ACCESSPRIVACY BY OSLER

IPC Prescribed Entities and Prescribed Persons Manual 2011 and 2024 Comparison: Part 4

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 IV	**ORGANIZATION AND OTHER DOCUMENTATION**	**ORGANIZATIONAL POLICIES, PROCEDURES AND PRACTICES**
		Governance and Accountability
Policy 1. **Privacy Governance and Accountability Framework**	• A privacy governance and accountability framework for ensuring compliance with the Act and its regulation and for ensuring compliance with the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity must be established.	• A privacy governance and accountability framework must be established for ensuring compliance with: o PHIPA and its regulations; and o The privacy policies, procedures and practices implemented by the prescribed person or prescribed entity.
	• Must stipulate that the Chief Executive Officer or the Executive Director, as the case may be, is ultimately accountable for ensuring that the prescribed person or prescribed entity and its agents comply with the Act and its regulation and comply with the privacy policies, procedures and practices implemented.	• The privacy governance and accountability framework must stipulate that the Chief Executive Officer or the Executive Director (or equivalent position), as the case may be, is ultimately accountable for ensuring that the prescribed person or prescribed entity and its agents comply with: o PHIPA and its regulations; and o The privacy policies, procedures and practices implemented by the prescribed person or prescribed entity.
	• Must identify the position(s) that have been delegated day-to-day authority to manage the privacy program and the nature of the reporting relationship to the Chief Executive Officer or the Executive Director must be described.	• The privacy governance and accountability framework must identify the position(s) that have been delegated day-to-day authority to manage the privacy program; and • The privacy governance and accountability framework must describe the nature of the reporting relationship to the Chief Executive Officer or the Executive Director (or equivalent position).
	• Shall set out the responsibilities and obligations of the position(s) that have been delegated day-to-day authority to manage the privacy program and identify the other individuals, committees and teams that support the position(s) that have been delegated day-to-day authority to manage the privacy program and their role in respect of the privacy program.	• The privacy governance and accountability framework must set out the responsibilities and obligations of the position(s) that have been delegated day-to-day authority to manage the privacy program; • The privacy governance and accountability framework must identify the other individuals, committees and teams that have been delegated supporting roles to manage the privacy program; and • The privacy governance and accountability framework must describe the role(s) of the individuals, committees and teams in respect of the privacy 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]
		Board of Directors
	• Must address the role of the Board of Directors in respect of the privacy program, including whether the privacy program is overseen by a committee of the Board of Directors.	• The privacy governance and accountability framework must describe the role of the Board of Directors in respect of the privacy program, including any committee of the Board of Directors to which privacy oversight has been delegated.
	• Shall set out the frequency with which and the method and manner by which the Board of Directors is updated with respect to the privacy program, the agent(s) responsible for providing such updates and the matters with respect to which the Board of Directors is required to be updated. • It is recommended that the Board of Directors be updated on an annual basis, preferably in the form of a written report.	• The privacy governance and accountability framework must address the frequency with which the Board of Directors is updated with respect to the privacy program which, at a minimum, should be annually, and preferably in the form of a written report; • The privacy governance and accountability framework must identify the agent(s) responsible for providing such updates; • The privacy governance and accountability framework must set out the method and manner by which the Board of Directors is required to be updated; and • The privacy governance and accountability framework must identify the type of matters with respect to which the Board of Directors is required to be updated.
	• The update provided to the Board of Directors must address the initiatives undertaken by the privacy program including privacy training and the development and implementation of privacy policies, procedures and practices. It shall also include a discussion of the privacy audits and privacy impact assessments conducted, including the results of and recommendations arising from the privacy audits and privacy impact assessments and the status of implementation of the recommendations. The Board of Directors must also be advised of any privacy breaches and privacy complaints that were investigated, including the results of and any recommendations arising from these investigations and the status of implementation of the recommendations.	• The update provided to the Board of Directors must, at a minimum, address risks that may negatively affect the prescribed person's or prescribed entity's ability to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information that has been ranked as being high risk on the corporate risk register. Such matters should include: o Major financial investments required to ensure a robust and sustainable privacy governance and accountability framework; o The development, implementation and evaluation of major information technology transformation projects and high-risk information processing applications with privacy implications, such as artificial intelligence; o Relevant initiatives undertaken by the privacy program including privacy training; o The development and implementation of new privacy-related policies, procedures and practices, including those that are of major, corporate-wide significance and have implications for the Board, its members and the proper functioning of its committees;

