IPC Prescribed Entities and Prescribed Persons Manual 2011 and 2024 Comparison: Part 3

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 III	**HUMAN RESOURCES DOCUMENTATION**	**HUMAN RESOURCES POLICIES, PROCEDURES AND PRACTICES**
		Privacy Training and Awareness
Policy 1. **2011 Manual: Policy and Procedures for Privacy Training and Awareness** **2024 Manual: Policy, Procedures and Practices for Privacy Training and Awareness**	• A policy and procedures must be developed and implemented requiring agents of the prescribed person or prescribed entity to attend initial privacy orientation as well as ongoing privacy training.	• A policy, procedures and practices must be developed and implemented requiring agents of the prescribed person or prescribed entity to attend initial privacy training as well as ongoing privacy training.
		Timing and Method of Initial and Ongoing Privacy Training
	• Shall set out the time frame within which agents must complete the initial privacy orientation as well as address the frequency of ongoing privacy training.	• The policy, procedures and practices must set out the timeframe within which agents must complete the initial privacy training as well as address the frequency of ongoing privacy training.
	• Shall require an agent to complete the initial privacy orientation prior to being given access to personal health information and to attend ongoing privacy training provided by the prescribed person or prescribed entity on an annual basis.	• The policy, procedures and practices must require an agent to complete the initial privacy training prior to being given access to personal health information; • The policy, procedures and practices must require an agent to complete ongoing privacy training provided by the prescribed person or prescribed entity on an annual basis thereafter; and • The policy, procedures and practices must address the method(s) by which the initial and ongoing privacy training will 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>Process for Preparing the Content and Delivering Privacy Training</u>
	• The agent(s) responsible for preparing and delivering the initial privacy orientation and ongoing privacy training shall be identified.	• The policy, procedures and practices must identify the agent(s) responsible for preparing the content and ensuring the delivery of the initial and ongoing privacy training.
	• Shall set out the process that must be followed in notifying the agent(s) responsible for preparing and delivering the initial privacy orientation when an agent has commenced or will commence an employment, contractual or other relationship with the prescribed person or prescribed entity. This shall include a discussion of the agent(s) responsible for providing notification, the time frame within which notification must be provided and the format of the notification.	• The policy, procedures and practices must require the content of the initial and ongoing privacy training to be reviewed on an annual basis, and updated as needed; • The policy, procedures and practices must specify the frequency with which the training will be reviewed; • The policy, procedures and practices must identify the agents(s) responsible for reviewing and updating the training; • The policy, procedures and practices must set out the process that must be followed in notifying the agent(s) responsible for ensuring the delivery of the initial privacy training when an agent has commenced or will commence an employment, contractual or other relationship with the prescribed person or prescribed entity; • The policy, procedures and practices must identify the agent(s) responsible for providing notification; and • The policy, procedures and practices must set out the format of the notification and the timeframe within which such notification must be provided.
		<u>Initial Privacy Training</u>
	• Shall identify the content of the initial privacy orientation to ensure that it is formalized and standardized. At a minimum, the policy and procedures shall require that the initial privacy orientation include: ○ A description of the status of the prescribed person or prescribed entity under the Act and the duties and responsibilities that arise as a result of this status; ○ A description of the nature of the personal health information collected and from whom this information is typically collected; ○ An explanation of the purposes for which personal health information is collected and used and how this collection and use is permitted by the Act and its regulation;	• The policy, procedures and practices must also require the content of the initial privacy training to be formalized and standardized, and be based on evolving industry privacy standards and best practices. At a minimum, the policy, procedures and practices must require that the initial privacy training include: ○ A description of the status of the prescribed person or prescribed entity under PHIPA and the duties and responsibilities that arise as a result of this status; ○ A description of the nature of the personal health information collected and from whom this information is typically collected;

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]
	○ Limitations placed on access to and use of personal health information by agents; ○ A description of the procedure that must be followed in the event that an agent is requested to disclose personal health information; ○ An overview of the privacy policies, procedures and practices that have been implemented by the prescribed person or prescribed entity and the obligations arising from these policies, procedures and practices; ○ The consequences of breach of the privacy policies, procedures and practices implemented ○ An explanation of the privacy program, including the key activities of the program and the agent(s) that have been delegated day-to-day authority to manage the privacy program; ○ The administrative, technical and physical safeguards implemented by the prescribed person or prescribed entity 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 duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by the prescribed person or prescribed entity; ○ A discussion of the nature and purpose of the Confidentiality Agreement that agents must execute and the key provisions of the Confidentiality Agreement; and ○ An explanation of the *Policy and Procedures for Privacy Breach Management* and the duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches.	○ An explanation of the purposes for which personal health information is collected and used and how this collection and use is permitted by PHIPA and its regulations; ○ Limitations placed on access to and use of personal health information by agents; ○ A description of the manner in which the agent's activities in the information environment will be logged, monitored and audited, including in relation to personal health information; ○ Limitations, conditions or restrictions placed on the personal health information, including prohibitions on collecting, using or disclosing personal health information if other information, such as de-identified and/or aggregate information, will serve the purpose identified and on collecting, using or disclosing more personal health information than is reasonably necessary; ○ A description of the procedure that must be followed in the event that an agent is requested to disclose personal health information; ○ An overview of the privacy policies, procedures and practices that have been implemented by the prescribed person or prescribed entity and the obligations arising from these policies, procedures and practices; ○ The consequences of breach of PHIPA or its regulations or breach of the privacy policies, procedures and practices implemented; ○ An explanation of the privacy program, including the key activities of the program and the agent(s) who have been delegated day-to-day authority to manage the privacy program; ○ The administrative, technical and physical safeguards implemented by the prescribed person or prescribed entity 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; ○ The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by the prescribed person or prescribed entity; ○ The purposes for which de-identified or aggregated information derived from personal health information collected by the prescribed person or prescribed entity may be used or disclosed;

