ○ Outline the process to be followed in tracking all third party service providers who are permitted to access or use personal health information which includes setting out the documentation that must be completed, provided and/or executed to verify that the agreements have been executed, including the: ○ Agent(s) responsible for completing, providing, executing and ensuring the execution of the documentation;

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		○ Agent(s) to whom this documentation must be provided; ○ Required content of the documentation; ○ Outline the process to be followed and the agent(s) responsible for identifying third party service providers who have not executed the agreement and for ensuring that these third party service providers do so, within a set timeframe; ○ Indicate where documentation related to the execution of third party service provider agreements will be retained; and ○ Identify the agent(s) responsible for retaining this documentation.
		<u>Compliance, Audit and Enforcement</u>
	• The prescribed person or prescribed entity must also require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. • Must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures. • Must stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Privacy Audits, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	The policy, procedures and practices must: • Require agents to comply with the policy, procedures and practices; • Require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices; • Identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; • Address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and, • Stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits*.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
Policy 20. **2011 Manual: Template Agreement for All Third Party Service Providers** **2024 Manual: Template Agreement for Third Party Service Providers**	• A written agreement must be entered into with third party service providers that will be permitted to access and use personal health information of the prescribed person or prescribed entity, including those that are contracted to retain, transfer or dispose of records of personal health information and those that are contracted to provide services for the purpose of enabling the prescribed person or prescribed entity to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information ("electronic service providers").	• A written third party service provider agreement must be entered into with third party service providers that will be permitted to access and use personal health information of the prescribed person or prescribed entity. This includes third party service providers contracted or otherwise engaged to retain, transfer or dispose of records of personal health information or to provide services for the purpose of enabling the prescribed person or prescribed entity to use electronic means to collect, use, modify, disclose, retain, transfer or dispose of personal health information ("electronic service providers").
	<u>General Provisions</u>	<u>General Provisions</u>
	• Must describe the status of the prescribed person or prescribed entity under the *Act* and the duties and responsibilities arising from this status.	• The third party service provider agreement must describe the status of the prescribed person or prescribed entity under PHIPA and the duties and responsibilities arising from this status.
	• Must state whether or not the third party service provider is an agent of the prescribed person or prescribed entity in providing services pursuant to the agreement.	• The third party service provider agreement must state whether or not the third party service provider is an agent of the prescribed person or prescribed entity in providing services pursuant to the agreement.
	• All third party service providers that are permitted to access and use personal health information in the course of providing services to the prescribed person or prescribed entity shall be considered agents of the prescribed entity or prescribed person, with the possible exception of electronic service providers.	• All third party service providers that are permitted to access and use personal health information in the course of providing services to the prescribed person or prescribed entity must be considered agents of the prescribed person or prescribed entity, with the possible exception of electronic service providers.
	• Agreements with electronic service providers must explicitly state whether or not the third party service provider is an agent of the prescribed person or prescribed entity in providing services pursuant to the agreement.	• Agreements with electronic service providers must explicitly state whether or not the third party service provider is also an agent of the prescribed person or prescribed entity in providing services pursuant to the agreement.
	• If the third party service provider is an agent of the prescribed person or prescribed entity, the agreement must require the third party service provider to comply with the provisions of the *Act* and its regulation relating to prescribed persons or prescribed entities, as the case may be, and to comply with the privacy and security policies and procedures implemented by the prescribed person or prescribed entity in providing services pursuant to the agreement.	• If the third party service provider is an agent of the prescribed person or prescribed entity, the third party service provider Agreement must require the third party service provider to comply with the provisions of PHIPA and its regulations relating to prescribed persons or prescribed entities, as the case may be, and to comply with the privacy and information security policies, procedures and practices implemented by the prescribed person or prescribed entity in providing services pursuant to the agreement.
	• It is recommended that the agreement provide a definition of personal health information and that the definition provided be consistent with the *Act* and its regulation.	• The third party service provider agreement should provide a definition of personal health information consistent with PHIPA and its regulations.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Where appropriate, the agreement should specify the precise nature of the personal health information that the third party service provider will be permitted to access and use in the course of providing services pursuant to the agreement.	• Where appropriate, the third party service provider agreement should also specify the precise nature of the personal health information that the third party service provider will be permitted to access and use in the course of providing services pursuant to the agreement.
	• Must require that the services provided by the third party service provider pursuant to the agreement be performed in a professional manner, in accordance with industry standards and practices, and by properly trained agents of the third party service provider.	• The third party service provider agreement must require that the services provided by the third party service provider pursuant to the agreement be performed in a professional manner, in accordance with evolving industry privacy and information security standards and best practices, and by properly trained agents of the third party service provider.
	<u>Obligations with Respect to Access and Use</u>	<u>Obligations with Respect to Access and Use</u>
	• Must identify the purposes for which the third party service provider is permitted to access and use the personal health information of the prescribed person or prescribed entity and any limitations, conditions or restrictions imposed thereon.	• The third party service provider agreement must identify the limited and narrowly defined purposes for which the third party service provider is permitted to access and use the personal health information of the prescribed person or prescribed entity and any limitations, conditions or restrictions imposed thereon, including where a third party service provider is not an agent of the prescribed person or prescribed entity (i.e. a third party service provider who acts solely as an electronic service provider).
	• In identifying the purposes for which the third party service provider is permitted to use personal health information, the prescribed person or prescribed entity must ensure that each use identified in the agreement is consistent with the uses of personal health information permitted by the *Act* and its regulation.	
	• Must prohibit the third party service provider from using personal health information except as permitted in the agreement. • Must prohibit the third party service provider from using personal health information if other information will serve the purpose and from using more personal health information than is reasonably necessary to meet the purpose.	• In the case of a third party service provider that is also an agent of the prescribed person or prescribed entity, the third party service provider Agreement must further: o Prohibit the third party service provider from using personal health information if other information, such as de-identified and/or aggregate information, will serve the purposes identified in the agreement; o Prohibit the use of more personal health information than is reasonably necessary to meet the purposes identified in the agreement; and o Identify one or more use(s) that is / are consistent with the uses of personal health information permitted by PHIPA and its regulations or another law.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• In the case of an electronic service provider that is not an agent of the prescribed person or prescribed entity, the agreement must explicitly prohibit the electronic service provider from using personal health information except as necessary in the course of providing services pursuant to the agreement.	• In the case of a third party service provider that is not an agent of the prescribed person or prescribed entity, the third party service provider agreement must prohibit third party service providers from using personal health information except: o As permitted in the third party service provider agreement; o For the purposes for which the prescribed person or prescribed entity is permitted to use personal health information under PHIPA and its regulations; and o As necessary in the course of providing services pursuant to the agreement or as required by law.
	<u>Obligations with Respect to Disclosure</u>	<u>Obligations with Respect to Disclosure</u>
	• Must identify the purposes, if any, for which the third party service provider is permitted to disclose the personal health information of the prescribed entity or prescribed person and any limitations, conditions or restrictions imposed thereon.	• The third party service agreement must identify the purposes, if any, for which the third party service provider is permitted to disclose the personal health information of the prescribed person or prescribed entity and any limitations, conditions or restrictions imposed thereon.
	• In identifying the purposes for which the third party service provider is permitted to disclose personal health information, the prescribed person or prescribed entity must ensure that each disclosure identified in the agreement is consistent with the disclosures of personal health information permitted by the *Act* and its regulation.	• In identifying the limited and narrowly defined purposes for which the third party service provider is permitted to disclose personal health information, the prescribed person or prescribed entity must ensure that each disclosure identified in the third party service provider Agreement is consistent with, and reasonably necessary for, the disclosures of personal health information permitted by PHIPA and its regulations and is not contrary to PHIPA, its regulations or another law.
	• In this regard, the agreement must prohibit the third party service provider from disclosing personal health information except as permitted in the agreement or as required by law, from disclosing personal health information if other information will serve the purpose and from disclosing more personal health information than is reasonably necessary to meet the purpose.	• In the case of a third party service provider that is also an agent of the prescribed person or prescribed entity, the third party service provider agreement must further prohibit the third party service provider from disclosing personal health information: o Except as permitted in the third party service provider agreement; o Except for the purposes for which the prescribed person or prescribed entity is permitted to disclose personal health information under PHIPA and its regulations; o If other information will serve the purposes identified in the third party service provider agreement; and o If the disclosure includes more personal health information than is reasonably necessary to meet the purposes identified in the agreement.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• In the case of an electronic service provider that is not an agent of the prescribed entity or prescribed person, the agreement must prohibit the electronic service provider from disclosing personal health information to which it has access in the course of providing services except as required by law.	• In the case of a third party service provider that is not an agent of the prescribed person or prescribed entity (i.e., a third party service provider who acts solely as an electronic service provider), the third party service provider agreement must prohibit the third party service provider from disclosing personal health information to which it has access in the course of providing services except as required by law.
	<u>Secure Transfer</u>	<u>Secure Transfer</u>
		• The third party service provider agreement must identify the purposes for which and the circumstances in which records of personal health information of the prescribed person or prescribed entity may be transferred to the third party service provider and transferred from the third party service provider back to the prescribed person or prescribed entity, if any.
	• Where it is necessary to transfer records of personal health information to or from the prescribed person or prescribed entity, the agreement must require the third party service provider to securely transfer the records of personal health information and must set out the responsibilities of the third party service provider in this regard.	• Where it is necessary to transfer records of personal health information to or from the prescribed person or prescribed entity, the third party service provider Agreement must require the third party service provider and the prescribed person or prescribed entity to transfer the records of personal health information in a secure manner and must set out the responsibilities of the third party service provider and prescribed person or prescribed entity in this regard.
	• Must specify the secure manner in which the records will be transferred by the third party service provider, the conditions pursuant to which the records will be transferred by the third party service provider, to whom the records will be transferred and the procedure that must be followed by the third party service provider in ensuring that the records are transferred in a secure manner.	• The third party service provider agreement: o Must specify the secure manner in which the records will be transferred; o Must specify the conditions pursuant to which the records will be transferred; o Must specify to whom the records will be transferred; and o Must specify the procedure that must be followed in ensuring that the records are transferred in a secure manner.
	• In identifying the secure manner in which records of personal health information must be transferred, the agreement shall have regard to the *Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.	• In identifying the secure manner in which records of personal health information must be transferred, the third party service provider agreement must have regard to the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Where the retention of records of personal health information or where the disposal of records of personal health information outside the premises of the prescribed person or prescribed entity is the primary service provided to the prescribed person or prescribed entity, the agreement must require the third party service provider to provide documentation to the prescribed person or prescribed entity setting out the date, time and mode of transfer of the records of personal health information and confirming receipt of the records of personal health information by the third party service provider.	• Where the retention or disposal of records of personal health information outside the premises of the prescribed person or prescribed entity is the primary service provided to the prescribed person or prescribed entity, the third party service provider Agreement must require the third party service provider to provide documentation to the prescribed person or prescribed entity setting out the date, time and mode of transfer of the records of personal health information and confirming receipt.