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 findings, mitigations and any other relevant recommendations arising from privacy audits and privacy impact assessments, including the status of implementation of the mitigations and any other relevant recommendations; ○ Privacy breaches, suspected privacy breaches and privacy complaints that were investigated, as applicable, including the findings, mitigations and any other relevant recommendations arising from these investigations and the status of implementation of the mitigations / recommendations; ○ Major privacy related litigation matters, including privacy class-action lawsuits facing the prescribed person or prescribed entity; ○ Privacy related issues that have been identified through whistle-blowers; ○ Major changes to the privacy governance and accountability framework, including changes of personnel in high-level position(s) that have been delegated day-to-day authority to manage the privacy program and related reporting relationships; and • The privacy governance and accountability framework must set out whether, and the circumstances in which, the above information is provided to the Board of Directors, including the level of detail in which the information is provided.
	• It is recommended that the privacy governance and accountability framework be accompanied by a privacy governance organizational chart.	• The privacy governance and accountability framework should be accompanied by a privacy governance organizational chart.
	• Shall set out the manner in which the privacy governance and accountability framework will be communicated to agents of the prescribed person or prescribed entity, the method by which it will be communicated and the agent(s) responsible for this communication.	• The privacy governance and accountability framework must specify the method and manner by which the privacy governance and accountability framework will be communicated to agents of the prescribed person or prescribed entity; and • The privacy governance and accountability framework must identify the agent(s) responsible for this communication.
		<u>Relationship to Information Security Governance and Accountability Framework</u>
	• [Note: This governance and accountability framework may either be a stand-alone document or may be combined with the *Security Governance and Accountability Framework*.]	• This governance and accountability framework may either be a stand-alone document or may be combined with the *Information Security Governance and Accountability Framework.*

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 2. **2011 Manual: Security Governance and Accountability Framework** **2024 Manual: Information Security Governance and Accountability Framework**	• A security governance and accountability framework for ensuring compliance with the Act and its regulation and for ensuring compliance with the security policies, procedures and practices implemented by the prescribed person or prescribed entity must be established.	• An information security governance and accountability framework for ensuring compliance with PHIPA and its regulations and for ensuring compliance with the information security policies, procedures and practices implemented by the prescribed person or prescribed entity must be established.
	• Must stipulate that the Chief Executive Officer or the Executive Director, as the case may be, is ultimately accountable for ensuring the security of personal health information and for ensuring that the prescribed person or prescribed entity and its agents comply with the security policies, procedures and practices implemented.	• The information security governance and accountability framework must stipulate that the Chief Executive Officer or the Executive Director (or equivalent position), as the case may be, is ultimately accountable for ensuring the: o Security of personal health information; and o prescribed person or prescribed entity and its agent(s) comply with the information security policies, procedures and practices implemented.
	• Must describe the position(s) that have been delegated day-to-day authority to manage the security program must be identified in the security governance and accountability framework and the nature of the reporting relationship to the Chief Executive Officer or the Executive Director.	• The information security governance and accountability framework must identify the position(s) that have been delegated day-to-day authority to manage the information security program; and • The information security governance and accountability framework must describe the nature of the reporting relationship to the Chief Executive Officer or the Executive Director (or equivalent position).
	• Shall set out the responsibilities and obligations of the position(s) that have been delegated day-to-day authority to manage the security program and identify the other individuals, committees and teams that support the position(s) that have been delegated day-to-day authority to manage the security program and their role in respect of the security program.	• The information security governance and accountability framework must set out the responsibilities and obligations of the position(s) that have been delegated day-to-day authority to manage the information security program; • The information security governance and accountability framework must identify the other individuals, committees and teams that have been delegated supporting roles in respect of the information security program; • The information security governance and accountability framework must set out the method and manner by which the information security governance and accountability framework will be communicated to agents of the prescribed person or prescribed entity; and • The information security governance and accountability framework must identify the agent(s) responsible for this 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]
		Board of Directors
	• Must address the role of the Board of Directors in respect of the security program, including whether the security program is overseen by a committee of the Board of Directors.	• The information security governance and accountability framework must also address the: o role of the Board of Directors in respect of the information security program, including any committee of the Board of Directors to which information security oversight has been delegated.
	• Shall set out the frequency with which and the method and manner by which the Board of Directors is updated with respect to the security program, the agent(s) responsible for providing such updates and the matters with respect to which the Board of Directors is required to be updated.	• Frequency with which the Board of Directors is updated with respect to the information security program which, at a minimum, should be annually and preferably in the form of a written report; • Matters on which the Board of Directors must be updated; • Method and manner by which the Board of Directors is updated; and • Agent(s) responsible for providing such updates.
	• Is recommended that the Board of Directors be updated on an annual basis, preferably in the form of a written report: o must address the initiatives undertaken by the security program including security training and the development and implementation of security policies, procedures and practices. o shall include a discussion of the security audits conducted, including the results of and recommendations arising from the security audits and the status of implementation of the recommendations. o Board of Directors must also be advised of any information security breaches investigated, including the results of and any recommendations arising from these investigations and the status of implementation of the recommendations.	• The update provided to the Board of Directors must, at a minimum, address risks that may negatively affect the prescribed person's or prescribed entity's ability to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information that have been ranked as being high risk on the corporate risk register. Such matters should include: o Regular updates on the level of cybersecurity risks facing the prescribed person or prescribed entity, and the measures that have been put in place to mitigate them; o Major financial and other investments required to ensure a robust and sustainable information security governance and accountability framework; o The development, implementation and evaluation of major information technology transformation projects and high-risk information processing applications with information security implications, such as artificial intelligence; o Relevant initiatives undertaken by the information security program including information security 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]
		○ The development and implementation of new information security-related policies, procedures and practices, including those that are of major, corporate-wide significance and have implications for the Board, its members and the proper functioning of its committees; ○ The findings and associated recommendations arising from information security audits, such as threat and risk assessments, including the status of implementation of the mitigations and any other relevant recommendations; ○ Information security breaches that were investigated, as applicable, including the findings, mitigations and other relevant recommendations arising from these investigations and the status of implementation of the mitigations / recommendations; ○ Major information security-related litigation matters, including information security class-action lawsuits facing the prescribed person or prescribed entity; ○ Information security related issues that have been identified through whistle-blowers; and ○ Major changes to the information security governance and accountability framework, including changes of personnel in high-level position(s) that have been delegated day-to- day authority to manage the information security program and related reporting relationships.
	• It is recommended that the security governance and accountability framework be accompanied by a security governance organizational chart.	• The information security governance and accountability framework should be accompanied by an information security governance organizational chart.
	• Shall set out the manner in which the security governance and accountability framework will be communicated to agents of the prescribed person or prescribed entity, the method by which it will be communicated and the agent(s) responsible for this communication.	• The information security governance and accountability framework must set out whether, and the circumstances in which, the above information is provided to the Board of Directors, including the level of detail in which the information is provided.
		<u>Relationship to *Information Security Governance and Accountability Framework*</u>
	• [Note: This governance and accountability framework may either be a stand-alone document or may be combined with the *Privacy Governance and Accountability Framework*.]	• This governance and accountability framework may either be a stand-alone document or may be combined with the *Privacy Governance and Accountability Framework*.