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]
		○ A prohibition on using de-identified or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is: ▪ Done in accordance with the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation*; and ▪ Permitted by PHIPA or another law, and a notice that compliance with this prohibition will be audited and monitored; ○ The nature and purpose of Privacy Notices and Confidentiality Agreements, and the key provisions of these notices and agreements; ○ An explanation of the *Policy, Procedures and Practices for Privacy Breach Management* and the related duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches, including the duty to notify the prescribed person or the prescribed entity, at the first reasonable opportunity, of a privacy breach or a suspected privacy breach; and ○ An explanation of the mandatory nature of privacy training, including the: ▪ Prohibition on all agents to handle personal health information without having completed initial privacy training; and ▪ Mandatory nature of ongoing privacy training on an annual basis thereafter.
		<u>Ongoing Privacy Training</u>
	• Shall require the ongoing privacy training to be formalized and standardized; to include role-based training in order to ensure that agents understand how to apply the privacy policies, procedures and practices in their day-to-day employment, contractual or other responsibilities; to address any new privacy policies, procedures and practices and significant amendments to existing privacy policies, procedures and practices; and to have regard to any recommendations with respect to privacy training made in privacy impact assessments, privacy audits and the investigation of privacy breaches and privacy complaints.	• The policy, procedures and practices must require the content of the ongoing privacy training to be formalized and standardized, and be based on evolving industry privacy standards and best practices. At a minimum, the policy, procedures and practices must require that ongoing privacy training: ○ Include role-based training in order to ensure that agents understand how to apply the privacy policies, procedures and practices in their day-to-day employment, contractual or other responsibilities as these may have evolved since their last training; ○ Address any new privacy policies, procedures and practices and significant amendments to existing privacy policies, procedures and practices; and ○ Incorporate any relevant changes since the last training, including:

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]
		▪ Recommendations with respect to privacy training made in privacy impact assessments, privacy audits and the investigation of privacy breaches and privacy complaints; ▪ Orders, decisions, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under PHIPA and its regulations; and ▪ Amendments to PHIPA and its regulations relevant to the prescribed person or prescribed entity.
		<u>Tracking, Auditing and Monitoring Privacy Training</u>
	• Must require that a log be maintained to track attendance at the initial privacy orientation as well as the ongoing privacy training and the policy and procedures must identify the agent(s) responsible for maintaining such a log and tracking attendance.	• The policy, procedures and practices must require a log to be maintained to track the attendance and completion of the initial and ongoing privacy training and identify the following: o Agent(s) responsible for maintaining such a log;
	• Must outline the process to be followed in tracking attendance at the initial privacy orientation as well as the ongoing privacy training, including the documentation that must be completed, provided and/or executed to verify attendance; the agent(s) responsible for completing, providing and/or executing the documentation; the agent to whom this documentation must be provided; and the required content of the documentation.	• The log must also identify: o Process to be followed in tracking completion of the initial and ongoing privacy training; o Documentation that must be completed, provided and/or executed to verify completion; o Agent(s) responsible for completing, providing and/or executing the documentation; o Agent to whom this documentation must be provided; o Required content of the documentation; o Where documentation related to completion of the initial and ongoing privacy training will be retained; and o 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]
	• Must identify the procedure to be followed and the agent(s) responsible for identifying agent(s) who do not attend the initial privacy orientation or the ongoing privacy training and for ensuring that such agent(s) attend the initial privacy orientation and the ongoing privacy training, including the time frame following the date of the privacy orientation or the ongoing privacy training within which this procedure must be implemented.	• The policy, procedures and practices must also set out the: o Agent(s) responsible for identifying agent(s) who do not complete the initial or ongoing privacy training; o Process for ensuring that completion of initial or ongoing privacy training takes place within the identified timeframe; and o Consequences for agents failing to complete the required privacy training within the identified timeframe, which must include the prescribed person's or prescribed entity's refusal or withdrawal of an agent's permission to access personal health information.
	• Recommended that the policy and procedures address where documentation related to attendance at the initial privacy orientation and the ongoing privacy training is to be retained and the agent(s) responsible for retaining this documentation.	
		<u>Other Mechanisms to Foster a Privacy Culture</u>
	• Shall discuss the other mechanisms implemented by the prescribed person or prescribed entity to foster a culture of privacy and to raise awareness of the privacy program and the privacy policies, procedures and practices implemented.	• The policy, procedures and practices must also address the: o Other mechanisms implemented by the prescribed person or prescribed entity to foster a culture of privacy and to raise awareness of the privacy program and the privacy policies, procedures and practices implemented;
	• Shall discuss the frequency with which the prescribed person or prescribed entity communicates with its agents in relation to privacy, the method and nature of the communication and the agent(s) responsible for the communication.	• The policy, procedures and practices must also address the: o Frequency with which the prescribed person or prescribed entity communicates with its agents in relation to privacy; o Method and nature of the communication; and o Agent(s) responsible for the communication.

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. • 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*.
		Relationship to Policy, Procedures and Practices for Information Security Training and Awareness
	• Note: This policy and its associated procedures may either be a stand-alone document or may be combined with the *Policy and Procedures for Security Training and Awareness*.	• This policy, procedures and practices may either be a stand-alone document or may be combined with the *Policy, Procedures and Practices for Information Security Training and Awareness*.
Policy 2. **2011 Manual: Log of Attendance at Initial Privacy Orientation and Ongoing Privacy Training** **2024 Manual: Log of Completion of Initial and Ongoing Privacy Training**	• A prescribed person or prescribed entity shall maintain a log of the attendance of agents at the initial privacy orientation and ongoing privacy training. At a minimum, the log must set out the name of the agent, the date that the agent attended the initial privacy orientation and the dates that the agent attended ongoing privacy training.	• A prescribed person or prescribed entity must maintain a log of the completion of the initial and ongoing privacy training by agents. At a minimum, the log must set out the: o Name of each agent; o Date that the agent commenced his or her employment, contractual or other relationship with the prescribed person or prescribed entity; o Date that the agent completed the initial privacy training; and o Each date that the agent completed ongoing privacy training.