	• In these circumstances, the agreement must also obligate the third party service provider to maintain a detailed inventory of the records of personal health information transferred.	• In these circumstances, the third party service provider agreement must also obligate the third party service provider to maintain a detailed inventory of the records of personal health information transferred.
	<u>Secure Retention</u>	<u>Secure Retention and Back-Up</u>
	• Must require the third party service provider to retain the records of personal health information, where applicable, in a secure manner and shall identify the precise methods by which records of personal health information in paper and electronic format will be securely retained by the third party service provider, including records of personal health information retained on various media.	• Where the third party is contracted to retain records of personal health information on behalf of the prescribed person or the prescribed entity, the third party service provider agreement must require the third party service provider to do so in a secure manner and must identify the precise methods by which records of personal health information will be securely retained by the third party service provider, including records in both paper and electronic format retained on various media.
	• Must further outline the responsibilities of the third party service provider in securely retaining the records of personal health information.	• The third party service provider agreement must further outline the responsibilities of the third party service provider in securely retaining the records of personal health information having regard to the *Policy, Procedures and Practices for Secure Retention of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• In identifying the secure manner in which the records of personal health information will be retained, and the methods by which the records of personal health information will be securely retained, the agreement shall have regard to the *Policy and Procedures for Secure Retention of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.	• The third party service provider 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 prescribed person or prescribed entity. • In identifying the secure manner by which the records of personal health information will be securely backed-up and retained, the agreement must: o Identify the precise methods by which the records will be securely backed-up and retained by the third party service provider, including records in both paper and electronic format retained on various media; and o Set out the responsibilities of the third party service provider in securely backing-up and retaining the records.
	• Where the retention of records of personal health information is the primary service provided to the prescribed person or prescribed entity by the third party service provider, the agreement must obligate the third party service provider to maintain a detailed inventory of the records of personal health information being retained on behalf of the prescribed person or prescribed entity as well as a method to track the records being retained.	• Where the retention of records of personal health information or backed-up records of personal health information is the primary service provided by the third party service provider, the third party service provider Agreement must require the third party service provider to: o Maintain a detailed inventory of the records of personal health information or backed-up records of personal health information being retained on behalf of the prescribed person or prescribed entity; and o A method to track the records being retained.
		• Where a third party service provider is contracted to retain records of personal health information or backed-up records of personal health information, or where a third party service provider backs up records of personal health information it has been contracted to retain, the third party service provider agreement must set out the circumstances in which the third party service provider is required to make such records available to the prescribed person or prescribed entity. In regard to the circumstances in which backed-up records of personal health information are required to be made available, the agreement must be in compliance with the *Policy, Procedures and Practices for Back-Up and Recovery of Records of Personal Health Information*. • The above requirements apply regardless of whether the third party service provider uses remote-based (cloud) systems or on-premise systems.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Secure Return or Disposal Following Termination of the Agreement	Secure Return or Disposal of Records of Personal Health Information
	• Must address, where applicable, whether records of personal health information will be securely returned to the prescribed person or prescribed entity or will be disposed of in a secure manner following the termination of the agreement.	• Where the third party service provider agreement provides that records of personal health information of the prescribed person or prescribed entity may be transferred to the third party service provider, the third party service provider agreement must address whether records of personal health information will be securely returned to the prescribed person or prescribed entity or will be disposed of in a secure manner following termination of the agreement. • The third party service provider agreement must require that records of personal health information of the prescribed person or prescribed entity transferred to the third party service provider be securely returned or disposed of in a secure manner following the termination of the agreement.
	• If the records of personal health information are required to be returned in a secure manner, the agreement must stipulate the time frame following the date of termination of the agreement within which the records of personal health information must be securely returned, the secure manner in which the records must be returned and the agent of the prescribed person or prescribed entity to whom the records must be securely returned.	• If the records of personal health information are required to be returned in a secure manner, the third party service provider agreement must stipulate the: o Timeframe within which the records of personal health information must be securely returned; o Secure manner in which the records must be returned; and o Agent of the prescribed person or prescribed entity to whom the records must be securely returned.
	• In identifying the secure manner in which the records of personal health information will be returned, the agreement must have regard to the *Policy and Procedures for Secure* Transfer *of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.	• In identifying the secure manner in which the records of personal health information will be returned, the third party service provider agreement must have regard to the *Policy, Procedures and Practices for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.
	• If the records of personal health information are required to be disposed of in a secure manner, the agreement must provide a definition of secure disposal that is consistent with the *Act* and its regulation and must identify the precise manner in which the records of personal health information are to be securely disposed of.	• If the records of personal health information are required to be disposed of in a secure manner, the third party service provider agreement must provide a definition of secure disposal that is consistent with PHIPA and its regulations.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• In identifying the secure manner in which the records of personal health information will be disposed of, it must be ensured that the method of secure disposal identified is consistent with the *Act* and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including *Fact Sheet 10: Secure Destruction of Personal Information*; and with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.	• At a minimum, the agreement must also identify the precise manner by which the records of personal health information are to be securely disposed of by the third party service provider, consistent with: o PHIPA and its regulations; o Orders and decisions issued by the Information and Privacy Commissioner of Ontario under PHIPA and its regulations, including Order HO-001 and Order HO-006; o Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to PHIPA and its regulations, including Fact Sheet 10: Secure Destruction of Personal Information; and o *The Policy, Procedures and Practices for Secure Disposal of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.
		Certificate of Destruction
	• Must stipulate the time frame following termination of the agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided to the prescribed person or prescribed entity. • Must identify the agent of the prescribed person or prescribed entity to whom the certificate of destruction must be provided and must identify the required content of the certificate of destruction. • The certificate of destruction must be required to identify the records of personal health information securely disposed of; to stipulate the date, time and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.	• The third party service provider agreement must identify the: o Agent of the prescribed person or prescribed entity to whom the certificate of destruction must be provided; o Timeframe following secure disposal within which the certificate of destruction must be provided; and o Required content of the certificate of destruction. • A certificate that evidences the destruction of records of personal health information must, at a minimum: o Identify the records of personal health information securely disposed of; o Stipulate the date, time and method of secure disposal employed; and o Bear the name and signature of the person who performed the secure disposal.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Secure Disposal as a Contracted Service	
	• Where the disposal of records of personal health information is the primary service provided to the prescribed person or prescribed entity by the third party service provider, in addition to the requirements set out above in relation to secure disposal, the agreement must further set out the responsibilities of the third party service provider in securely disposing of the records of personal health information, including: • The time frame within which the records are required to be securely disposed of; • The precise method by which records in paper and/or electronic format must be securely disposed of, including records retained on various media; • The conditions pursuant to which the records will be securely disposed of; and • The person(s) responsible for ensuring the secure disposal of the records. • Should enable the prescribed person or prescribed entity, at its discretion, to witness the secure disposal of the records of personal health information subject to such reasonable terms or conditions as may be required in the circumstances.	• The third party service provider agreement must also stipulate the responsibilities of the third party service provider in securely disposing of the records of personal health information, including the: ○ Conditions pursuant to which the records will be securely disposed of by the third party service provider; ○ Precise method by which records must be securely disposed of, including records retained on various media, in both paper and/or electronic format; and ○ Person(s) responsible for ensuring the secure disposal of the records.
	Implementation of Safeguards	Implementation of Safeguards
	• Must require the third party service provider to take steps that are reasonable in the circumstances to ensure that the personal health information accessed and used in the course of providing services pursuant to the agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information subject to the agreement are protected against unauthorized copying, modification or disposal.	• The third party service provider agreement must require the third party service provider to take steps that are reasonable in the circumstances to ensure that the records of personal health information subject to the agreement are accessed and used in the course of providing services pursuant to the agreement are protected against theft, loss and unauthorized collection, use or disclosure and protected against unauthorized copying, modification or disposal.
	• Must detail the reasonable steps that are required to be implemented by the third party service provider.	• The third party service provider agreement must detail the reasonable steps required to be implemented by the third party service provider having regard to the *Policy, Procedures and Practices for Secure Retention of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	<u>Training of Agents of the Third Party Service Provider</u>	<u>Training of Agents of the Third Party Service Provider</u>
	• Must require the third party service provider to provide training to its agents on the importance of protecting the privacy of individuals whose personal health information is accessed and used in the course of providing services pursuant to the agreement and on the consequences that may arise in the event of a breach of these obligations.	• The third party service provider agreement must require the third party service provider to provide training to its agents on the importance of protecting the privacy of individuals whose personal health information is accessed and used in the course of providing services pursuant to the agreement. • The third party service provider agreement must require the third party service provider to inform its agents of the consequences that may arise in the event of a breach of these obligations.
	• Must require the third party service provider to ensure that its agents who will have access to the records of personal health information are aware of and agree to comply with the terms and conditions of the agreement prior to being given access to the personal health information.	• The third party service provider agreement must require the third party service provider to ensure that its agents who will have access to the records of personal health information are aware of and agree to comply with the terms and conditions of the agreement prior to being given access to the personal health information.
	• Must set out the method by which this will be ensured. This may include requiring agents to sign an acknowledgement, prior to being granted access to the personal health information, indicating that they are aware of and agree to comply with the terms and conditions of the agreement.	• The third party service provider agreement must set out the method by which this will be ensured. This should include requiring agents of the third party service provider to sign an acknowledgement, prior to being granted access to the personal health information, indicating that they are aware of and agree to comply with the terms and conditions of the agreement.
	<u>Subcontracting of the Services</u>	
	• In the event that the agreement permits the third party service provider to subcontract the services provided under the agreement, the third party service provider must be required to acknowledge and agree that it will provide the prescribed person or prescribed entity with advance notice of its intention to do so, that the third party service provider will enter into a written agreement with the subcontractor on terms consistent with its obligations to the prescribed person or prescribed entity and that a copy of the written agreement will be provided to the prescribed person or prescribed entity.	• In the event that the third party service provider agreement permits the third party service provider to subcontract the services provided under the agreement, the third party service provider must be required to: o Acknowledge and agree that it will provide the prescribed person or prescribed entity with advance notice of its intention to do so; o Enter into a written agreement with the subcontractor on terms consistent with its obligations to the prescribed person or prescribed entity; and o Provide the prescribed person or prescribed entity with a right to obtain a copy of the written subcontracting agreement, upon request.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Notification	Breach Notification to Prescribed Person or Prescribed Entity
	• Must require the third party service provider to notify the prescribed person or prescribed entity at the first reasonable opportunity if there has been a breach or suspected breach of the agreement or if personal health information handled by the third party service provider on behalf of the prescribed person or prescribed entity is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons.	• The third party service provider agreement must require the third party service provider to notify the prescribed person or prescribed entity at the first reasonable opportunity if: o There has been a breach or suspected breach of the third party service provider Agreement; o Personal health information handled by the third party service provider on behalf of the prescribed person or prescribed entity is stolen, lost or collected, used or disclosed without authority; or o Personal health information handled by the third party service provider on behalf of the prescribed person or prescribed entity is believed to have been stolen, lost or collected, used or disclosed without authority.