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 3. **2011 Manual: Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program** **2024 Manual: Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Information Security Program**	• The prescribed person or prescribed entity shall establish terms of reference for each committee that has a role in respect of the privacy and/or the security program. • For each committee, the terms of reference must identify the membership of the committee, the chair of the committee, the mandate and responsibilities of the committee in respect of the privacy and/or the security program and the frequency with which the committee meets. • Shall set out to whom the committee reports; the types of reports produced by the committee, if any; the format of the reports; to whom these reports are presented; and the frequency of these reports.	• The prescribed person or prescribed entity must establish terms of reference for each committee that has a role in respect of the privacy and/or the information security program. • For each committee, the terms of reference must identify the: o Membership of the committee; o Chair of the committee; o Mandate and responsibilities of the committee in respect of the privacy and/or the information security program; o Duration of the committee; and o Frequency with which the committee meets. • The terms of reference must also set out: o To whom the committee reports; o The types of reports produced by the committee, if any; o The format of the reports; o To whom these reports are presented; and o The frequency of these reports.
		<u>Risk Management</u>
Policy 4. **Corporate Risk Management Framework**	• A prescribed person or prescribed entity must develop and implement a comprehensive and integrated corporate risk management framework to identify, assess, mitigate and monitor risks, including risks that may negatively affect its ability to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.	• A prescribed person or prescribed entity must develop and implement a comprehensive and integrated corporate risk management framework to: o Identify, assess, rank, mitigate and monitor risks, including risks that may negatively affect its ability to protect the privacy of individuals whose personal health information is received; and o Maintain the confidentiality of that 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]
		Risk Identification, Assessment and Ranking
	• Must address the agent(s) responsible and the process that must be followed in identifying risks that may negatively affect the ability of 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.	• The corporate risk management framework must address the agent(s) responsible; and the process that must be followed and criteria that must be considered in identifying privacy and information security-related risks, and ranking them in terms of their likelihood of occurrence and their potential impact, which must include a discussion of the:
	• Shall include a discussion of the agents or other persons or organizations that must be consulted in identifying the risks; 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.	• Agents or other persons or organizations that must be consulted in identifying, assessing and ranking the risks; • Documentation that must be completed, provided and/or executed. • Agent(s) responsible for completing, providing and/or executing the documentation. • Required content of the documentation, including a description of the rationale underlying the assessment and ranking of risks; and • Agent(s) to whom this documentation must be provided.
		Risk Mitigation