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]
		Information Security Training and Awareness
Policy 3. **2011 Manual: Policy and Procedures for Security Training and Awareness** **2024 Manual: Policy, Procedures and Practices for Information Security Training and Awareness**	• A policy and procedures must be developed and implemented requiring agents of the prescribed person or prescribed entity to attend initial security orientation as well as ongoing security training.	• A policy, procedures and practices must be developed and implemented requiring agents of the prescribed person or prescribed entity to complete initial information security training as well as ongoing information security training.
		Timing and Method of Initial and Ongoing Information Security Training
	• Shall set out the time frame within which agents must complete the initial security orientation as well as address the frequency of ongoing security training.	• The policy, procedures and practices must set out the timeframe within which agents must complete the initial information security training as well as address the frequency of ongoing information security training.
	• Shall require an agent to complete the initial security orientation prior to being given access to personal health information and to attend ongoing security training provided by the prescribed person or prescribed entity on an annual basis.	• At a minimum, the policy, procedures and practices must: o Require agent(s) to complete the initial information security training prior to being given access to personal health information; o Require agent(s) to complete ongoing information security training provided by the prescribed person or prescribed entity on an annual basis thereafter; and o Specify the method(s) by which the initial and ongoing information security training will be provided.
		Process for Preparing and Delivering Information Security Training
	• Shall identify the agent(s) responsible for preparing and delivering the initial security orientation and ongoing security training.	• The policy, procedures and practices must identify the agent(s) responsible for preparing the content and ensuring the delivery of the initial and ongoing information security training; • The policy, procedures and practices must require the content of the initial and ongoing information security training to be reviewed and updated on a regular basis; • The policy, procedures and practices must set out the frequency with which the training will be reviewed; • The policy, procedures and practices must identify the agents(s) responsible for reviewing and updating the training; 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 require the initial training to be reviewed on an annual basis, and updated as needed.
	• Shall set out the process that must be followed in notifying the agent(s) responsible for preparing and delivering the initial security orientation when an agent has commenced or will commence an employment, contractual or other relationship with the prescribed person or prescribed entity	• The policy, procedures and practices must set out a process that must be followed in notifying the agent(s) responsible for ensuring the delivery of the initial information security training when an agent has commenced or will commence an employment, contractual or other relationship with the prescribed person or prescribed entity;
	• Shall include a discussion of the agent(s) responsible for providing notification, the time frame within which notification must be provided and the format of the notification.	• The policy, procedures and practices must identify the agent(s) responsible for providing such notification; • The policy, procedures and practices must specify the timeframe within which notification must be provided; and • The policy, procedures and practices must set out the format of the notification.
		<u>Initial Information Security Training</u>
	• Shall identify the content of the initial security orientation to ensure that it is formalized and standardized. At a minimum, the policy and procedures shall require that the initial security orientation include: o An overview of the security policies, procedures and practices that have been implemented by the prescribed person or prescribed entity and the obligations arising from these policies, procedures and practices; o The consequences of breach of the security policies, procedures and practices implemented; o An explanation of the security program, including the key activities of the program and the agent(s) that have been delegated day-to-day authority to manage the security program; o The administrative, technical and physical safeguards implemented by the prescribed person or prescribed entity 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 policy, procedures and practices must also require the content of the initial information security training to be formalized and standardized, and be based on evolving industry information security standards and best practices. At a minimum, the policy, procedures and practices must require that the initial information security training include: o An overview of the information security policies, procedures and practices that have been implemented by the prescribed person or prescribed entity and the obligations arising from these policies, procedures and practices; o The consequences of breach of PHIPA or its regulations or breach of the information security policies, procedures and practices implemented; o An explanation of the information security program, including the key activities of the program and the agent(s) who have been delegated day-to-day authority to manage the information security program;

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 duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by the prescribed person or prescribed entity; and ○ An explanation of the *Policy and Procedures for Information Security Breach Management* and the duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of information security breaches.	○ The administrative, technical and physical safeguards implemented by the prescribed person or prescribed entity 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; ○ The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by the prescribed person or prescribed entity; ○ An explanation of the *Policy, Procedures and Practices for Information Security Breach Management* and the related duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of information security breaches, including the duty to provide notification to the prescribed person or the prescribed entity at the first reasonable opportunity of an information security breach or information security incident; and ○ An explanation of the mandatory nature of information security training, including the prohibition on all agents to handle personal health information without having completed initial information security training, and the mandatory nature of ongoing information security training on an annual basis thereafter.
		<u>Ongoing Information Security Training</u>
	• Shall require the ongoing security training to be formalized and standardized; to include role-based training in order to ensure that agents understand how to apply the security policies, procedures and practices in their day-to-day employment, contractual or other responsibilities; to address any new security policies, procedures and practices and significant amendments to existing security policies, procedures and practices; and to have regard to any recommendations with respect to security training made in privacy impact assessments, the investigation of information security breaches and the conduct of security audits including threat and risk assessments, security reviews or assessments, vulnerability assessments, penetration testing, ethical hacks and reviews of system control and audit logs.	• The policy, procedures and practices must also require the content of the ongoing information security training to be formalized and standardized, and be based on evolving industry information security standards and best practices. At a minimum, the policy, procedures and practices must require that ongoing information security training: • Include role-based training in order to ensure that agents understand how to apply the information security policies, procedures and practices in their day-to-day employment, contractual or other responsibilities, as these may have evolved since their last training; ○ Address any new information security policies, procedures and practices and significant amendments to existing information security policies, procedures and practices; and ○ Incorporate any relevant changes since their last training, including: • Recommendations made with respect to:

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]
		▪ Information security training made in privacy impact assessments; ▪ The investigation of information security breaches; ▪ The conduct of information security audits including threat and risk assessments, security reviews or assessments, vulnerability assessments, penetration testing or ethical hacks; and ▪ The audits of privacy and information security events; o Orders, decisions, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under PHIPA and its regulations; and o Amendments to PHIPA and its regulations relevant to the prescribed person or prescribed entity.
		<u>Tracking, Auditing and Monitoring Information Security Training</u>
	• Must require that a log be maintained to track attendance at the initial security orientation as well as the ongoing security training and the policy and procedures must identify the agent(s) responsible for maintaining such a log and tracking attendance.	• The policy, procedures and practices must require that a log be maintained to track attendance and completion of the initial and ongoing information security training and identify the following: o Agent(s) responsible for maintaining such a log.
	• Shall outline the process to be followed in tracking attendance at the initial security orientation as well as the ongoing security training, including the documentation that must be completed, provided and/or executed to verify attendance; the agent(s) responsible for completing, providing and/or executing the documentation; the agent to whom this documentation must be provided; and the required content of the documentation.	• The policy, procedures and practices must require that a log be maintained to track attendance and completion of the initial and ongoing information security training and identify the following: o Process to be followed in tracking completion of the initial and ongoing information security training; o Documentation that must be completed, provided and/or executed to verify completion; o Agent(s) responsible for completing, providing and/or executing the documentation; o Agent(s) to whom this documentation must be provided; 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]
		○ Required content of the documentation; ○ Where documentation related to the completion of the initial and ongoing information security training will be retained; and ○ Agent(s) responsible for retaining this documentation.
	• Shall identify the procedure to be followed and the agent(s) responsible for identifying agent(s) who do not attend the initial security orientation or the ongoing security training and for ensuring that such agent(s) attend the initial security orientation and the ongoing security training, including the time frame following the date of the security orientation or the ongoing security training within which this procedure must be implemented.	• The policy, procedures and practices must identify the agent(s) responsible for identifying agent(s) who do not complete the initial or ongoing information security training; • The policy, procedures and practices must set out a process for ensuring that completion of initial and ongoing information security training take place within an identified timeframe; and • The policy, procedures and practices must set out the consequences for agents failing to complete the required information security training within the identified timeframe, which must include the prescribed person's or prescribed entity's refusal or withdrawal of agent's permission to access personal health information.
	• Recommended that the policy and procedures address where documentation related to attendance at the initial security orientation and the ongoing security training will be retained and the agent(s) responsible for retaining this documentation.	
		<u>Other Mechanisms to Raise Information Security Awareness</u>
	• Shall discuss the other mechanisms implemented by the prescribed person or prescribed entity to raise awareness of the security program and the security policies, procedures and practices implemented.	• The policy, procedures and practices must address other mechanisms implemented by the prescribed person or prescribed entity to raise awareness of the information security program and the information security policies, procedures and practices implemented.
	• Shall discuss the frequency with which the prescribed person or prescribed entity communicates with its agents in relation to information security, the method and nature of the communication and the agent(s) responsible for the communication.	• The policy, procedures and practices must address the frequency with which the prescribed person or prescribed entity communicates with its agents in relation to information security:

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 address the method and nature of the communication; and • The policy, procedures and practices must address the agent(s) responsible for the communication.
		<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 Security 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 Information Security 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 Information Security Breach Management*, if an agent breaches or believes there may have been a 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 Information Security Audits*.
		<u>Relationship to Policy, Procedures and Practices for Privacy Training and Awareness</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 Training and Awareness*.	• This policy, procedures and practices may either be a stand-alone document or may be combined with the *Policy, Procedures and Practices for Privacy Training and Awareness*.