	• Should identify whether the notification must be verbal, written or both and to whom the notification must be provided.	• The third party service provider agreement should also identify whether the notification must be oral, written or both and to whom the notification must be provided.
	• The third party service provider must be required to take steps that are reasonable in the circumstances to contain the breach and to contain the theft, loss or access by unauthorized persons.	• The third party service provider agreement must require the third party service provider to take steps that are reasonable in the circumstances to contain the breach, or to contain the theft, loss or any unauthorized collection, use or disclosure and collaborate with the prescribed person or prescribed entity in its investigation.
	Consequences of Breach and Monitoring Compliance	Consequences of Breach and Monitoring Compliance
	• Must outline the consequences of breach of the agreement and must indicate whether the prescribed person or prescribed entity will be auditing compliance with the agreement and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided to the third party service provider of the audit.	• The third party service provider agreement must provide the prescribed person or prescribed entity with the right to audit the third party service provider'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 third party service provider of the audit. The third party service provider Agreement should also allow the prescribed person or prescribed entity to request and obtain a copy of any independent audit of the third party service provider's privacy and information security policies, procedures and practices. • The third party service provider agreement must outline the consequences of breach of the agreement.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
Policy 21. **Log of Agreements with Third Privacy Service Providers**	• A prescribed person or prescribed entity must maintain a log of executed agreements with third party service providers. At a minimum, the log must include:	• A prescribed person or prescribed entity must maintain a log of executed agreements with third party service providers that are permitted to access and use personal health information. At a minimum, the log must include:
	• The name of the third party service provider;	• The name of the third party service provider;
	• The nature of the services provided by the third party service provider that require access to and use of personal health information;	• The nature of the services provided by the third party service provider that require access to and use of personal health information;
	• The date that the agreement with the third party service provider was executed;	• The date that the agreement with the third party service provider was executed;
	• The date that the records of personal health information or access to the records of personal health information, if any, was provided;	• The date that the records of personal health information or access to the records of personal health information, if any, was first provided;
	• The nature of the personal health information provided or to which access was provided;	• The nature of the personal health information provided or to which access was provided;
	• The date of termination of the agreement with the third party service provider;	• The date of termination of the agreement with the third party service provider;
		• Whether the records of personal health information were transferred to the third party service provider, and if so the nature of the records transferred;
	• Whether the records of personal health information, if any, will be securely returned or will be securely disposed of following the date of termination of the agreement; and	• Whether the records of personal health information, if any, will be securely returned or will be securely disposed of upon termination of the agreement; and
	• The date the records of personal health information were securely returned or a certificate of destruction was provided or the date that access to the personal health information was terminated or the date by which the records of personal health information must be returned or disposed of or access terminated.	• The date the records of personal health information were securely returned or a certificate of destruction was provided or the date that access to the personal health information was terminated or the date by which the records of personal health information must be returned or disposed of or access terminated.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Data Linkage, De-Identification and Aggregation
Policy 22. **2011 Manual: Policy and Procedures for the Linkage of Records of Personal Health Information** **2024 Manual: Policy, Procedures and Practices for the Linkage of Records of Personal Health Information**	• Must be developed and implemented with respect to linkages of records of personal health information.	• A policy, procedures and practices must be developed and implemented with respect to linkages of records of personal health information.
	• Must identify whether or not the prescribed person or prescribed entity permits the linkage of records of personal health information and if it is not permitted, the policy and procedures must expressly prohibit the linkage of records of personal health information. If the linkage of records of personal health information is permitted, the purposes for which and the circumstances in which such linkages are permitted must be identified.	• The policy, procedures and practices must identify whether or not the prescribed person or prescribed entity permits the linkage of records of personal health information and, if it is not permitted, the policy, procedures and practices must explicitly prohibit the linkage of records of personal health information. If the linkage of records of personal health information is permitted, the purposes for which and the circumstances in which such linkages are permitted must be identified.
	• In identifying the purposes for which and the circumstances in which the linkage of records of personal health information is permitted, regard must be had to the sources of the records of personal health information that are requested to be linked and the identity of the person or organization that will ultimately make use of the linked records of personal health information, including:	• In identifying the purposes for which and the circumstances in which the linkage of records of personal health information is permitted, regard must be had to the sources of the records of personal health information that are requested to be linked and the identity of the person or organization that will ultimately make use of the linked records of personal health information, including where the linkage of records of personal health information is:
	• The linkage of records of personal health information solely in the custody of the prescribed person or prescribed entity for the exclusive use of the linked records of personal health information by the prescribed person or prescribed entity;	• Solely in the custody of the prescribed person or prescribed entity for the exclusive use by the prescribed person or prescribed entity;
	• The linkage of records of personal health information in the custody of the prescribed person or prescribed entity with records of personal health information to be collected from another person or organization for the exclusive use of the linked records of personal health information by the prescribed person or prescribed entity;	• In the custody of the prescribed person or prescribed entity with records of personal health information to be collected from another person or organization for the exclusive use by the prescribed person or prescribed entity;
	• The linkage of records of personal health information solely in the custody of the prescribed person or prescribed entity for purposes of disclosure of the linked records of personal health information to another person or organization; and	• Solely in the custody of the prescribed person or prescribed entity for purposes of disclosure of the linked records of personal health information to another person or organization; and
	• The linkage of records of personal health information in the custody of the prescribed person or prescribed entity with records of personal health information to be collected from another person or organization for purposes of disclosure of the linked records of personal health information to that other person or organization.	• In the custody of the prescribed person or prescribed entity with records of personal health information to be collected from another person or organization for purposes of disclosure of the linked records of personal health information to that other person or organization.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Review and Approval Process	Reviewing and Approving Requests to Link Records of Personal Health Information
	• Must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny the request to link records of personal health information and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny the request to link records of personal health information and the process that must be followed. This request process must set out the: ○ Documentation that must be completed, provided and/or executed; ○ Agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; ○ Agent(s) to whom the documentation must be provided; and ○ Required content of the documentation.
	• Must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request to link records of personal health information.	• The policy, procedures and practices must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request to link records of personal health information.
	• Should also set out the manner in which the decision approving or denying the request to link records of personal health information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	• The policy, procedures and practices must address the manner of documenting the decision approving or denying the request to link records of personal health information and the reasons for the decision; and • The policy, procedures and practices must address the method and format in which the decision will be communicated and to whom.
	Conditions or Restrictions on the Approval	Conditions or Restrictions on the Approval
	• Where the linked records of personal health information will be disclosed by the prescribed person or prescribed entity to another person or organization, the policy and procedures must require that the disclosure be approved pursuant to the *Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements* or the *Policy and Procedures for Disclosure of Personal Health Information For Purposes Other Than Research*, as may be applicable.	• Where the linked records of personal health information will be disclosed by the prescribed person or prescribed entity to another person or organization, the policy, procedures and practices must require that the disclosure be approved pursuant to the *Policy, Procedures and Practices for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements* or the *Policy, Procedures and Practices for Disclosure of Personal Health Information For Purposes Other Than Research*, as applicable.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Where the linked records of personal health information will be used by the prescribed person or prescribed entity, the policy and procedures must require that the use be approved pursuant to the *Policy and Procedures for the Use of Personal Health Information for Research or the Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information*, as may be applicable.	• Where the linked records of personal health information will be used by the prescribed person or prescribed entity, the policy, procedures and practices must require that the use be approved pursuant to the *Policy, Procedures and Practices for the Use of Personal Health Information for Research* or the *Policy, Procedures and Practices for Limiting Agent Access to and Use of Personal Health Information*, as may be applicable.
	• Must require that the linked records of personal health information be de-identified and/or aggregated as soon as practicable pursuant to the *Policy and Procedures with Respect to De-Identification and Aggregation* and that, to the extent possible, only de-identified and/or aggregate information be used by agents of the prescribed person or prescribed entity.	• The policy, procedures and practices must require that the linked records of personal health information be de-identified and/or aggregated as soon as reasonably possible pursuant to the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation* and that, to the extent possible, only de-identified and/or aggregate information be used by agents of the prescribed person or prescribed entity.
	<u>Process for the Linkage of Records of Personal Health Information</u>	<u>Process for the Linkage of Records of Personal Health Information</u>
	• Must outline the process to be followed in linking records of personal health information, the manner in which the linkage of records of personal health information must be conducted and the agent(s) responsible for linking records of Personal Health Information when approved in accordance with this policy and its procedures.	• The policy, procedures and practices must outline the process to be followed in linking records of personal health information, the manner in which the linkage of records of personal health information must be conducted and the agent(s) responsible for linking records of personal health information when approved in accordance with this policy, procedures and practices.
	<u>Retention</u>	<u>Secure Retention</u>
	• Must require that linked records of personal health information be retained in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information* until they are de-identified and/or aggregated pursuant to the *Policy and Procedures with Respect to De-Identification and Aggregation*.	• The policy, procedures and practices must require that linked records of personal health information be retained in compliance with the *Policy, Procedures and Practices for Secure Retention of Records of Personal Health Information* until they are de-identified and/or aggregated pursuant to the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation*.
	<u>Secure Disposal</u>	<u>Secure Disposal</u>
	• Must address the secure disposal of records of personal health information linked by the prescribed person or prescribed entity and, in particular, must require that the records of personal health information be securely disposed of in compliance with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information*.	• The policy, procedures and practices must address the secure disposal of records of personal health information linked by the prescribed person or prescribed entity and, in particular, must require that the records of personal health information be securely disposed of in compliance with the *Policy, Procedures and Practices for Secure Disposal of Records of Personal Health Information.*

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	Compliance, Audit and Enforcement	Compliance, Audit and Enforcement
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	• The policy, procedures and practices must require agents to comply with the policy, procedures and practices; • The policy, procedures and practices must address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*;
	• Must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	• The policy, procedures and practices must stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audit*s; • The policy, procedures and practices must identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; and
	• Must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.	• The policy, procedures and practices must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices.
	Tracking Approved Linkages of Records of Personal Health Information	Tracking Approved Linkages of Records of Personal Health Information
	• Must require that a log be maintained of the linkages of records of personal health information approved by the prescribed person or prescribed entity and must identify the agent(s) responsible for maintaining such a log.	• The policy, procedures and practices must require that the prescribed person or prescribed entity maintain information with regard to all requests and approvals to link records of personal health information approved by the prescribed person or prescribed entity in such a manner that the prescribed person or prescribed entity can promptly generate a log from the information. • The policy, procedures and practices must identify the agent(s) responsible for maintaining the information;
	• It is also recommended that the policy and procedures address where documentation related to the receipt, review, approval or denial of requests to link records of personal health information will be retained and the agent(s) responsible for retaining this documentation.	• The policy, procedures and practices must address where documentation related to the receipt, review, approval or denial of requests to link records of personal health information will be retained; and • The policy, procedures and practices must identify the agent(s) responsible for retaining this documentation.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
Policy 23. **Log of Approved Linkages of Records of Personal Health Information**	• A prescribed person or prescribed entity must maintain a log of linkages of records of personal health information approved by the prescribed person or prescribed entity.	• A prescribed person or prescribed entity, as the case may be, must maintain information with regard to all requests and approvals to link records of personal health information. The information with regard to all requests and approvals must be maintained in such a manner that the prescribed person or prescribed entity can promptly generate a log from the information.