	• Must address the agent(s) responsible, the process that must be followed and the criteria that must be considered in ranking the risks and assessing the likelihood of the risks occurring and the potential impact if they occur.	• The corporate risk management framework must identify the:
		  ○ Agent(s) responsible.
		  ○ Process that must be followed; and
		  ○ Criteria that must be considered in identifying strategies to mitigate the privacy and information security-related risks that were identified, assessed and ranked.

	• Shall include a discussion of the agents or other persons or organizations that must be consulted in assessing and ranking the risks; the documentation that must be completed, provided and/or executed in assessing and ranking the risks; the documentation that must be completed, provided and/or executed in setting out the rationale for the assessment and ranking of the risks; 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 corporate risk management framework must include a process for implementing the mitigation strategies and evaluating the residual risks likely to remain after the mitigation strategies have been implemented. The corporate risk management framework must further identify the:
		  ○ Agents or other persons or organizations that must be consulted in identifying and implementing the mitigation strategies.
		  ○ Agent(s) responsible for:
		  ▪ Assigning other agent(s) to address the mitigations and any other recommendations as required.

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, the process that must be followed and the criteria that must be considered in identifying strategies to mitigate the actual or potential risks to privacy that were identified and assessed, the process for implementing the mitigation strategies and the agents or other persons or organizations that must be consulted in identifying and implementing the mitigation strategies. o This includes identifying the agent(s) responsible for assigning other agent(s) to implement the mitigation strategies, for establishing timelines to implement the mitigation strategies, and for monitoring and ensuring that the mitigation strategies have been implemented.	▪ Establishing timelines to address the mitigations and any other recommendations. ▪ Monitoring and ensuring the treatment of the mitigations and any other relevant recommendations within stated timelines; and ▪ Evaluating the residual risks remaining after implementation.
	• Must address the documentation that must be completed, provided and/or executed in identifying, implementing, monitoring and ensuring the implementation of the mitigation strategies; 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.	• Documentation that must be completed, provided and/or executed. • Agent(s) responsible for completing, providing and/or executing the documentation. • Required content of the documentation, including a description of the rationale underlying the strategies to mitigate risks and evaluating residual risks; and • Agent(s) to whom this documentation must be provided.
		<u>Approval</u>
		• The corporate risk management framework must set a process for approving and endorsing the results of the risk management process, which includes the identification, assessment and ranking of risks, the identification, implementation, and monitoring of mitigation strategies, and the evaluation of residual risks. • The corporate risk management framework must also: o Identify the agent(s) responsible for determining whether to approve and endorse or not to approve and endorse the results of the risk management process. o Address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve and endorse, or to not approve and endorse, the results of the risk management process; and o Set out the manner of documenting the: ▪ Decision to approve and endorse, or to not approve and endorse.

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]
		▪ Results of the risk management process and the reasons for the decision; and ▪ Agent(s) responsible for completing this documentation.
		<u>Risk Communication and Reporting</u>
	• Must also address the manner and format in which the results of the corporate risk management process, including the identification and assessment of risks, the strategies to mitigate actual or potential risks to privacy and the status of implementation of the mitigation strategies, are communicated and reported. o This involves identifying the agent(s) responsible for communicating and reporting the results of the corporate risk management process, the nature and format of the communication; and to whom the results will be communicated and reported, including to the Chief Executive Officer or the Executive Director. Approval and endorsement of the results of the risk management process, including the agent(s) responsible for approval and endorsement, shall also be outlined.	• The corporate risk management framework must: o Address the manner, circumstances and format in which the results of the corporate risk management processes are communicated and reported, which involves identifying: ▪ The agent(s) responsible for communicating and reporting the results of the corporate risk management process, the nature, format and content of the communication, including the level of detail. ▪ To whom the results of the corporate risk management process will be communicated and reported to, including whether the results must be communicated to the Chief Executive Officer or the Executive Director (or equivalent position); and o Outline the process that must be followed for the approval and endorsement of the results of the risk management process, including the agent(s) responsible for approval and endorsement.
		<u>Risk Register</u>
	• Must require that a corporate risk register be maintained and that the corporate risk register be reviewed on an ongoing basis in order to ensure that all the risks that may negatively affect the ability of 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 continue to be identified, assessed and mitigated. • Must identify the frequency with which the corporate risk register must be reviewed and the agent(s) responsible and the process that must be followed in reviewing and amending the corporate risk register.	• Further, the corporate risk management framework must: o Require that the corporate risk register be maintained and reviewed on an ongoing basis, and at a minimum on an annual basis, in order to ensure that all relevant privacy and information security-related risks continue to be identified, assessed, ranked and mitigated. o Identify the frequency with which the corporate risk register must be reviewed. o Specify the agent(s) responsible for the review; and o Identify the process that must be followed in reviewing and amending the corporate risk register.