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 4. **2011 Manual: Log of Attendance at Initial Security Orientation and Ongoing Security Training** **2024 Manual: Log of Completion of Initial and Ongoing Information Security Training**	• A prescribed person or prescribed entity shall maintain a log of the attendance of agents at the initial security orientation and ongoing security training. At a minimum, the log must set out the name of the agent, the date that the agent attended the initial security orientation and the dates that the agent attended ongoing security training.	• A prescribed person or prescribed entity must maintain a log of the completion of the initial and ongoing information security training by agents. At a minimum, the log must set out the: o Name of the agent; o Date that the agent commenced his or her employment, contractual or other relationship with the prescribed person or prescribed entity; o Dates that the agent completed the initial information security training; and o Each date the agent completed ongoing information security training.
		<u>Confidentiality Agreements</u>
Policy 5. **2011 Manual: Policy and Procedures for the Execution of Confidentiality Agreements by Agents** **2024 Manual: Policy, Procedures and Practices for the Execution of Confidentiality Agreements by Agents**	• A policy and procedures must be developed and implemented requiring agents to execute a Confidentiality Agreement in accordance with the *Template Confidentiality Agreement with Agents* at the commencement of their employment, contractual or other relationship with the prescribed person or prescribed entity and prior to being given access to personal health information.	• A policy, procedures and practices must be developed and implemented requiring agents to execute a Confidentiality Agreement that contains the requirements set out in the *Template Confidentiality Agreement with Agents.*
		<u>Timing of Confidentiality Agreements</u>
	• Recommended that the policy and procedures require that a Confidentiality Agreement be executed by agents on an annual basis and identify the time frame each year in which the Confidentiality Agreement is required to be executed.	• The policy, procedures and practices must set out the timeframe within which agents must execute the Confidentiality Agreement. At a minimum, the policy, procedures and practices must: o Require agents to execute a Confidentiality Agreement prior to being given access to personal health information, including personal health information that has been de-identified and/or aggregated, and on an annual basis thereafter; and o Identify the timeframe each year within which agents are required to execute the Confidentiality Agreement on an ongoing 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]
		<u>Process for Executing Confidentiality Agreements</u>
	• Must identify the agent(s) responsible for ensuring that a Confidentiality Agreement is executed with each agent of the prescribed person or prescribed entity at the commencement of the employment, contractual or other relationship and thereafter on an annual basis and the process that must be followed in this regard.	• The policy, procedures and practices must further identify the agent(s) responsible for ensuring that each agent executes a Confidentiality Agreement in compliance with the policy, procedures and practices of the prescribed person or prescribed entity.
	• Shall outline the process that must be followed in notifying the responsible agent(s) each time an agent has commenced or will commence an employment, contractual or other relationship with the prescribed person or prescribed entity. This shall include a discussion of the agent(s) responsible for providing notification, the time frame within which notification must be provided and the format of the notification.	• The policy, procedures and practices must identify the process for notifying the responsible agent(s) each time an agent has commenced or will commence an employment, contractual or other relationship with the prescribed person or prescribed entity; • The policy, procedures and practices must identify the agent(s) responsible for providing such notification; • The policy, procedures and practices must identify the timeframe within which such notification must be provided; and • The policy, procedures and practices must identify the format of the notification.
		<u>Tracking Execution of Confidentiality Agreements</u>
	• Shall outline the process that must be followed by the responsible agent(s) in tracking the execution of Confidentiality Agreements, including the process that must be followed where an executed Confidentiality Agreement is not received within a defined period of time following the commencement of the employment, contractual or other relationship or within a defined period of time following the date that the Confidentiality Agreement is required to be executed on an annual basis.	• The policy, procedures and practices must outline the process that must be followed by the responsible agent(s) in tracking and ensuring the execution of Confidentiality Agreements, including the process that must be followed: o Where an agent's executed Confidentiality Agreement is not received within a defined period of time following the commencement of the employment, contractual or other relationship; or o Within a defined period of time following the date that the Confidentiality Agreement is required to be executed on an annual basis.
	• Shall require that a log be maintained of executed Confidentiality Agreements and must identify the agent(s) responsible for maintaining such a log.	• The policy, procedures and practices must require that a log of executed Confidentiality Agreements be maintained; and • The policy, procedures and practices must identify the agent(s) responsible for maintaining the log and for tracking and ensuring that the Confidentiality Agreements have been executed.

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]
	• Recommended that the policy and procedures address where documentation related to the execution of Confidentiality Agreements will be retained and the agent(s) responsible for retaining this documentation.	• In outlining the process to be followed, the policy, procedures and practices must set out: o The documentation that must be completed, provided and/or executed to verify that Confidentiality Agreements have been executed; o The agent(s) responsible for completing, providing, executing and ensuring the execution of the documentation; o The agent(s) to whom this documentation must be provided; o The required content of the documentation; o Where documentation related to the Confidentiality Agreements will be retained; and o The agent(s) responsible for retaining this documentation.
		<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 with the policy and its procedures and with the Confidentiality Agreement 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 its 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]
Policy 6. **Template Confidentiality Agreement with Agents**	• A Confidentiality Agreement must be executed by each agent of the prescribed person or prescribed entity in accordance with the *Policy and Procedures for the Execution of Confidentiality Agreements by Agents* that, at a minimum, addresses the matters set out below.	• A Confidentiality Agreement must be executed by each agent of the prescribed person or prescribed entity in accordance with the *Policy, Procedures and Practices for the Execution of Confidentiality Agreements by Agents* that, at a minimum, addresses the matters set out below.
	<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 Confidentiality 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 that individuals executing the agreement are agents of the prescribed person or prescribed entity in respect of personal health information and must outline the responsibilities associated with this status.	• The Confidentiality Agreement must state that individuals executing the agreement are agents of the prescribed person or prescribed entity in respect of personal health information and must outline the responsibilities associated with this status.
		<u>Required Compliance</u>

	• Must require agents to comply with the provisions of the Act and its regulation relating to prescribed persons or prescribed entities, as the case may be, and with the terms of the Confidentiality Agreement as may be amended from time to time.
	• Agents must also be required to acknowledge that they have read, understood and agree to comply with the privacy and security policies, procedures and practices implemented by the prescribed person or prescribed entity and to comply with any privacy and security policies, procedures and practices as may be implemented or amended from time to time following the execution of the Confidentiality Agreement.
		• The Confidentiality Agreement must require agents to:
		  ○ Comply with the:
		  ▪ Provisions of PHIPA and its regulations relating to the role of the prescribed persons or prescribed entities, as the case may be; and
		  ▪ Terms of the Confidentiality Agreement as may be amended from time to time; and
		  ○ Acknowledge that they have read, understood and agree to comply with:
		  ▪ The privacy and information security policies, procedures and practices implemented by the prescribed person or prescribed entity; and
		  ▪ Any privacy and information security policies, procedures and practices as may be implemented or amended from time to time following the execution of the Confidentiality Agreement.