	Log Requirements	
	• Must include the name of the agent, person or organization who requested the linkage; the date that the linkage of records of personal health information was approved; and the nature of the records of personal health information linked.	• At a minimum, the information, and any subsequent log generated from the information, must include the: o Name of the agent, person or organization who requested the linkage; o Date that the linkage of records of personal health information was approved; and o Nature of the records of personal health information linked.
Policy 24. **2011 Manual: Policy and Procedures with Respect to De-Identification and Aggregation** **2024 Manual: Policy, Procedures and Practices with Respect to De-Identification and Aggregation**	• A policy and procedures must be developed and implemented with respect to de-identification and aggregation.	• A policy, procedures and practices must be developed and implemented with respect to de- identification and aggregation that takes a risk-based approach.
	• Must require that personal health information not be used or disclosed if other information, namely de-identified and/or aggregate information, will serve the identified purpose.	• The policy, procedures and practices must require that personal health information not be used or disclosed if other information, namely de-identified and/or aggregate information, will serve the identified purpose.
	• The policy of the prescribed person or prescribed entity with respect to cell-sizes of less than five and the exceptions thereto must also be articulated. In articulating the policy with respect to cell-sizes of less than five, regard must be had to the restrictions related to cell-sizes of less than five contained in data sharing agreements, research agreements and written research plans pursuant to which the personal health information was collected by the prescribed person or prescribed entity.	
	• Must provide a definition of de-identified information and aggregate information that identifies the meaning ascribed to each of these terms. The definitions adopted and the policy of the prescribed person or prescribed entity with respect to cell-sizes of less than five shall have regard to, and must be consistent with, the meaning of "identifying information" in subsection 4(2) of the *Act*.	• The policy, procedures and practices must provide a definition of de-identified information and aggregate information which must have regard to small cell-sizes (e.g. less than five), and be consistent with, the meaning of "identifying information" in subsection 4(2) of PHIPA and the meaning of "de-identify" in section 2 of PHIPA.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must identify the information that must be removed, encrypted and/or truncated in order to constitute de-identified information and the manner in which the information must be grouped, collapsed or averaged in order to constitute aggregate information.	• The policy, procedures and practices must require removal, encryption, transformation and/or truncation in order to constitute de-identified information and sets out the manner in which the information must be grouped, collapsed or averaged in order to constitute aggregate information;
	• Must address the agent(s) responsible for de-identifying and/or aggregating information and the procedure to be followed in this regard.	• The policy, procedures and practices must identify the agent(s) responsible for de-identifying and/or aggregating information and the procedure to be followed.
	• Must require de-identified and/or aggregate information, including information of cell-sizes of less than five, to be reviewed prior to use or disclosure in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for conducting this review must also be identified.	• The policy, procedures and practices must require de-identified and/or aggregate information, including information in small cell sizes (e.g. less than five), to be reviewed prior to use or disclosure in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. • The policy, procedures and practices must identify the agent(s) responsible for conducting this review.
	• The process to be followed in reviewing the de-identified and/or aggregate information and the criteria to be used in assessing the risk of re-identification shall also be set out.	• The policy, procedures and practices must set out the process to be followed in reviewing the de-identified and/or aggregate information and the criteria to be used in assessing and calculating the risk of re- identification.
		<u>Different Release Models</u>
		• The policy, procedures, and practices may address the following three different release models for de-identified and/or aggregate information: “public,” “semi-public,” and “non-public,” having regard to the Information and Privacy Commissioner of Ontario’s De-Identification Guidelines for Structured Data as well as evolving industry information security standards and best practices. Depending on the release model used, the required level of de-identification and/or aggregation may vary.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Small Cell Sizes
		• The policy, procedures and practices must address small cell-sizes (e.g. less than five) and must require that the prescribed person or prescribed entity take a risk-based approach that involves calculating an acceptable level of re-identification risk for a given data release that utilizes techniques such as masking, generalization and suppression. • The policy, procedures and practices must set out the process and criteria for conducting such a risk-based analysis, having regard to the Information and Privacy Commissioner of Ontario's De-Identification Guidelines for Structured Data as well as evolving industry information security standards and best practices. • In articulating the policy, procedures and practices with respect to small cell-sizes, regard must be had to the restrictions related to small cell-sizes (e.g. less than five) contained in *Data Sharing Agreements*, *Research Agreements* and written research plans pursuant to which the personal health information was collected by the prescribed person or prescribed entity.
		Re-Identification
	• In establishing the criteria to be used in assessing the risk of re-identification, the prescribed person or prescribed entity shall have regard to the type of identifying information available, including information that can be used to identify an individual directly (e.g., name, address, health card number) or indirectly (e.g., date-of-birth, postal code, gender).	• In establishing the criteria to be used in assessing the risk of re-identification, the prescribed person or prescribed entity must have regard to the type of identifying information available, including information that can be used to identify an individual directly (e.g., name, address, health card number) or indirectly (e.g., date-of-birth, postal code, gender).
		• The policy, procedures and practices must identify the limited and specific purposes for which, and circumstances in which, de-identified and/or aggregate information may be re-identified and must identify the conditions or restrictions imposed on an agent granted approval to re-identify an individual from de-identified and/or aggregate information. • The prescribed person or prescribed entity must ensure that any such approvals are granted in accordance with the policy, procedures and practices and are permitted by PHIPA or another Act.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		• The policy, procedures and practices must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny the request to re-identify an individual from de-identified and/or aggregate information and the process that must be followed. This process must set out the: o Documentation that must be completed, provided and/or executed; o Agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; o Agent(s) to whom the documentation must be provided; and o Required content of the documentation.
	• Recommended that the prescribed person or prescribed entity explore new tools that are being developed to assist in ensuring that the policy and procedures developed with respect to de-identification and aggregation are based on an assessment of the actual risk of re-identification.	• The prescribed person or prescribed entity should explore new tools available or that are being developed to assist in ensuring that the policy, procedures and practices developed with respect to de-identification and aggregation are based on an assessment of the actual risk of re-identification.
	• Must prohibit agents from using de-identified and/or aggregate information, including information in cell-sizes of less than five, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.	• The policy, procedures and practices must also prohibit agents from using de-identified and/or aggregate information, including information in small cell-sizes, to identify an individual, unless the re-identification is done in accordance with the policy, procedures and practices and is permitted by PHIPA or another Act. This must include prohibiting any attempt to decrypt information that is encrypted for the purpose of re-identification, or identifying an individual based on unencrypted information and/or prior knowledge.
	• Must identify the mechanisms implemented to ensure that the persons or organizations to whom de-identified and/or aggregate information is disclosed will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual.	• The policy, procedures and practices must identify the mechanisms implemented to ensure that the persons or organizations to whom de-identified and/or aggregate information is disclosed will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual, unless such re-identification is permitted by PHIPA or another Act.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Compliance, Audit and Enforcement
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	• The policy, procedures and practices must require agents to comply with the policy, procedures and practices. • The policy, procedures and practices must address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*.
	• Must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	• The policy, procedures and practices must stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audit*s. • The policy, procedures and practices must identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices.
	• Must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management,* if an agent breaches or believes there may have been a breach of this policy or its procedures	• The policy, procedures and practices must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices.
		Privacy Impact Assessments
Policy 25. **2011 Manual: Privacy Impact Assessment Policy and Procedures** **2024 Manual: Policy, Procedures and Practices for Privacy Impact Assessments**	• Must be developed and implemented to identify the circumstances in which privacy impact assessments are required to be conducted.	• 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, it is recommended that the policy and procedures ensure that prescribed persons or prescribed entities conduct privacy impact assessments on existing and proposed data holdings involving personal health information and whenever a new or a change to an existing information system, technology or program involving personal health information is contemplated.	• In identifying the circumstances in which privacy impact assessments are required to be conducted, the policy, procedures and practices should ensure that prescribed persons or prescribed entities conduct privacy impact assessments:
		  ○ On existing and proposed data holdings involving personal health information; and
		  ○ Whenever a new or a change to an existing information system, technology or program involving personal health information is contemplated.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		• 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: o Process that must be followed in determining when privacy impact assessments are required to be completed and reviewed and the agent(s) responsible for making this determination; and o Process to be followed in ensuring that privacy impact assessments are in fact conducted, completed, reviewed and amended, as necessary, and the agent(s) responsible for conducting the required follow-up.
		<u>Circumstances in which Privacy Impact Assessments are Not Required</u>
	• If there are limited and specific circumstances in which privacy impact assessments are not required to be conducted on existing and proposed data holdings involving personal health information and whenever a new or a change to an existing information system, technology or program involving personal health information is contemplated, these must be outlined in the policy and procedures along with a rationale for why privacy impact assessments are not required. The policy and procedures must further identify the agent(s) responsible for making this determination and must require the determination and the reasons for the determination to be documented.	• 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: o Require documentation of the rationale for why a privacy impact assessment is not required; o Set out the documentation that must be completed, provided and/or executed; o Identify the agent(s) responsible for completing, providing and/or executing the documentation; o Identify the agent(s) to whom this documentation must be provided; and o 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.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Timing of Conducting and Reviewing Privacy Impact Assessments
	• Must also address the timing of privacy impact assessments. With respect to proposed data holdings involving personal health information and new or changes to existing information systems, technologies or programs involving personal health information, the policy and procedures must require that privacy impact assessments be conducted at the conceptual design stage and that they be reviewed and amended, if necessary, during the detailed design and implementation stage. With respect to existing data holdings involving personal health information, the policy and procedures must require that a timetable be developed to ensure privacy impact assessments are conducted and the policy and procedures must identify the agent(s) responsible for developing the timetable.	• The policy, procedures and practices must also address the timing of privacy impact assessments: • With respect to proposed data holdings involving personal health information and the introduction of new or changes to existing information systems, technologies or programs involving personal health information, the policy, procedures and practices must require that privacy impact assessments be: o Conducted at the conceptual design stage; and o Reviewed and amended, if necessary, during the detailed design and implementation stage. • With respect to existing data holdings involving personal health information, the policy, procedures and practices must require: • A timetable be developed to ensure privacy impact assessments are conducted, as and/or updated, as and when necessary; and • The identification of the agent(s) responsible for developing the timetable.
	• Once privacy impact assessments have been completed, the policy and procedures shall require that they be reviewed on an ongoing basis in order to ensure that they continue to be accurate and continue to be consistent with the information practices of the prescribed person or prescribed entity. The policy and procedures must also identify the circumstances in which and the frequency with which privacy impact assessments are required to be reviewed.	• Once privacy impact assessments have been completed, the policy, procedures and practices must require the: o Review of privacy impact assessments to take place on an ongoing basis in order to ensure that they continue to be accurate and continue to be consistent with the information practices of the prescribed person or prescribed entity; and o Identification of the circumstances in which and the frequency with which privacy impact assessments are required to be reviewed.