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]
		Integration of Risk Management Framework
	• Shall address the manner in which the corporate risk management framework will be integrated into the policies, procedures and practices of the prescribed person or prescribed entity and into the projects undertaken by the prescribed person or prescribed entity and the agent(s) responsible for integration.	• The corporate risk management framework of the prescribed person or prescribed entity must: o Ensure that the risks identified in the corporate risk management framework are addressed in the policies, procedures and practices of the prescribed person or prescribed entity and in the projects undertaken by the prescribed person or prescribed entity; and o Identify the agent(s) responsible for ensuring that the risks are addressed.
		Compliance, Audit and Enforcement
		• 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* and/or the *Policy, Procedures and Practices for Information Security Breach Management*, as the case may be, if an agent breaches or believes there may have been breach of this policy, procedures or practices. 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 5. **Corporate Risk Register**	• A prescribed person or prescribed entity must develop and maintain a corporate risk register that identifies each risk identified that may negatively affect the ability of 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.	• A prescribed person or prescribed entity must develop and maintain a corporate risk register that: o Identifies and integrates privacy and information security-related risks, among other enterprise-wide risks, that may negatively affect the ability of 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.
	• For each risk identified, the corporate risk register shall include an assessment of the risk, a ranking of the risk, the mitigation strategy to reduce the likelihood of the risk occurring and/or to reduce the impact of the risk if it does occur, the date that the mitigation strategy was implemented or is required to be implemented, and the agent(s) responsible for implementation of the mitigation strategy.	• For each privacy and information security-related risk identified, the corporate risk register must include: o An assessment of the risk; o A ranking of the risk; o The mitigation strategy that has been identified to reduce the risk, including the: o Date that the mitigation strategy was implemented or is required to be implemented; o Agent(s) responsible for implementation of the mitigation strategy; and o Residual risk likely to remain despite implementation of the mitigation strategy.

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 Maintaining a Consolidated Log of Recommendations** **2024 Manual: Policy, Procedures and Practices for Maintaining a Consolidated Log of Recommendations**	• The prescribed person or prescribed entity shall develop and implement a policy and associated procedures requiring a consolidated and centralized log to be maintained of all recommendations arising from privacy impact assessments, privacy audits, security audits and the investigation of privacy breaches, privacy complaints and security breaches.	• A prescribed person or prescribed entity must at a minimum, develop and implement a policy, procedures and practices that: o Requires a consolidated and centralized log of all findings, mitigations and other recommendations arising from privacy impact assessments, privacy audits, information security audits and the investigation of privacy breaches, privacy complaints and/or information security breaches.
	• Shall include recommendations made by the Information and Privacy Commissioner of Ontario that must be addressed by the prescribed person or prescribed entity prior to the next review of its practices and procedures.	• Requires the inclusion of recommendations, orders and decisions made by the Information and Privacy Commissioner of Ontario under PHIPA and its regulations.
	• Shall set out the frequency with which and the circumstances in which the consolidated and centralized log must be reviewed, the agent(s) responsible for reviewing and amending the log and the process that must be followed in this regard.	• Sets out the: o Frequency with which and the circumstances in which the consolidated and centralized log must be reviewed; o Agent(s) responsible for reviewing and amending the log; and o Process that must be followed.
	• Recommended that the log be updated each time that a privacy impact assessment, privacy audit, security audit, investigation of a privacy breach, investigation of a privacy complaint, investigation of an information security breach or review by the Information and Privacy Commissioner of Ontario is completed and each time that a recommendation has been addressed.	• The log should be updated each time that: o A privacy impact assessment, privacy audit, information security audit, investigation of a privacy breach, investigation of a privacy complaint, investigation of an information security breach, or review by the Information and Privacy Commissioner of Ontario is completed; and o One or more recommendations, orders or decisions, including those issued by the Information and Privacy Commissioner of Ontario under PHIPA and its regulations, have been addressed.
	• Recommended that the consolidated and centralized log be reviewed on an ongoing basis in order to ensure that the recommendations are addressed in a timely manner.	• The consolidated and centralized log should be reviewed on an ongoing basis in order to ensure that the mitigations / recommendations, orders and decisions, including those issued by the Information and Privacy Commissioner of Ontario under PHIPA and its regulations, are addressed in a timely manner.