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]
	• It is also recommended that the Confidentiality Agreement provide a definition of personal health information and that the definition provided be consistent with the Act and its regulation.	• The Confidentiality Agreement must provide definitions of the terms "personal health information", "de-identified information" and "aggregate information". Where the definitions provided for: o "Personal health information" must be consistent with PHIPA and its regulations; and o "De-identified information" and "aggregate information" must be consistent with those definitions provided in the *Policy, Procedures and Practices with Respect to De- Identification and Aggregation.*
	<u>Obligations with Respect to Collection, Use and Disclosure of Personal Health Information</u>	<u>Obligations with Respect to Collection, Use and Disclosure of Personal Health Information</u>
	• Shall identify the purposes for which agents are permitted to collect, use and disclose personal health information on behalf of the prescribed person or prescribed entity and any limitations, conditions or restrictions imposed thereon.	• The Confidentiality Agreement must identify the purposes for which agents are permitted to collect, use and disclose personal health information on behalf of the prescribed person or prescribed entity and any limitations, conditions or restrictions imposed thereon.
	• In identifying the purposes for which agents are permitted to collect, use or disclose personal health information, the prescribed person or prescribed entity must ensure that each collection, use or disclosure identified in the Confidentiality Agreement is permitted by the Act and its regulation.	• In identifying the purposes for which agents are permitted to collect, use or disclose personal health information, the prescribed person or prescribed entity must ensure that each collection, use or disclosure identified in the Confidentiality Agreement is permitted by: o PHIPA and its regulations; and o The policies, procedures and practices put in place pursuant thereto.
	• Must prohibit agents from collecting and using personal health information except as permitted in the Confidentiality Agreement and from disclosing such information except as permitted in the Confidentiality Agreement or as required by law.	• The Confidentiality Agreement must prohibit agents from collecting, using or disclosing personal health information except as permitted in the Confidentiality Agreement or as required by 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]
	• Must prohibit agents from collecting, using or disclosing personal health information if other information will serve the purpose and from collecting, using or disclosing more personal health information than is reasonably necessary to meet the purpose.	• The Confidentiality Agreement must prohibit agents from collecting, using or disclosing personal health information if other information will serve the purpose and from collecting, using or disclosing more personal health information than is reasonably necessary to meet the purpose.
		<u>Obligations with Respect to De-Identified and Aggregate Information</u>
		• The Confidentiality Agreement must: ○ Identify the purposes for which agents are permitted to use and disclose personal health information which has been de-identified or aggregated, as the case may be; and ○ Prohibit agents from using the de-identified or aggregate information, either alone or with other information, to identify an individual, unless the re-identification is done in accordance with the *Policy, Procedures and Practices with Respect to De-Identification and Aggregation* and is permitted by PHIPA or another law. This must include prohibiting: ▪ Any attempt to decrypt information that is encrypted; or ▪ Identification of an individual based on unencrypted information and/or prior knowledge.
	<u>Termination of the Contractual, Employment or Other Relationship</u>	<u>Termination of the Contractual, Employment or Other Relationship</u>
	• Shall require agents to securely return all property of the prescribed person or prescribed entity, including records of personal health information and all identification cards, access cards and/or keys, on or before the date of termination of the employment, contractual or other relationship in accordance with the *Policy and Procedures For Termination or Cessation of the Employment or Contractual Relationship.*	• The Confidentiality Agreement must require agents to securely return all property of the prescribed person or prescribed entity, including records of personal health information and all identification cards, access cards and/or keys, on or before the date of termination of the employment, contractual or other relationship in accordance with the *Policy, Procedures and Practices upon Termination or Cessation of the Employment or Contractual Relationship*.

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]
	• Shall stipulate the time frame within which the property of the prescribed person or prescribed entity must be securely returned, the secure manner in which the property must be returned and the agent to whom the property must be securely returned.	• The Confidentiality Agreement must stipulate the: o Timeframe within which the property of the prescribed person or prescribed entity must be securely returned; o Secure manner in which the property must be returned; and o Agent to whom the property must be securely returned.
	Notification	Breach Notification to Prescribed Person or Prescribed Entity
	• Shall 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* and/or the *Policy and Procedures for Information Security Breach Management*, if the agent breaches or believes that there may have been a breach of the Confidentiality Agreement or if the agent breaches or believes that there may have been a breach of the privacy or security policies, procedures and practices implemented by the prescribed person or prescribed entity.	• The Confidentiality Agreement must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity and in accordance with the *Policy, Procedures and Practices for Privacy Breach Management* and/or the *Policy, Procedures and Practices for Information Security Breach Management*, if the agent breaches or believes that there may have been a breach of the Confidentiality Agreement or if the agent breaches or believes that there may have been a breach of the privacy or information security policies, procedures and practices implemented by the prescribed person or prescribed entity.
	Consequences of Breach and Monitoring Compliance	Consequences of Breach and Monitoring Compliance
	• Must outline the consequences of breach of the agreement and must address the manner in which compliance with the Confidentiality Agreement will be enforced.	• The Confidentiality Agreement must outline the consequences of breach of the agreement and must address the manner in which compliance with the Confidentiality Agreement will be enforced, in accordance with the *Policy, Procedures and Practices for Discipline and Corrective Action*.
	• Must stipulate that compliance with the Confidentiality Agreement will be audited and must address the manner in which compliance will be audited.	• The Confidentiality Agreement must stipulate that compliance with the Confidentiality Agreement will be audited; and • The Confidentiality Agreement must address the manner in which compliance will be audited.

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.
 	
Log of Executed Confidentiality Agreements with Agents
	• A prescribed person or prescribed entity must maintain a log of Confidentiality Agreements that have been executed by agents at the commencement of their employment, contractual or other relationship with the prescribed person or prescribed entity and on an annual basis.
	  ○ At a minimum, the log must include the name of the agent, the date of commencement of the employment, contractual or other relationship with the prescribed person or prescribed entity and the dates that the Confidentiality Agreements were executed.
		• A prescribed person or prescribed entity must maintain a log of Confidentiality Agreements that have been executed by agents at the commencement of their employment, contractual or other relationship with the prescribed person or prescribed entity and on an annual basis. At a minimum, the log must include the:
		  ○ Name of the agent;
		  ○ Date of commencement of the employment, contractual or other relationship with the prescribed person or prescribed entity; and
		  ○ Dates that the Confidentiality Agreement(s) were executed.