	• Must identify the agent(s) responsible and the process that must be followed in identifying when privacy impact assessments are required; in identifying when privacy impact assessments are required to be reviewed in accordance with the policy and procedures; in ensuring that privacy impact assessments are conducted and completed; and in ensuring that privacy impact assessments are reviewed and amended, if necessary. The role of agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified in respect of privacy impact assessments.	

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Required Content of Privacy Impact Assessments
	• Must stipulate the required content of privacy impact assessments. At a minimum, the privacy impact assessments must be required to describe:	• The policy, procedures and practices must also stipulate the required content of privacy impact assessments. At a minimum, the privacy impact assessments must be required to describe:
	• The data holding, information system, technology or program at issue;	• The data holding, information system, technology or program at issue;
	• Nature and type of personal health information collected, used or disclosed or that is proposed to be collected, used or disclosed;	• The nature and type of personal health information collected, used or disclosed or that is proposed to be collected, used or disclosed;
	• Sources of the personal health information;	• The sources of the personal health information;
	• Purposes for which the personal health information is collected, used or disclosed or is proposed to be collected, used or disclosed;	• The purposes for which the personal health information is collected, used or disclosed or is proposed to be collected, used or disclosed;
	• Reason that the personal health information is required for the purposes identified;	• The reason that the personal health information is required for the purposes identified;
	• Flows of the personal health information;	• The flows of the personal health information;
	• Statutory authority for each collection, use and disclosure of personal health information identified;	• The statutory authority for each collection, use and disclosure of personal health information identified;
	• Limitations imposed on the collection, use and disclosure of the personal health information;	• The limitations imposed on the collection, use and disclosure of the personal health information;
	• Whether or not the personal health information is or will be linked to other information;	• Whether or not the personal health information is or will be linked to other information;
		• Whether or not the personal health information will be de-identified and/or aggregated and the specific purposes for which and circumstances in which the de-identified and/or aggregate information will be re-identified, if any, the conditions or restrictions imposed;
	• Retention period for the records of personal health information;	• The retention period for the records of personal health information;
	• The secure manner in which the records of personal health information are or will be retained, transferred and disposed of;	• The secure manner in which the records of personal health information are or will be retained, transferred and disposed of;

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• The functionality for logging access, use, modification and disclosure of the personal health information and the functionality to audit logs for unauthorized use or disclosure;	• The functionality for logging access, use, modification and disclosure of the personal health information and the functionality to audit logs for unauthorized use or disclosure;
	• Risks to the privacy of individuals whose personal health information is or will be part of the data holding, information system, technology or program and an assessment of the risks;	• The risks to the privacy of individuals whose personal health information is or will be part of the data holding, information system, technology or program and an assessment of the risks;
	• Recommendations to address and eliminate or reduce the privacy risks identified; and	• Recommendations to address and eliminate or reduce the privacy risks identified; and
	• Administrative, technical and physical safeguards implemented or proposed to be implemented to protect the personal health information.	• The administrative, technical and physical safeguards implemented or proposed to be implemented to protect the personal health information.
		<u>Privacy Impact Assessment Findings and Recommendations</u>
	• The process for addressing the recommendations arising from privacy impact assessments, including the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations, is also required to be outlined.	• The policy, procedures and practices must also outline the process for documenting the findings, and reviewing and addressing the mitigations and any other recommendations arising from privacy impact assessments, including the agent(s) responsible for: o Assigning other agent(s) to address the mitigations and any other relevant recommendations; o Establishing timelines to address the mitigations and any other recommendations; o Monitoring and ensuring the treatment of the mitigations and any other relevant recommendations within stated timelines; and o Evaluating the residual risks remaining after implementation.
	• Must require that a log be maintained of privacy impact assessments that have been completed; that have been undertaken but that have not been completed; and that have not been undertaken. The policy and procedures must also identify the agent(s) responsible for maintaining such a log.	• The policy, procedures and practices must require that a log be maintained of: o Privacy impact assessments that have been completed; o Privacy impact assessments that have been undertaken but that have not been completed; o Privacy impact assessments that have not been undertaken; and o The identification of the agent(s) responsible for maintaining such a log.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Relationship to the Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act
	• Recommended that regard be had to the *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act,* published by the Information and Privacy Commissioner of Ontario.	• In developing the policy, procedures and practices regard should be given to the P*rivacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*, published by the Information and Privacy Commissioner of Ontario.
		Compliance, Audit and Enforcement
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits,* must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	• The policy, procedures and practices must require agents to comply with the policy, procedures and practices; • The policy, procedures and practices must identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; • The policy, procedures and practices must address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and, • The policy, procedures and practices must stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audit*s.
	• Must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.	• The policy, procedures and practices must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
Policy 26. **Log of Privacy Impact Assessments**	• A prescribed person or prescribed entity shall maintain a log of privacy impact assessments that have been completed and of privacy impact assessments that have been undertaken but that have not been completed.	• A prescribed person or prescribed entity must maintain a log of privacy impact assessments that have been completed and of privacy impact assessments that will be or have been undertaken, but that have not yet been completed.
	• Shall describe the data holding, information system, technology or program involving personal health information that is at issue; the date that the privacy impact assessment was completed or is expected to be completed; the agent(s) responsible for completing or ensuring the completion of the privacy impact assessment; the recommendations arising from the privacy impact assessment; the agent(s) responsible for addressing each recommendation, the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.	• The log must describe the: o Data holding, information system, technology or program involving personal health information that is at issue; o Date that the privacy impact assessment was completed or is expected to be completed; o Agent(s) responsible for completing or ensuring the completion of the privacy impact assessment; o Findings, mitigations and any other recommendations arising from the privacy impact assessment; o Agent(s) responsible for addressing each mitigation and any other recommendation; the date that each mitigation or recommendation was or is expected to be addressed; and o Manner in which each recommendation was or is expected to be addressed.
	• A prescribed person or prescribed entity shall also maintain a log of data holdings involving personal health information and of new or changes to existing information systems, technologies or programs involving personal health information for which privacy impact assessments have not been undertaken.	• A prescribed person or prescribed entity must also maintain a log of data holdings involving personal health information and of new or changes to existing information systems, technologies or programs involving personal health information for which privacy impact assessments have not been undertaken.
	• For each such data holding, information system, technology or program, the log shall either set out the reason that a privacy impact assessment will not be undertaken and the agent(s) responsible for making this determination or set out the date that the privacy impact assessment is expected to be completed and the agent(s) responsible for completing or ensuring the completion of the privacy impact assessment.	• For each such data holding, information system, technology or program, the log either set out the: o Reasons that a privacy impact assessment will not be undertaken; o Agent(s) responsible for making this determination; and o Date the determination was made.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Privacy Audit Program
Policy 27. **2011 Manual: Policy and Procedures in Respect of Privacy Audits** **2024 Manual: Policy, Procedures and Practices in Respect of Privacy Audits**	• Must be developed and implemented that sets out the types of privacy audits that are required to be conducted.	• A policy, procedures and practices must be developed and implemented that sets out the types of privacy audits that are required to be conducted.
	• The audits required to be conducted shall include audits to assess compliance with the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and audits of the agent(s) permitted to access and use personal health information pursuant to *Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information*.	• The audits required to be conducted must include: o Audits to assess compliance with the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity; and o Audits of the agent(s) permitted to access and use personal health information pursuant to *Policy, Procedures and Practices for Limiting Agent Access to and Use of Personal Health Information*.
	• With respect to each privacy audit that is required to be conducted, the policy and procedures must set out the purposes of the privacy audit; the nature and scope of the privacy audit (i.e. document reviews, interviews, site visits, inspections); the agent(s) responsible for conducting the privacy audit; and the frequency with which and the circumstances in which each privacy audit is required to be conducted. In this regard, the policy and procedures shall require a privacy audit schedule to be developed and shall identify the agent(s) responsible for developing the privacy audit schedule.	• With respect to each privacy audit that is required to be conducted, the policy, procedures and practices must: o Set out the purposes of the privacy audit; o Describe the nature and scope of the privacy audit (i.e. document reviews, interviews, site visits, inspections); o Identify the agent(s) responsible for conducting the privacy audit; o Establish the frequency with which and the circumstances in which each privacy audit is required to be conducted; o Require a privacy audit schedule to be developed; and o Identify the agent(s) responsible for developing the privacy audit schedule.
		• At a minimum, audits of agents granted approval to access and use personal health information under the *Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information* must be conducted on an annual basis.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• For each type of privacy audit that is required to be conducted, the policy and procedures shall also set out the process to be followed in conducting the audit. This is to include the criteria that must be considered in selecting the subject matter of the audit and whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification must be provided.	• 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: o Criteria that must be considered in selecting the subject matter of the audit; and o 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.
		<u>Required Documentation</u>
	• Must further discuss the documentation that must be completed, provided and/or executed in undertaking each privacy audit; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must further discuss the requirements for undertaking each privacy audit, including the: o Documentation that must be completed, provided and/or executed; o Agent(s) responsible for completing, providing and/or executing the documentation; o Agent(s) to whom this documentation must be provided; and o Required content of the documentation.
	• The role of agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.	
	• Shall set out the process that must be followed in addressing the recommendations arising from privacy audits, including the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations.	• The policy, procedures and practices must also set out the process that must be followed in reviewing and addressing the mitigations and any other recommendations resulting from privacy audits, including the agent(s) responsible for: o Assigning other agent(s) to address the mitigations and any other recommendations as required; o Establishing timelines to address the mitigations and any other relevant recommendations; o Monitoring and ensuring the treatment of mitigations and any other recommendations within the stated timelines; and o Evaluating the residual risks remaining after implementation.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must set out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the privacy audit, including the agent(s) responsible for completing, providing and/or executing the documentation, the agent(s) to whom the documentation must be provided and the required content of the documentation.	• The policy, 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: o Agent(s) responsible for completing, providing and/or executing the documentation; o Agent(s) to whom the documentation must be provided; and o Required content of the documentation.
		<u>Privacy Audit Findings</u>
	• Must address the manner and format in which the findings of privacy audits, including the recommendations arising from the privacy audits and the status of addressing the recommendations, are communicated. This shall include a discussion of the agent(s) responsible for communicating the findings of the privacy audit; the mechanism and format for communicating the findings of the privacy audit; the time frame within which the findings of the privacy audit must be communicated; and to whom the findings of the privacy audit will be communicated, including the Chief Executive Officer or the Executive Director.	• The policy, 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: o Identifying the agent(s) responsible for communicating the findings of the privacy audit; o The mechanism and format for communicating the findings of the privacy audit, including the level of detail for communicating the findings; o The timeframe within which the findings of the privacy audit must be communicated; and o 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).