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* and the *Policy and Procedures In Respect of Security Audits*, as the case may be, and must set out the frequency with which the policy and procedures will be audited and 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*, as the case may be, 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* and/or the *Policy, Procedures and Practices for Information Security Breach Management*, as the case may be, if an agent breaches or believes there may have been breach of this policy, procedures or practices; 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 7. **Consolidated Log of Recommendations**	• A prescribed person or prescribed entity must develop and maintain a consolidated and centralized log of all recommendations arising from privacy impact assessments, privacy audits, security audits, the investigation of privacy breaches, the investigation of privacy complaints, the investigation of information security breaches and reviews by the Information and Privacy Commissioner of Ontario.	• The consolidated log of recommendations of a prescribed person or prescribed entity must be developed and maintained to include: o A consolidated and centralized log of all findings, mitigations and other recommendations arising from privacy impact assessments, privacy audits, information security audits, the investigation of privacy breaches, the investigation of privacy complaints, and/or the investigation of information security breaches; and o Recommendations, orders and decisions made by 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]
	• Must set out the name and date of the document, investigation, audit and/or review from which the recommendation arose.	• The consolidated log of recommendations must set out the: o Name and date of the document, investigation, audit; and/or o Review from which the findings, mitigations and other recommendations, orders or decisions, including those issued by the Information and Privacy Commissioner of Ontario under PHIPA and its regulations, arose.
	• For each recommendation, the log must set out the recommendation made, the manner in which the recommendation was addressed or is proposed to be addressed, the date that the recommendation was addressed or by which it is required to be addressed, and the agent(s) responsible for addressing the recommendation.	• For each finding, mitigation and other recommendations, order or decision, the log must set out the: o Finding, recommendation, order or decision made; o Manner in which the recommendation, order or decision was addressed or is proposed to be addressed; o Date that the mitigation / recommendation, order or decision was addressed or by which it is required to be addressed; and o Agent(s) responsible for addressing the recommendation, order or decision.
		<u>Business Continuity and Disaster Recovery</u>
Policy 8. **Business Continuity and Disaster Recovery Plan**	• A policy and associated procedures must be developed and implemented to protect and ensure the continued availability of the information technology environment of the prescribed person or prescribed entity in the event of short and long-term business interruptions and in the event of threats to the operating capabilities of the prescribed person or prescribed entity, including natural, human, environmental and technical interruptions and threats.	• A policy, procedures and practices must be developed and implemented to protect and ensure the continued availability of the information environment of the prescribed person or prescribed entity in the event of: o Short and long-term business interruptions; and o Threats to the operating capabilities of the prescribed person or prescribed entity, including natural, human, environmental and technical interruptions and threats.
	• Must address notification of the interruption or threat, documentation of the interruption or threat, assessment of the severity of the interruption or threat, activation of the business continuity and disaster recovery plan and recovery of personal health information.	• The business continuity and disaster recovery plan must also address the: o Notification of the interruption or threat; o Documentation of the interruption or threat; o Assessment of the severity of the interruption or threat; o Activation of the business continuity and disaster recovery plan; and o Recovery 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]
		Notification of Interruption or Threat
	• In relation to notification of the interruption or threat, shall identify the agent(s) as well as the other persons or organizations that must be notified of short and long-term business interruptions and threats to the operating capabilities of the prescribed person or prescribed entity and the agent(s) responsible for providing such notification.	• In relation to notification of the interruption or threat, the business continuity and disaster recovery plan must identify the: o Agent(s) as well as the other persons or organizations that must be notified of short and long-term business interruptions and threats to the operating capabilities of the prescribed person or prescribed entity; and o Agent(s) responsible for providing such notification;.
	• Must address the time frame within which notification must be provided, the manner and format of notification, the nature of the information that must be provided upon notification and any documentation that must be completed, provided and/or executed	• Timeframe within which notification must be provided; • Manner and format of notification; • Nature of the information that must be provided upon notification; and • Documentation that must be completed, provided and/or executed.
	• A contact list must be required to be developed and maintained of all agents, service providers, stakeholders and other persons or organizations that must be notified of business interruptions and threats and the business continuity and disaster recovery plan must identify the agent(s) responsible for creating and maintaining this contact list.	• Process for developing and maintaining an updated contact list of all agents, service providers, stakeholders and other persons or organizations that must be notified; and • Agent(s) responsible for creating and maintaining this contact list.
		Severity Assessment
	• In relation to the assessment of the severity level of the interruption or threat, shall identify the agent(s) responsible for the assessment, the criteria pursuant to which this assessment is to be made and the agents and other persons or organizations that must be consulted in assessing the severity level of the interruption or threat.	• In relation to the assessment of the severity level of the interruption or threat, the business continuity and disaster recovery plan must identify the: o The agent(s) responsible for the assessment; o The criteria pursuant to which this assessment is to be made; and o The agents and other persons or organizations that must be consulted in assessing the severity level of the interruption or threat.
	• Must address the documentation that must be completed, provided and/or executed resulting from or arising out of this assessment; the required content of the documentation; the agent(s) to whom the documentation must be provided; and to whom the results of this assessment must be reported.	• The documentation that must be completed, provided and/or executed resulting from or arising out of this assessment, including the required content of the documentation; • The agent(s) to whom the documentation must be provided; and • To whom the results of this assessment must be reported.