		<u>Privacy and Information Security Leadership</u>
Policy 8. **Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program**	• A job description for the position(s) that have been delegated day-to-day authority to manage the privacy program on behalf of the prescribed person or prescribed entity must be developed.	• A job description for the position(s) that have been delegated day-to-day authority to manage the privacy program on behalf of the prescribed person or prescribed entity must be developed.
	• Shall set out the reporting relationship of the position(s) that have been delegated day-to-day authority to manage the privacy program to the Chief Executive Officer or the Executive Director, as the case may be.	• The job description must set out the reporting relationship of this position(s) to the Chief Executive Officer or the Executive Director (or equivalent position), as the case may be.

	• Must identify the responsibilities and obligations of the position(s) in respect of the privacy program. At a minimum, these responsibilities and obligations must include:
	  • Developing, implementing, reviewing and amending privacy policies, procedures and practices;
	  • Ensuring compliance with the privacy policies, procedures and practices implemented;
	  • Ensuring transparency of the privacy policies, procedures and practices implemented;
	  • Facilitating compliance with the Act and its regulation;
	  • Ensuring agents are aware of the Act and its regulation and their duties thereunder;
		• The job description must identify the responsibilities and obligations of the position(s) in respect of the privacy program. At a minimum, these responsibilities and obligations must include:
		  ○ Developing, implementing, reviewing and amending privacy policies, procedures and practices;
		  ○ Ensuring compliance with the privacy policies, procedures and practices implemented;
		  ○ Ensuring transparency of the privacy policies, procedures and practices implemented;
		  ○ Facilitating compliance with PHIPA and its regulations;
		  ○ Ensuring agents are aware of PHIPA and its regulations and their duties thereunder;

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]
	• Ensuring agents are aware of the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and are appropriately informed of their duties and obligations thereunder; • Directing, delivering or ensuring the delivery of the initial privacy orientation and the ongoing privacy training and fostering a culture of privacy; • Conducting, reviewing and approving privacy impact assessments; • Receiving, documenting, tracking, investigating, remediating and responding to privacy complaints pursuant to the *Policy and Procedures for Privacy Complaints*; • Receiving and responding to privacy inquiries pursuant to the *Policy and Procedures for Privacy Inquiries*; • Receiving, documenting, tracking, investigating and remediating privacy breaches or suspected privacy breaches pursuant to the *Policy and Procedures for Privacy Breach Management*; and • Conducting privacy audits pursuant to the *Policy and Procedures In Respect of Privacy Audits*.	○ Ensuring agents are aware of the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and are appropriately informed of their duties and obligations thereunder; ○ Directing, delivering or ensuring the delivery of the initial and ongoing privacy training and fostering a culture of privacy; ○ Conducting, reviewing and approving privacy impact assessments in accordance with the *Policy, Procedures and Practices for Privacy Impact Assessments*; ○ Receiving, documenting, tracking, investigating, remediating and responding to privacy complaints pursuant to the *Policy, Procedures and Practices for Privacy Complaints*; ○ Receiving and responding to privacy inquiries pursuant to the *Policy, Procedures and Practices for Privacy Inquiries*; ○ Receiving, documenting, tracking, investigating and remediating privacy breaches or suspected privacy breaches pursuant to the *Policy, Procedures and Practices for Privacy Breach Management*; and ○ Conducting privacy audits pursuant to the *Policy, Procedures and Practices in Respect of Privacy Audits*.
Policy 9. **2011 Manual: Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program** **2024 Manual: Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Information Security Program**	• A job description for the position(s) that have been delegated day-to-day authority to manage the security program on behalf of the prescribed person or prescribed entity must be developed.	• A job description for the position(s) that have been delegated day-to-day authority to manage the information security program on behalf of the prescribed person or prescribed entity must be developed.
	• Shall set out the reporting relationship of the position(s) that have been delegated day-to-day authority to manage the security program to the Chief Executive Officer or the Executive Director, as the case may be.	• The job description must set out the reporting relationship of this position(s) to the Chief Executive Officer or the Executive Director (or equivalent position), as the case may be.
	• The job description must also identify the responsibilities and obligations of the position(s) in respect of the security program. At a minimum, these responsibilities and obligations must include:	• The job description must identify the responsibilities and obligations of the position(s) in respect of the information security program. At a minimum, these responsibilities and obligations must include:

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]
	• Developing, implementing, reviewing and amending security policies, procedures and practices; • Ensuring compliance with the security policies, procedures and practices implemented; • Ensuring agents are aware of the security policies, procedures and practices implemented by the prescribed person or prescribed entity and are appropriately informed of their duties and obligations thereunder; • Directing, delivering or ensuring the delivery of the initial security orientation and the ongoing security training and fostering a culture of information security awareness; and • Receiving, documenting, tracking, investigating and remediating information security breaches or suspected information security breaches pursuant to the *Policy and Procedures for Information Security Breach Management*; and Conducting security audits pursuant to the *Policy and Procedures In Respect of Security Audits*.	○ Developing, implementing, reviewing and amending information security policies, procedures and practices; ○ Ensuring compliance with the information security policies, procedures and practices implemented; ○ Ensuring agents are aware of the information security policies, procedures and practices implemented by the prescribed person or prescribed entity and are appropriately informed of their duties and obligations thereunder; ○ Directing, delivering or ensuring the delivery of the initial and ongoing information security training and fostering a culture of information security awareness; ○ Logging, monitoring and auditing of privacy and information security events pursuant to the *Policy, Procedures and Practices for Logging, Monitoring and Auditing Privacy and Information Security Events*; ○ Receiving, documenting, tracking, investigating and remediating information security breaches or information security incidents pursuant to the *Policy, Procedures and Practices for Information Security Breach Management*; and ○ Conducting information security audits pursuant to the *Policy, Procedures and Practices in Respect of Information Security Audits*.