	• Must further require that a log be maintained of privacy audits and must identify the agent(s) responsible for maintaining the log and for tracking that the recommendations arising from the privacy audits are addressed within the identified time frame. They should further address where documentation related to privacy audits will be retained and the agent(s) responsible for retaining this documentation.	• The policy, procedures and practices must require that a log be maintained of privacy audits; • The policy, procedures and practices must identify the agent(s) responsible for maintaining the log of findings, mitigations and other recommendations and for tracking that the mitigations / recommendations arising from the privacy audits are addressed within the identified timeframe; • The policy, procedures and practices must address where documentation related to privacy audits will be retained; and • The policy, procedures and practices must identify the agent(s) responsible for retaining this documentation.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Compliance, Audit and Enforcement
	• Must require the agent(s) responsible for conducting the privacy audit to notify the prescribed person or prescribed entity, at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with the *Policy and Procedures for Privacy Breach Management* and of an information security breach or suspected information security breach in accordance with the *Policy and Procedures for Information Security Breach Management.*	• The policy, procedures and practices must require the agent(s) responsible for conducting privacy audits to notify the prescribed person or prescribed entity, at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, and/or of an information security breach or information security incident in accordance with the *Policy, Procedures and Practices for Information Security Breach Management*.
Policy 28. **Log of Privacy Audits**	• A prescribed person or prescribed entity must maintain a log of privacy audits that have been completed. • Must set out the nature and type of the privacy audit conducted; the date that the privacy audit was completed; the agent(s) responsible for completing the privacy audit; the recommendations arising from the privacy audit; the agent(s) responsible for addressing each recommendation; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.	• A prescribed person or prescribed entity must maintain a log of privacy audits that have been completed. The log must set out the: o Nature and type of the privacy audit conducted; o Date that the privacy audit was completed; o Agent(s) responsible for completing the privacy audit; o Findings, mitigations and other relevant recommendations arising from the privacy audit; o Agent(s) responsible for addressing each recommendation; o Date that each recommendation was or is expected to be addressed; and o Manner in which each recommendation was or is expected to be addressed.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Privacy Breaches
Policy 29. **2011 Manual: Policy and Procedures for Privacy Breach Management** **2024 Manual: Policy, Procedures and Practices for Privacy Breach Management**	• Must be developed and implemented to address the identification, reporting, containment, notification, investigation and remediation of privacy breaches.	• A policy, procedures and practices must be developed and implemented to address the identification, reporting, containment, notification, investigation and remediation of privacy breaches.
	• Must provide a definition of the term "privacy breach." At a minimum, a privacy breach shall be defined to include:	• The policy, procedures and practices must define the term "privacy breach" to, at a minimum, include:
	• The collection, use and disclosure of personal health information that is not in compliance with the *Act* or its regulation;	• The collection, use and disclosure of personal health information that is not in compliance with PHIPA or its regulations
	• A contravention of the privacy policies, procedures or practices implemented by the prescribed person or prescribed entity;	• A contravention of the privacy policies, procedures or practices implemented by the prescribed person or prescribed entity, related to the requirements of the Manual;
	• A contravention of data sharing agreements, research agreements, confidentiality agreements and agreements with third party service providers retained by the prescribed person or prescribed entity; and	• A contravention of written acknowledgments, data sharing agreements, research agreements, confidentiality agreements and third party service provider agreements, related to the requirements of the Manual;
	• Circumstances where personal health information is stolen, lost or subject to unauthorized use or disclosure or where records of personal health information are subject to unauthorized copying, modification or disposal.	• Circumstances where personal health information is stolen, lost or collected, used or disclosed without authority or where records of personal health information are subject to unauthorized copying, modification or disposal.
		• 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.
		• The policy, procedures and practices must set out the manner in which privacy breaches or suspected privacy breaches will be identified by agents of the prescribed person or prescribed entity. At a minimum, the policy, procedures, and practices must indicate that privacy breaches or suspected privacy breaches will be identified through notifications, including by agents and electronic service providers of the prescribed person or prescribed entity, privacy audits, and privacy complaints and inquiries.
	• Must impose a mandatory requirement on agents to notify the prescribed person or prescribed entity of a privacy breach or suspected privacy breach.	• The policy, procedures and practices must require that agents notify the prescribed person or prescribed entity of a privacy breach or suspected privacy breach at the first reasonable opportunity.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Identification of Privacy Breaches
	• Must identify the agent(s) who must be notified of the privacy breach or suspected privacy breach and shall provide contact information for the agent(s) who must be notified.	• The policy, procedures and practices must identify the agent(s) who must be notified of the privacy breach or suspected privacy breach and must provide their contact information;
	• Must stipulate the time frame within which notification must be provided, whether the notification must be provided verbally and/or in writing and the nature of the information that must be provided upon notification.	• The policy, procedures and practices must 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;
	• Must address the documentation that must be completed, provided and/or executed with respect to notification; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must address the documentation that must be completed, provided and/or executed with respect to notification, including the: o Agent(s) responsible for completing, providing and/or executing the documentation; o Agent(s) to whom this documentation must be provided; and o Required content of the documentation.
		Determination of Whether a Privacy Beach Occurred
	• Upon notification, the policy and procedures must require a determination to be made of whether a privacy breach has in fact occurred and if so, what, if any, personal health information has been breached. The agent(s) responsible for making this determination must also be identified.	• The policy, procedures and practices must require a determination to be made as to: o Whether a privacy breach has in fact occurred, and if so, what, if any, personal health information has been breached; o The extent of the privacy breach; o Whether the breach is a privacy breach, or an information security breach, or both; and o The identification of the agent(s) responsible for making this determination.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		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: o Specific criteria for determining the prioritization level for a particular privacy breach or suspected privacy breach at a given point in time, allowing for escalation or de-escalation in response to an evolving situation; and o Criteria that includes the consideration of factors, such as the: ▪ Potential impact of the privacy breach; ▪ Recoverability from the privacy breach or suspected privacy breach; and ▪ The extent to which personal health information may be affected. • Where a prioritization framework is included, the policy, procedures and practices should identify the: o Agent(s) responsible for the prioritization framework; o Agent(s) responsible for approving the prioritization framework; o Procedures that must be followed, including any documentation that must be completed, provided and/or executed by the agent(s) responsible for developing the prioritization framework and approving the prioritization framework; o Agent(s) to whom this documentation must be provided; and o Required content of the documentation.
		Breach Notification to Senior Management
	• Must address when senior management, including the Chief Executive Officer or the Executive Director, will be notified. This shall include a discussion of the agent(s) responsible for notifying senior management; the time frame within which notification must be provided; the manner in which this notification must be provided; and the nature of the information that must be provided to senior management upon notification.	• The policy, 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: o Identifying the agent(s) responsible for notifying senior management; o The timeframe within which notification must be provided; o The manner in which this notification must be provided; and o The nature of the information that must be provided to senior management upon notification, including the level of detail that must be provided.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		<u>Relationship to Policy, Procedures and Practices for Information Security Breach Management</u>
		• The policy, procedures and practices must address the process to be followed in identifying, reporting, containing, notifying, investigating and remediating an event that is both a privacy breach or suspected privacy breach, as well as an information security breach or information security incident.
		<u>Containment</u>
	• Must require that containment be initiated immediately and shall identify the agent(s) responsible for containment and the procedure that must be followed in this regard, including any documentation that must be completed, provided and/or executed by the agent(s) responsible for containing the breach and the required content of the documentation.	• The policy, procedures and practices must require that containment be initiated immediately and must identify the: o Agent(s) responsible for containment and the procedure that must be followed, including any documentation that must be completed, provided and/or executed by the agent(s) responsible for containing the breach; and o Required content of the documentation.
	• In undertaking containment, the policy and procedures must ensure that reasonable steps are taken in the circumstances to protect personal health information from further theft, loss or unauthorized use or disclosure and to protect records of personal health information from further unauthorized copying, modification or disposal. At a minimum, these steps shall include ensuring that no copies of the records of personal health information have been made and ensuring that the records of personal health information are either retrieved or disposed of in a secure manner. Where the records of personal health information are securely disposed of, written confirmation should be obtained related to the date, time and method of secure disposal. These steps must also include ensuring that additional privacy breaches cannot occur through the same means and determining whether the privacy breach would allow unauthorized access to any other information and, if necessary, taking further action to prevent additional privacy breaches.	• The policy, procedures and practices must ensure that reasonable steps are taken in the circumstances to protect personal health information from further theft, loss or unauthorized collection, use or disclosure and to protect records of personal health information from further unauthorized copying, modification or disposal. At a minimum, these steps must include ensuring that: o No copies of the records of personal health information have been made; and o The records of personal health information are either retrieved or disposed of in a secure manner. • Where the records of personal health information are securely disposed of, written confirmation should be obtained relating to the date, time and method of secure disposal, as well as: o Assurance that additional privacy breaches cannot occur through the same means; o A determination of whether the privacy breach would allow unauthorized access to any other information; and, o If necessary an acknowledgement of further actions being taken to prevent additional privacy breaches.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• The agent(s) responsible and the process to be followed in reviewing the containment measures implemented and determining whether the privacy breach has been effectively contained or whether further containment measures are necessary, must be identified in the policy and procedures.	• The policy, procedures and practices must 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; • The policy, procedures and practices must identify the agent(s) responsible for reviewing the containment measures;
	• Must address the documentation that must be completed, provided and/or executed by the agent(s) responsible for reviewing the containment measures; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must identify the documentation that must be completed, provided and/or executed in reviewing the containment measures; • The policy, procedures and practices must identify the agent(s) responsible for completing, providing and/executing the documentation; • The policy, procedures and practices must identify agent(s) to whom this documentation must be provided; and • The policy, procedures and practices must identify required content of the documentation.
		<u>Breach Notification to Custodians or Other Organizations</u>
	• Must require the health information custodian or other organization that disclosed the personal health information to the prescribed person or prescribed entity to be notified at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization.	• The policy, procedures and practices must require the prescribed person or prescribed entity to notify, at the first reasonable opportunity, the custodian or other organization that disclosed the personal health information to the prescribed person or prescribed entity whenever personal health information has been or is believed to be stolen, lost or collected, used or disclosed without authority and whenever required pursuant to the agreement with the custodian or other organization.
	• Must set out the agent(s) responsible for notifying the health information custodian or other organization, the format of the notification and the nature of the information that must be provided upon notification.	• The policy, procedures and practices must set out the agent(s) responsible for notifying the custodian or other organization; • The policy, procedures and practices must set out the format of the notification; and • The policy, procedures and practices must set out the nature of the information that must be provided upon notification.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must require the health information custodian or other organization to be advised of the extent of the privacy breach, the nature of the personal health information at issue, the measures implemented to contain the privacy breach and further actions that will be undertaken with respect to the privacy breach, including investigation and remediation. As a secondary collector of personal health information, a prescribed person or prescribed entity should not directly notify the individual to whom the personal health information relates of a privacy breach. The required notification must be provided by the health information custodian.	• The policy, procedures and practices must require the custodian or other organization to be advised of: o The extent of the privacy breach; o The nature of the personal health information at issue; o The measures implemented to contain the privacy breach: and o Further actions that will be undertaken with respect to the privacy breach, including investigation and remediation.