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]
		Initial Impact Assessment
	• In relation to the assessment of the interruption or threat, shall set out the agent(s) responsible and the process that must be followed in conducting an initial impact assessment of the interruption or threat, including its impact on the technical and physical infrastructure and business processes of the prescribed person or prescribed entity. This includes the agents and other persons or organizations that are required to be consulted in undertaking the assessment; the requirements that must be satisfied and the criteria that must be utilized in conducting the assessment; 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 agent(s) to whom the results of the initial impact assessment must be communicated.	• In relation to the assessment of the interruption or threat, the business continuity and disaster recovery plan must set out: o The agent(s) responsible for the business continuity and disaster recovery plan; and o The process that must be followed in conducting an initial impact assessment of the interruption or threat, including its impact on the technical and physical infrastructure and business processes of the prescribed person or prescribed entity. o In outlining the initial impact assessment process to be followed, the business continuity and disaster recovery plan must identify the: ▪ Agent(s) and other person(s) or organization(s) that are required to be consulted in undertaking the assessment; ▪ Requirements that must be satisfied and the criteria that must be utilized in conducting the assessment; ▪ Documentation that must be completed, provided and/or executed; ▪ Agent(s) responsible for completing, providing and/or executing the documentation; ▪ Agent(s) to whom the documentation must be provided; and ▪ Agent(s) to whom the results of the initial impact assessment must be communicated.
		Damage Assessment
	• Must identify the agent(s) responsible for conducting and preparing a detailed damage assessment in order to evaluate the extent of the damage caused by the threat or interruption and the expected effort required to resume, recover and restore infrastructure elements, information systems and/or services.	• The business continuity and disaster recovery plan must identify the agent(s) responsible for conducting and preparing a detailed damage assessment in order to evaluate the extent of the damage caused by the threat or interruption and the expected effort required to resume, recover and restore components within the information environment.

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 the assessment is required to be conducted;
	  ○ the agents and other persons or organizations that are required to be consulted in undertaking the assessment;
	  ○ the requirements that must be satisfied and the criteria that must be considered in undertaking the assessment;
	  ○ 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 agent(s) to whom the results of the assessment must be communicated.
		• The business continuity and disaster recovery plan must identify the:
		  ○ Manner in which the assessment is required to be conducted;
		  ○ Agent(s) and other persons or organizations that are required to be consulted in undertaking the assessment;
		  ○ Requirements that must be satisfied and the criteria that must be considered in undertaking the assessment;
		  ○ Documentation that must be completed, provided and/or executed;
		  ○ Agent(s) responsible for completing, providing and/or executing the documentation;
		  ○ Agent(s) to whom the documentation must be provided; and
		  ○ Agent(s) to whom the results of the assessment must be communicated.

		<u>Resumption and Recovery Following the Interruption or Threat</u>

	• Shall identify the agent(s) responsible for resumption and recovery, the procedure that must be utilized in resumption and recovery for each critical application and business function, the prioritization of resumption and recovery activities, the criteria pursuant to which the prioritization of resumption and recovery activities is determined, and the recovery time objectives for critical applications.	• The business continuity and disaster recovery plan must also identify the:
		  ○ Agent(s) responsible for resumption and recovery;
		  ○ Procedure that must be utilized in resumption and recovery for each critical application and business function;
		  ○ Prioritization of resumption and recovery activities;
		  ○ Criteria pursuant to which the prioritization of resumption and recovery activities is determined; and
		  ○ Recovery time objectives for critical applications.