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]
		Termination or Cessation
Policy 10. **2011 Manual: Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship** **2024 Manual: Policy, Procedures and Practices upon Termination or Cessation of the Employment or Contractual Relationship**	• Shall require agents, as well as their supervisors, to notify the prescribed person or prescribed entity of the termination of the employment, contractual or other relationship.	• The policy, procedures and practices must require agents, as well as their supervisors, to notify the prescribed person or prescribed entity of the termination or cessation of the employment, contractual or other relationship;
	• Shall identify the agent(s) to whom notification must be provided, the nature and format of the notification, the time frame within which notification must be provided and the process that must be followed in providing notification.	• The policy, procedures and practices must identify the: o Agent(s) to whom notification must be provided; o Nature and format of the notification; o Timeframe within which notification must be provided; and o Process that must be followed in providing notification.
		Secure Return of All Property
	• Shall also require agents to securely return all property of the prescribed person or prescribed entity on or before the date of termination of the employment, contractual or other relationship. In this regard, a definition of property must be provided and this definition must, at a minimum, include records of personal health information, identification cards, access cards and/or keys.	• The policy, procedures and practices must require agents to securely return all property of the prescribed person or prescribed entity on or before the date of termination or cessation of the employment, contractual or other relationship. In this regard, a definition of property must be provided in the policy, procedures and practices and this definition must, at a minimum, include records of personal health information, computing equipment, mobile devices, identification cards, access cards and/or keys.
	• Shall identify the agent(s) to whom the property must be securely returned; the secure method by which the property must be returned; the time frame within which the property must be securely returned; the documentation that must be completed, provided and/or executed; 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 identify the: o Agent(s) to whom the property must be securely returned; o Secure method by which the property must be returned; o Timeframe within which the property must be securely returned; o Documentation that must be completed, provided and/or executed; o Agent(s) responsible for completing, providing and/or executing the documentation; 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]
	• Shall address the procedures to be followed in the event that the property of the prescribed person or prescribed entity is not securely returned upon termination of the employment, contractual or other relationship, including the agent(s) responsible for implementing the procedure and the time frame following termination within which the procedure must be implemented.	• The policy, procedures and practices must identify the procedure to be followed in the event that the property of the prescribed person or prescribed entity is not securely returned upon termination or cessation of the employment, contractual or other relationship; and • The policy, procedures and practices must identify the agent(s) responsible for implementing the procedure and the timeframe following termination or cessation within which the procedure must be implemented.
		<u>Terminating Access to Premises and Information Environment</u>
	• Shall require that access to the premises of the prescribed person or prescribed entity, to locations within the premises where records of personal health information are retained and to the information technology operational environment, be immediately terminated upon the cessation of the employment, contractual or other relationship.	• The policy, procedures and practices must require that access to the premises of the prescribed person or prescribed entity, to locations within the premises where records of personal health information are retained, to components within the information environment, be immediately terminated upon the termination or cessation of the employment, contractual or other relationship;
	• Must identify the agent(s) responsible for terminating access; the procedure to be followed in terminating access; the time frame within which access must be terminated; the documentation that must be completed, provided and/or executed and the agent(s) responsible for completing, providing and/or executing the documentation.	• The policy, procedures and practices must identify the: o Agent(s) responsible for terminating access; o Procedure to be followed in terminating access; o Timeframe within which access must be terminated; o Documentation that must be completed, provided and/or executed; and o Agent(s) responsible for completing, providing and/or executing 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 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. • 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 and/or the Policy and Procedures for Information Security 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]
		Discipline and Corrective Action
Policy 11. **2011 Manual: Policy and Procedures for Discipline and Corrective Action** **2024 Manual: Policy, Procedures and Practices for Discipline and Corrective Action**	• Shall develop and implement a policy and associated procedures for discipline and corrective action in respect of personal health information.	• The prescribed person or prescribed entity must develop and implement a policy, procedures and practices for discipline and corrective action for breaches of agents' obligations and responsibilities in respect of protecting the privacy of individuals whose personal health information the prescribed person or prescribed entity receives and maintaining the confidentiality of that information.
	• Shall address the investigation of disciplinary matters, including the person(s) responsible for conducting the investigation; the procedure that must be followed in undertaking the investigation; any documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the required content of the documentation; and the agent(s) to whom the results of the investigation must be reported.	• The policy, procedures and practices must address: o The investigation of disciplinary matters, including the person(s) responsible for conducting the investigation; o The procedure that must be followed in undertaking the investigation; o Any documentation that must be completed, provided and/or executed in undertaking the investigation; o The agent(s) responsible for completing, providing and/or executing the documentation; o The required content of the documentation; and o The agent(s) to whom the results of the investigation must be reported.
	• Shall set out the types of discipline that may be imposed by the prescribed person or prescribed entity and the factors that must be considered in determining the appropriate discipline and corrective action shall also be set out in the policy and procedures.	• The policy, procedures and practices must also set out the: o Types of discipline that may be imposed by the prescribed person or prescribed entity on its agent(s); and o Factors that must be considered in determining the appropriate discipline and corrective action to be taken.
	• Shall identify the agent(s) responsible for determining the appropriate discipline and corrective action, the procedure to be followed in making this determination, the agent(s) that must be consulted in making this determination; and the documentation that must be completed, provided and/or executed.	• Agent(s) responsible for determining the appropriate discipline and corrective action; • Procedure to be followed in making this determination; • Agent(s) who must be consulted in making this determination; and • Documentation that must be completed, provided and/or executed.

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]
	• Recommended that the policy and procedures address the retention of documentation related to the discipline and corrective action taken, including where this documentation will be retained and the agent(s) responsible for retaining the documentation.	• The policy, procedures and practices should also address the retention of documentation related to the discipline and corrective action taken, including: o Where this documentation will be retained; and o The agent(s) responsible for retaining the documentation.