		<u>Breach Notification to Affected Individuals</u>
	• As a secondary collector of personal health information, a prescribed person or prescribed entity should not directly notify the individual to whom the personal health information relates of a privacy breach. The required notification must be provided by the health information custodian.	• As a secondary collector of personal health information, a prescribed person or prescribed entity should not directly notify the individual to whom the personal health information relates of a privacy breach. Where applicable, the required notification to individuals must be provided by the relevant custodian(s), unless an alternative decision regarding breach notification to affected individuals is approved by the Information and Privacy Commissioner of Ontario.
		<u>Breach Notification to the Information and Privacy Commissioner of Ontario</u>
	• Must set out whether any other persons or organizations must be notified of the privacy breach and shall set out the agent(s) responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification and the time frame for notification.	• The policy, procedures and practices must also set out a process for determining whether the Information and Privacy Commissioner of Ontario, or any other persons or organizations must be notified of the privacy breach and must set out the: o Agent(s) responsible for providing such notification; o Format of the notification; o Nature of the information that must be provided upon notification; and o Timeframe for notification.
		• The prescribed persons or prescribed entities must notify the Information and Privacy Commissioner of Ontario, at the first reasonable opportunity, of privacy breaches in the circumstances set out in subsections 6.3(1) and 18.3(1) of PHIPA's regulations, as if the prescribed person or prescribed entity were a custodian.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Investigation of Breach
	• Must identify the agent(s) responsible for investigating the privacy breach, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the privacy breach. This shall include a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. The role of agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.	• The policy, procedures and practices must further identify the: o Agent(s) responsible for investigating the privacy breach; o Nature and scope of the investigation (i.e., document reviews, interviews, site visits, inspections); o Process that must be followed in investigating the privacy breach. This process must set out the: o Documentation that must be completed, provided and/or executed in undertaking the investigation; o Agent(s) responsible for completing, providing and/or executing the documentation; o Agent(s) to whom this documentation must be provided; and o Required content of the documentation.
	• Must identify the agent(s) responsible for assigning other agent(s) to address the recommendations; for establishing timelines to address the recommendations; for addressing the recommendations; and for monitoring and ensuring that the recommendations are implemented within the stated timelines. • Must 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 investigation of the privacy breach, including the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must also identify the agent(s) responsible for: o Assigning other agent(s) to address the mitigations and any other relevant recommendations as required; o Establishing timelines to address the mitigations and any other recommendations; o Monitoring and ensuring the treatment of the mitigations and any other recommendations within the stated timelines; and o 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: o Agent(s) responsible for completing, providing and/or executing the documentation; o Agent(s) to whom the documentation must be provided; and o Required content of the documentation.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Communication of Findings of Investigation and Recommendations
	• Must address the manner and format in which the findings of the investigation of the privacy breach, including the recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This shall include a discussion of the agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings of the investigation must be communicated, including the Chief Executive Officer or the Executive Director.	• 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: o The agent(s) responsible for communicating the findings of the investigation; o The mechanism and format for communicating the findings of the investigation, including the level of detail for communicating the findings; o The timeframe within which the findings of the investigation must be communicated; and o 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).
	• Must address whether the process to be followed in identifying, reporting, containing, notifying, investigating and remediating a privacy breach is different where the breach is both a privacy breach or suspected privacy breach, as well as an information security breach or suspected information security breach.	
		Tracking Privacy Breaches
	• Must require that a log be maintained of privacy breaches and must identify the agent(s) responsible for maintaining the log and for tracking that the recommendations arising from the investigation of privacy breaches are addressed within the identified timelines. They should further address where documentation related to the identification, reporting, containment, notification, investigation and remediation of privacy breaches will be retained and the agent(s) responsible for retaining this documentation.	• The policy, procedures and practices must: o Require that a log be maintained of privacy breaches; o Identify the agent(s) responsible for maintaining the log and for tracking the findings, mitigations or other relevant recommendations arising from the investigation of privacy breaches are addressed within the identified timelines. o Address where documentation related to the identification, reporting, containment, notification, investigation and remediation of privacy breaches will be retained; and o Identify the agent(s) responsible for retaining this documentation.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Compliance, Audit and Enforcement
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	• The policy, procedures and practices must: o Require agents to comply with the policy, procedures and practices; o Require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices; o Identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; o Address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and o Stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits.*
	• It is recommended that the prescribed person or prescribed entity have regard to the guidelines produced by the Information and Privacy Commissioner of Ontario entitled *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector*.	• The prescribed person or prescribed entity must have regard to the guidelines produced by the Information and Privacy Commissioner of Ontario entitled Responding to a Health Privacy Breach: Guidelines for the Health Sector.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
Policy 30. **Log of Privacy Breaches**	• A prescribed person or prescribed entity shall maintain a log of privacy breaches setting out: • Date of the privacy breach; • Date that the privacy breach was identified or suspected; • Whether the privacy breach was internal or external; • Nature of the personal health information that was the subject matter of the privacy breach and the nature and extent of the privacy breach; • Date that the privacy breach was contained and the nature of the containment measures; • Date that the health information custodian or other organization that disclosed the personal health information to the prescribed person or prescribed entity was notified; • Date that the investigation of the privacy breach was completed; • The agent(s) responsible for conducting the investigation; • The recommendations arising from the investigation; • The agent(s) responsible for addressing each recommendation; • The date each recommendation was or is expected to be addressed; and • The manner in which each recommendation was or is expected to be addressed.	• A prescribed person or prescribed entity must maintain a log of privacy breaches and suspected privacy breaches. At a minimum, the log must set out: ○ The date of the privacy breach or suspected privacy breach; ○ The date that the privacy breach was identified or suspected; ○ The nature of the personal health information, if any, that was the subject matter of the privacy breach and the nature and extent of the privacy breach or suspected privacy breach; ○ A description of the privacy breach or suspected privacy breach and who identified the privacy breach or suspected privacy breach; ○ The cause of the privacy breach or suspected privacy breach, ○ Whether an unauthorized person who is not an agent or electronic service provider caused the privacy breach or suspected privacy breach and the name or a description of the unauthorized person, if applicable; ○ The date that the Chief Executive Officer or Executive Director (or equivalent position) and senior management were notified of the privacy breach or suspected privacy breach, if applicable; ○ The date that the privacy breach or suspected privacy breach was contained and the nature of the containment measures; ○ The name of the agent(s) responsible for containing the privacy breach or suspected privacy breach; ○ The date that the investigation was commenced; ○ The date that the investigation was completed; ○ The agent(s) responsible for conducting the investigation; ○ The findings, mitigations and other relevant recommendations arising from the investigation; ○ The agent(s) responsible for addressing each recommendation; ○ The manner in which each recommendation was or is expected to be addressed; ○ The date by which each recommendation was or is expected to be addressed;

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		○ The date that the Chief Executive Officer or Executive Director (or equivalent position) and senior management were notified of the findings, mitigations and other relevant recommendations arising from the investigation, if applicable; ○ The date that the custodian or other organization that disclosed the personal health information to the prescribed person or prescribed entity was notified, if applicable; ○ The date that notification was provided to the Information and Privacy Commissioner of Ontario, if applicable; and ○ The date that notification was provided to individuals, if applicable.
Policy 31. **2011 Manual: Policy and Procedures for Privacy Complaints** **2024 Manual: Policy, Procedures and Practices for Privacy Complaints**		<u>Privacy Complaints and Inquiries</u>
	• A policy and procedures must be developed and implemented to address the process to be followed in receiving, documenting, tracking, investigating, remediating and responding to privacy complaints	• A 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.
	• Must provide a definition of the term "privacy complaint" that, at a minimum, includes concerns or complaints relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with the *Act* and its regulation.	• A definition of the term "privacy complaint" must be provided that, at a minimum, includes concerns or complaints relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with PHIPA and its regulations.
	• 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	• 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.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• The name and/or title, mailing address and contact information of the agent(s) to whom concerns or complaints may be directed and information related to the manner in which and format in which privacy concerns or complaints may be directed to the prescribed person or prescribed entity should be made publicly available. • Recommended that individuals be advised that they may make a complaint regarding compliance with the *Act* and its regulation to the Information and Privacy Commissioner of Ontario and that the mailing address and contact information for the Information and Privacy Commissioner of Ontario be provided.	• At a minimum, the following must be made publicly available: o The name and/or title, mailing address and contact information of the agent(s) to whom concerns or complaints may be directed; o Information related to the manner in which and format in which privacy concerns or complaints may be directed to the prescribed person or prescribed entity; o Information advising individuals that they may make a complaint to the Information and Privacy Commissioner of Ontario regarding the prescribed person's or prescribed entity's compliance with PHIPA and its regulations; and o The mailing address and contact information for the Information and Privacy Commissioner of Ontario.
		<u>Process for Receiving Complaints</u>
	• Must establish the process to be followed in receiving privacy complaints. This shall include any documentation that must be completed, provided and/or executed by the individual making the privacy complaint; the agent(s) responsible for receiving the privacy complaint; the required content of the documentation, if any; and the nature of the information to be requested from the individual making the privacy complaint.	• The policy, procedures and practices must further establish the process to be followed in receiving privacy complaints. This must include: o Any documentation that must be completed, provided and/or executed by the complainant; o The agent(s) responsible for receiving the privacy complaint; o The required content of the documentation, if any; and o The nature of the information to be requested from the complainant.
		<u>Determination of Whether to Investigate a Complaint</u>
	• Upon receipt of a privacy complaint, the policy and procedures shall require a determination to be made of whether or not the privacy complaint will be investigated. • Must identify the agent(s) responsible for making this determination, the time frame within which this determination must be made and the process that must be followed and the criteria that must be used in making the determination, including any documentation that must be completed, provided and/or executed and the required content of the documentation.	• 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: o Agent(s) responsible for making this determination; o Timeframe within which this determination must be made; o Process that must be followed; o Criteria that must be used in making the determination, including any documentation that must be completed, provided and/or executed; and o Required content of the documentation.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Where Complaint Will Not Be Investigated
	• In the event that it is determined that an investigation will not be undertaken, the policy and procedures must require that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; providing a response to the privacy complaint; advising that an investigation of the privacy complaint will not be undertaken; advising the individual that he or she may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that the prescribed person or prescribed entity has contravened or is about to contravene the *Act* or its regulation; and providing contact information for the Information and Privacy Commissioner of Ontario.	• In the event that it is determined that an investigation will not be undertaken, the policy, procedures and practices must require that a letter be provided to the complainant that includes: o Acknowledgement of receipt of the privacy complaint; o A response to the privacy complaint; o Advising that an investigation of the privacy complaint will not be undertaken along with the rationale for the decision not to investigate; o Advising the complainant that they may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that the prescribed person or prescribed entity has contravened or is about to contravene PHIPA or its regulations; and o The contact information for the Information and Privacy Commissioner of Ontario.