	• Shall include a discussion of the agents and other persons or organizations that are required to be consulted with respect to resumption and recovery activities; the documentation that must be completed, provided and/or executed; the required content of the documentation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of these activities must be communicated.	• Agents and other persons or organizations that are required to be consulted with respect to resumption and recovery activities; • Documentation that must be completed, provided and/or executed; • Required content of the documentation; • Agent(s) responsible for completing, providing and/or executing the documentation; • Agent(s) to whom the documentation must be provided; and • Agent(s) to whom the results of these activities must be communicated.

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]
		Inventory of Critical Applications, Business Functions, Hardware and Software
	• Must require that an inventory be developed and maintained of all critical applications and business functions and of all hardware and software, software licences, recovery media, equipment, system network diagrams, hardware configurations, software configuration settings, configuration settings for database systems and network settings for firewalls, routers, domain name servers, email servers and the like.	• The business continuity and disaster recovery plan must require that an inventory be developed and maintained of all critical applications and business functions and of all hardware and software, software licences, recovery media, equipment, system network diagrams, hardware configurations, software configuration settings, configuration settings for database systems and configuration settings for methods to detect unauthorized connections and devices, routers, domain name servers, email servers and the like.
	• Must identify the agent(s) responsible for developing and maintaining the inventory, the agent(s) and other persons and organizations that must be consulted in developing the inventory, and the criteria upon which the determination of critical applications and business functions must be made.	• The business continuity and disaster recovery plan must identify the: o Agent(s) responsible for developing and maintaining the inventory; o Agent(s) and other person(s) and organization(s) that must be consulted in developing the inventory; and o Criteria upon which the determination of critical applications and business functions must be made.
		Documenting Business Interruptions and Threats
	• Must discuss the procedure by which decisions made and actions taken during business interruptions and threats to the operating capabilities of the prescribed person or prescribed entity will be documented and communicated and by whom and to whom they will be communicated.	• The policy, procedures and practices must detail: o How decisions made and actions taken during business interruptions and threats to the operating capabilities of the prescribed person or prescribed entity will be documented and communicated; o The agent(s) responsible; and o By whom and to whom the business interruptions and threats to the operating capabilities 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]
		Testing, Maintenance and Assessment of Business Continuity and Disaster Recovery Plan
	• Must address the testing, maintenance and assessment of the business continuity and disaster recovery plan. This includes identifying the frequency of testing; the agent(s) responsible for ensuring that the business continuity and discovery plan is tested, maintained and assessed; the agent(s) responsible for amending the business continuity and discovery plan as a result of the testing; the procedure to be followed in testing, maintaining, assessing and amending the business continuity and discovery plan; and the agent(s) responsible for approving the business continuity and disaster recovery plan and any amendments thereto.	• The business continuity and disaster recovery plan must also address the testing, maintenance and assessment of the business continuity and disaster recovery plan. This includes identifying the: o Frequency of testing, which at a minimum must be done on an annual basis; o Agent(s) responsible for ensuring that the business continuity and disaster recovery plan is tested, maintained and assessed; o Agent(s) responsible for amending the business continuity and disaster recovery plan as a result of the testing; o Procedure to be followed in testing, maintaining, assessing and amending the business continuity and disaster recovery plan; and o Agent(s) responsible for approving the business continuity and disaster recovery plan and any amendments thereto.
		Communication of Business Continuity and Disaster Recovery Plan
	• Must address the agent(s) responsible and the procedure to be followed in communicating the business continuity and disaster recovery plan to all agents, including any amendments thereto, and the method and nature of the communication.	• The business continuity and disaster recovery plan must identify: o The agent(s) responsible and the procedure to be followed in communicating the business continuity and disaster recovery plan to all agents, including: ▪ Any amendments thereto; and ▪ The method and nature of the communication.
	• Shall identify the agent(s) responsible for managing communications in relation to the threat or interruption, including the method and nature of the communication.	• The agent(s) responsible for managing communications in relation to the threat or interruption, including the method and nature of 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 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* and/or the *Policy, Procedures and Practices for Information Security Breach Management*, as the case may be, if an agent breaches or believes there may have been breach of this policy, procedures or practices; 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*.