		Where Complaint Will Be Investigated
	• In the event that it is determined that an investigation will be undertaken, the policy and procedures must require that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; advising that an investigation of the privacy complaint will be undertaken; explaining the privacy complaint investigation procedure; indicating whether the individual will be contacted for further information concerning the privacy complaint; setting out the projected time frame for completion of the investigation; and identifying the nature of the documentation that will be provided to the individual following the investigation.	• 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: o Acknowledgement of receipt of the privacy complaint; o Advising that an investigation of the privacy complaint will be undertaken; o Explanation of the privacy complaint investigation procedure; o An indication of whether the complainant will be contacted for further information concerning the privacy complaint; o The projected timeframe for completion of the investigation; and o Identification of the nature of the documentation that will be provided to the complainant following the investigation.
	• Must identify the agent(s) responsible for sending the above noted letters to the individuals making privacy complaints and the time frame within which the letters will be sent to the individuals.	• The policy, procedures and practices must identify the agent(s) responsible for sending the above noted letters to complainants and the timeframe within which the letters will be sent to the individuals.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Where an investigation of a privacy complaint will be undertaken, the policy and procedures must identify the agent(s) responsible for investigating the privacy complaint, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the privacy complaint. This must include a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	• Where an investigation of a privacy complaint will be undertaken, the policy, procedures and practices must identify the: o Agent(s) responsible for investigating the privacy complaint; o Nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections); o Process that must be followed in investigating the privacy complaint; and o Documentation that must be completed, provided and/or executed in undertaking the investigation, including the: o Agent(s) responsible for completing, providing and/or executing the documentation; o Agent(s) to whom this documentation must be provided; and o Required content of the documentation.
	• Must identify the role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program	
	• The process for addressing the recommendations arising from the investigation of privacy complaints and the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations and for monitoring and ensuring the implementation of the recommendations shall also be addressed in the policy and procedures.	• The policy, procedures and practices must set out the process for addressing the mitigations and any other relevant recommendations arising from the investigation of privacy complaints and the agent(s) responsible for: o Assigning other agent(s) to address the mitigations and any other relevant recommendations; o Establishing timelines to address the mitigations and any other recommendations o Monitoring and ensuring the treatment of the mitigations and any other relevant recommendations within the stated timelines; and o Evaluating the residual risks remaining after implementation.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must set out the nature of the documentation that will be completed, provided and/or executed at the conclusion of the investigation of the privacy complaint, including the agent(s) responsible for completing, preparing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.	• The policy, 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: o Agent(s) responsible for completing, preparing and/or executing the documentation; o Agent(s) to whom the documentation must be provided; and o Required content of the documentation.
	• Must address the manner and format in which the findings of the investigation of the privacy complaint, including recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This shall include a discussion of the agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings must be communicated, including the Chief Executive Officer or the Executive Director.	• The policy, 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: o Identifying the agent(s) responsible for communicating the findings of the investigation; o The mechanism and format for communicating the findings of the investigation, including the level of detail for communicating the findings; o The timeframe within which the findings of the investigation must be communicated; and o 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).
	• Must require the individual making the privacy complaint to be notified, in writing, of the nature and findings of the investigation and of the measures taken, if any, in response to the privacy complaint. The individual making the privacy complaint must also be advised that he or she may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that the *Act* or its regulation has been or is about to be contravened. The contact information for the Information and Privacy Commissioner of Ontario must also be provided. The agent(s) responsible for providing the written notification to the individual making the privacy complaint and the time frame within which the written notification must be provided, must also be addressed.	• The policy, procedures and practices must further require the complainant to be notified, in writing, of: o The nature and findings of the investigation and of the measures taken, if any, in response to their privacy complaint; o Their right to make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that PHIPA or its regulations has been or is about to be contravened; and o The contact information for the Information and Privacy Commissioner of Ontario.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		• The policy, procedures and practices must also identify the agent(s) responsible for providing the written notification to the complainant and the timeframe within which the written notification must be provided.
	• Should address whether any other person or organization must be notified of privacy complaints and the results of the investigation of privacy complaints, and if so, the manner by which, the format in which and the time frame within which the notification must be provided and the agent(s) responsible for providing the notification.	• The policy, procedures and practices should also address whether and in what circumstances: ○ Any other person or organization must be notified of privacy complaints and the results of the investigation of privacy complaints, and if so the: • Manner and format in which notification must be provided; • Timeframe within which the notification must be provided; and • Agent(s) responsible for providing the notification.
		<u>Tracking Privacy Complaints</u>
	• Must require that a log be maintained of privacy complaints and must identify the agent(s) responsible for maintaining the log and for tracking whether the recommendations arising from the investigation of privacy complaints are addressed within the identified timelines. They should further address where documentation related to the receipt, investigation, notification and remediation of privacy complaints will be retained and the agent(s) responsible for retaining this documentation.	• The policy, procedures and practices must require a log to be maintained of privacy complaints; • The policy, procedures and practices must identify the agent(s) responsible for maintaining the log and for tracking the findings; • The policy, procedures and practices must assess whether the mitigations and other relevant recommendations arising from the investigation of privacy complaints are addressed within the identified timelines; • The policy, procedures and practices must specify where documentation related to the receipt, investigation, notification and remediation of privacy complaints will be retained; and • The policy, procedures and practices must detail the agent(s) responsible for retaining the documentation.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Compliance, Audit and Enforcement
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. • Must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	• The policy, procedures and practices must: o Require agents to comply with the policy, procedures and practices; o Require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices; o Identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; o Address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and, o Stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits*.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		Relationship to Other Policies, Procedures and Practices
	• The relationship between this policy and its procedures and the *Policy and Procedures for Privacy Breach Management* shall also be addressed. • This policy and its associated procedures may either be a stand-alone document or may be combined with the *Policy and Procedures for Privacy Inquiries*.	• 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*.

Policy 32.
 	
Log of Privacy Complaints
	• A prescribed person or prescribed entity must maintain a log of privacy complaints received that, at a minimum, sets out:
	• The date that the privacy complaint was received and the nature of the privacy complaint;
	• The determination as to whether or not the privacy complaint will be investigated and the date that the determination was made;
	• The date that the individual making the complaint was advised that the complaint will not be investigated and was provided a response to the complaint;
	• The date that the individual making the complaint was advised that the complaint will be investigated;
	• The agent(s) responsible for conducting the investigation;
	• The dates that the investigation was commenced and completed;
	• The recommendations arising from the investigation;
	• The agent(s) responsible for addressing each recommendation;
	• The date each recommendation was or is expected to be addressed;
	• The manner in which each recommendation was or is expected to be addressed; and
	• The date that the individual making the privacy complaint was advised of the findings of the investigation and the measures taken, if any, in response to the privacy complaint.
		• A prescribed person or prescribed entity must maintain a log of privacy complaints received that, at a minimum, sets out:
		  • The date that the privacy complaint was received and the nature of the privacy complaint;
		  • The determination as to whether the privacy complaint will be investigated and the date that the determination was made;
		  • The agent(s) who made the determination as to whether the privacy complaint would be investigated;
		  • Where the determination was made that the privacy complaint will not be investigated, the date that the complainant was advised that the complaint will not be investigated and informed of their right to file their complaint with the Information and Privacy Commissioner of Ontario; and
		  • Where the determination is made that the privacy complaint will be investigated:
		  ○ The date that the complainant was advised that the complaint will be investigated;
		  ○ The agent(s) responsible for conducting the investigation;
		  ○ The dates that the investigation was commenced and completed;
		  ○ The findings and other relevant recommendations arising from the investigation;
		  ○ The date that the Chief Executive Officer or Executive Director (or equivalent position) and senior management were notified of the findings and other relevant recommendations arising from the investigation, if applicable;
		  ○ The agent(s) responsible for addressing each recommendation;
		  ○ The date that each recommendation was or is expected to be addressed;

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
		○ The manner in which each recommendation was or is expected to be addressed; and ○ The date that the complainant was advised of the findings of the investigation, of the measures taken, if any, in response to the privacy complaint and of their right to file their complaint with the Information and Privacy Commissioner of Ontario.
Policy 33. **2011 Manual: Policy and Procedures for Privacy Inquiries** **2024 Manual: Policies, Procedures and Practices for Privacy Inquiries**	• A policy and procedures must be developed and implemented to address the process to be followed in receiving, documenting, tracking and responding to privacy inquiries.	• A policy, procedures and practices must be developed and implemented to address the process to be followed in receiving, documenting, tracking and responding to privacy inquiries.
	• A definition of the term "privacy inquiry" shall be provided that, at a minimum, includes inquiries relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with the *Act* and its regulation.	• A definition of the term "privacy inquiry" must be provided that, at a minimum, includes inquiries relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with PHIPA and its regulations.
	• The information that must be communicated to the public relating to the manner in which, to whom and where individuals may direct privacy inquiries shall also be identified.	• A prescribed person or prescribed entity must communicate to the public the manner in which, to whom and where individuals may direct privacy inquiries.
	• At a minimum, the information communicated to the public must include the name and/or title, mailing address and contact information of the agent(s) to whom privacy inquiries may be directed; information relating to the manner in which privacy inquiries may be directed to the prescribed person or prescribed entity; and information as to where individuals may obtain further information about the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity.	• At a minimum, the information communicated to the public must include: ○ The name and/or title, mailing address and contact information of the agent(s) to whom privacy inquiries may be directed; ○ Information relating to the manner in which privacy inquiries may be directed to the prescribed person or prescribed entity; and ○ Information as to where individuals may obtain further information about the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity.

Policy	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2011]	IPC: Manual for the Review and Approval of Prescribed Persons and Prescribed Entities [2024]
	• Must establish the process to be followed in receiving and responding to privacy inquiries. This must include the agent(s) responsible for receiving and responding to privacy inquiries; any documentation that must be completed, provided and/or executed; the required content of the documentation; and the format and content of the response to the privacy inquiry. The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program must also be identified.	• The policy, procedures and practices must further establish the process to be followed in receiving and responding to privacy inquiries. This must include: o The agent(s) responsible for receiving and responding to privacy inquiries; o The role of the agent(s) who have been delegated day-to-day authority to manage the privacy program and the information security program must also be identified. o Any documentation that must be completed, provided and/or executed; and o The required content and format of the documentation the prescribed person or prescribed entity would issue in response to a privacy inquiry.
		<u>Compliance, Audit and Enforcement</u>
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. • Must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures. The relationship between this policy and its procedures and the *Policy and Procedures for Privacy Complaints* and the *Policy and Procedures for Privacy Breach Management* must be addressed.	• The policy, procedures and practices must: o Require agents to comply with the policy, procedures and practices; o Require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy, Procedures and Practices for Privacy Breach Management*, if an agent breaches or believes there may have been breach of this policy, procedures or practices; o Identify the agent(s) responsible for ensuring compliance with the policy, procedures and practices; o Address how and by whom compliance will be enforced and the consequences of breach, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*; and, o Stipulate that compliance will be audited in accordance with the *Policy, Procedures and Practices In Respect of Privacy Audits*.
		<u>Relationship to Policy, Procedures and Practices for Privacy Complaints</u>
	[Note: this policy and its associated procedures may either be a stand-alone document or may be combined with the *Policy and Procedures for Privacy Complaints.*]	[Note: 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*.]